EMCO Ping Monitor 9

Table of Contents

Chapter 1: Introduction

Welcome to EMCO Ping Monitor. You have chosen an easy-to-use software product that allows you to monitor host states and the connection quality of monitored hosts. The program is designed to alert you when there are issues with monitoring hosts, when hosts change their states or when monitoring values exceed thresholds. The program collects monitoring statistics, including different monitoring metrics, and can generate reports with detailed information on the performance of any monitored host. This manual provides you with detailed information on all of the program features.
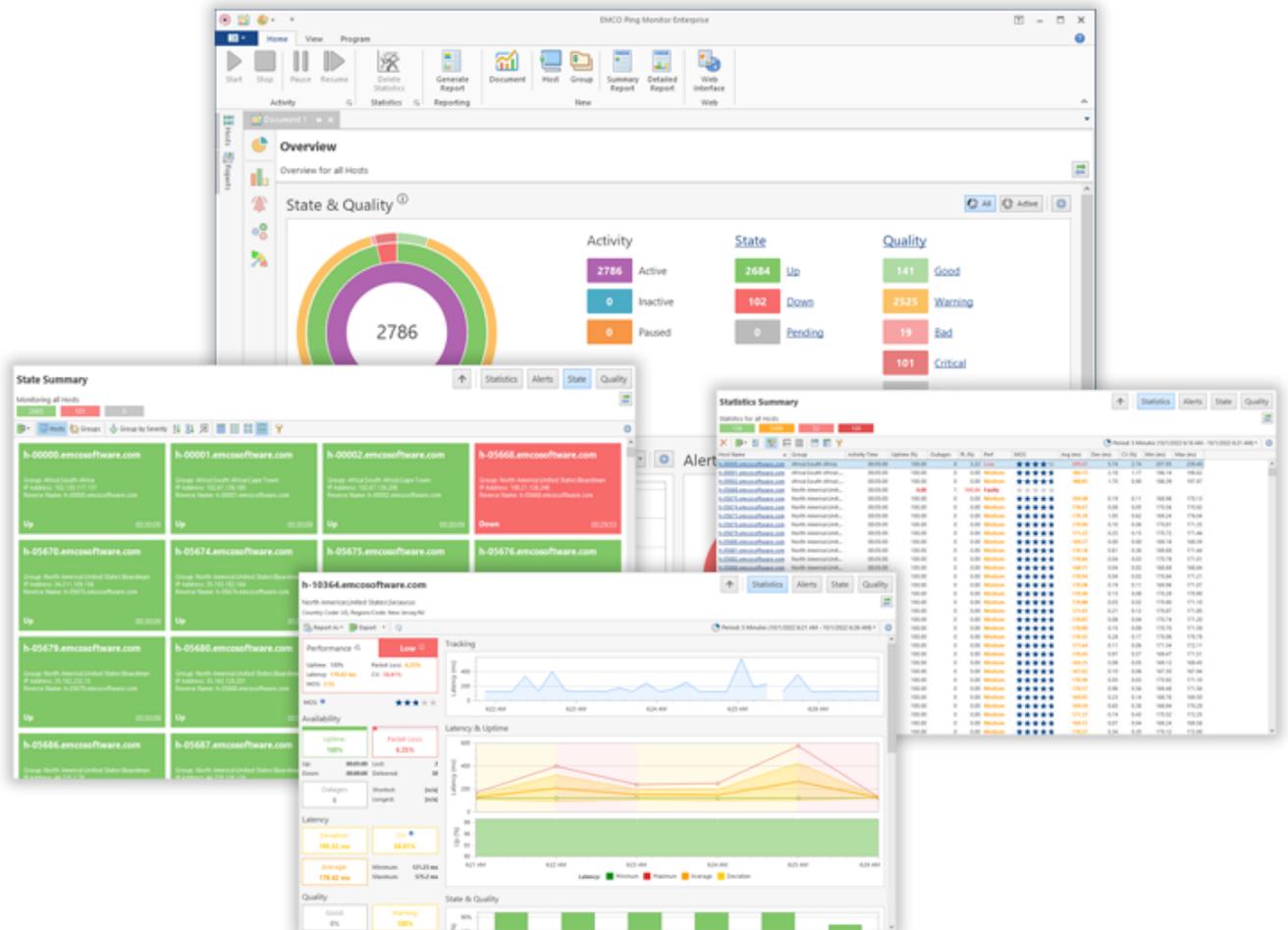
Using Documentation

EMCO Ping Monitor was designed to be a tool with an intuitive user interface that can be used by people with different levels of technological knowledge. The program encompasses an initial configuration wizard that helps you to configure the program for the first start. In addition, every interface dialog provides you with hints and clear error messages. It should help you to use the program successfully without reading this manual. Anyway, it's recommended to review the Getting Started guide to familiarize yourself with the main features of the program.

To get detailed information on the program features, settings and user interface views, browse the manual content and choose the section you want to read.

Getting Help

If you face a problem, it makes sense to check the errors reported in the **Log** view. If the problem can be resolved by a user, the error in the log includes troubleshooting information, so you can follow the suggestions to resolve the problem. In other cases, you may contact the support team at *https://emcosoftware.com/support*.

To get help on the problem, you need to provide the support team with the problem details. For example, you can send the error notification you received and the steps you had performed before getting this error. Provide the support team with all the available information regarding the problem to speed up the problem reproduction and troubleshooting.

Chapter 2: Getting Started

EMCO Ping Monitor is software that monitors multiple hosts simultaneously. The program sends ICMP echo requests to hosts on a regular basis and analyzes echo replies to detect the state and the connection quality of the monitored hosts. Ping results are saved by the program and are analyzed to calculate metrics used to evaluate the quality of the connection between the monitoring server and the monitored host.

Ping Monitor is a tool that helps you to proactively identify problems in your network infrastructure and reduce downtime. Below you can find a list of typical scenarios of using Ping Monitor.

- **Host state monitoring**. You can use the program to continuously monitor the state of hosts (i.e. to detect if they are up or down) using ICMP pings and be notified when a host state changes. The program provides you with information on the current state of every host and the entire monitoring system by displaying the quantity of hosts in different states.

- **Connection quality monitoring**. In addition to monitoring the host states, the program can monitor the quality of the network connections using the metrics based on ICMP pings. When a host is up, its connection quality may vary; therefore, a continuous monitoring of the quality allows preventing potential problems. The program can send you notifications when the connection quality changes, so you can take required actions if needed.

6

- **Host performance analysis**. The program saves monitoring statistics, so you can access it anytime to see how the host performance metrics changed over time. You can estimate the host performance for any historical time range and generate reports with detailed statistics.

- **Integration with other systems**. It is possible to integrate the program with other systems. For example, the program can notify other systems when the host state or quality change. You can also export raw ping data to open them in other systems.

In the following chapters, you can learn how to use the program in the scenarios listed above and in other cases. Getting Started provides you with a general overview of the program features and practical advices on using the program. For detailed information, you can refer to other sections of the product documentation.

How the Program Works

The program is designed for simultaneous monitoring of multiple hosts. The number of monitored hosts depends on the program license. The Free edition allows monitoring of up to five hosts, and the Professional edition allows monitoring of up to 250 hosts. The Enterprise edition doesn't limit the number of hosts. The practical limit of monitored hosts depends on the used hardware. You can monitor 8,000+ hosts on modern hardware. The technical limit of the program is 32,000 hosts.

What is Ping Monitoring and How it Works

The program uses the ICMP protocol to monitor hosts over a network. Every host is monitored independently from other hosts to guarantee a high monitoring performance. The program sends ICMP echo requests to a monitored host and analyzes its echo replies. Echo requests, which are called pings, are sent on a regular basis at particular time intervals, so the program continuously interacts with the host and can detect the moment when it stops replying to ping requests.

When the program sends a ping echo request and gets a reply from the host, the ping is considered as passed, and the program saves its round-trip time. When there is no echo reply from the host, the ping is considered as failed. If pings fail, it means that there is no connection between the program (the Ping Monitor server that sends pings) and the monitored host.

> What is the reason for ping failure? A ping can fail due to different reasons, for example, when the pinged host is turned off, when there is a network problem between the source and destination, or when there is a DNS problem and the host name cannot be resolved to the correct IP address. Usually, a ping fails when its round-trip time exceeds the configured timeout. It happens when the pinged host or the network infrastructure is overloaded and ping requests cannot be processed in time.

How the Host State is Detected

One of the main goals of Ping Monitor is helping you to detect problems with the monitored hosts automatically, so the program continuously monitors the hosts to detect their current state. The Up state means that the monitored host works and replies to ping requests. The Down state means that the monitored host is unreachable and it doesn't reply to ping requests.

How does the program detect the host states using pings? If pings pass successfully, it means that the host works, so it has the Up state. If pings fail, it means that the monitored host isn't reachable. A single failed ping usually doesn't indicate a problem, because pings can fail sometimes even for properly working hosts. However, if several pings fail in a row, it means that there is a problem and the host state should be changed to Down.

All the monitoring parameters used by the program are configurable and can be changed if required. Below you can see an example of a host monitoring sequence to understand how monitoring works and what parameters are used in the monitoring configuration.

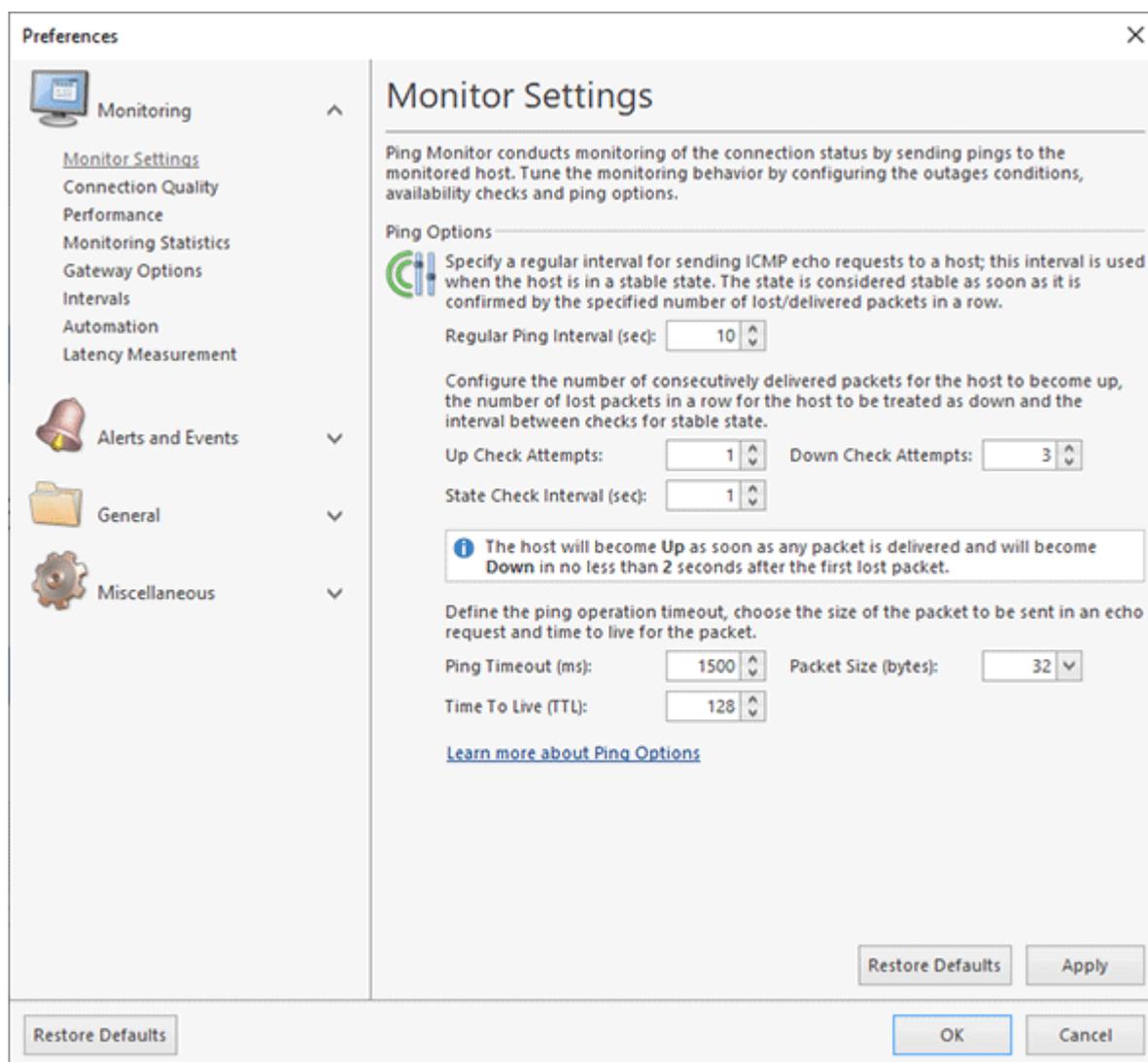## Monitoring Sequence
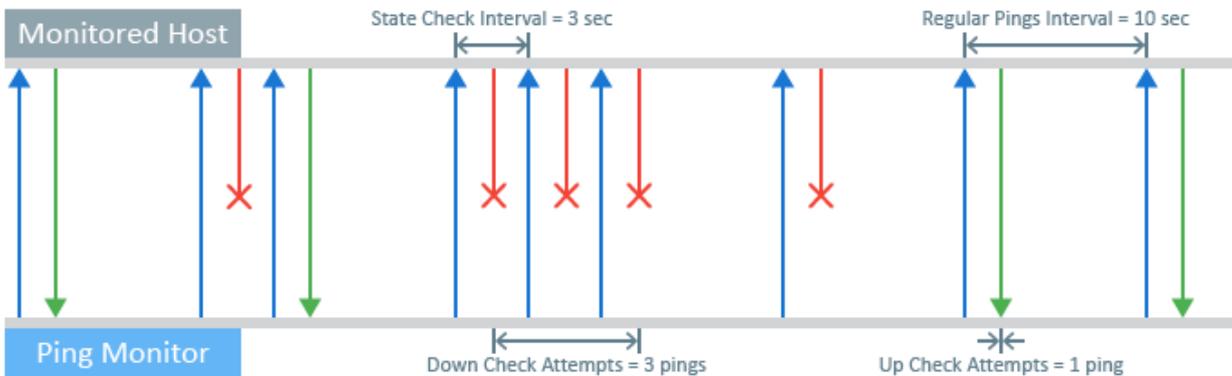
Host States

The program continuously monitors a host by sending ping echo requests on a regular basis at a **Regular Pings Interval** (*10 sec* in the example). If a ping fails, the next ping request is sent after a **State Check Interval** (*3 sec* in the example). As you can see, the program uses different ping intervals when the host state is stable (either Up or Down) and when it is changing (from Up to Down or vice versa). Using different intervals allows you to tune monitoring according to your needs.

The program uses **Up Check Attempts** (*1 ping* in the example) and **Down Check Attempts** (*3 pings* in the example) to detect the state changes. For example, using the default settings the state changes from Up to Down when 3 pings fail in a row. Using the default settings, the host state changes from Down to Up when 1 ping has passed.

When a host goes Down, the program creates an alert to inform you about the problem. A list of active alerts is displayed in the program, so you can review the current problems. You can configure the program to send e-mail notifications, show balloons in Windows Tray, play sounds or execute custom actions on alerts or events, such as host state changes, etc.

Changing and Tuning the Monitoring Settings

You can change the used configuration on the **Monitor Settings** page of the program preferences `Pic 1`. These settings are used by all monitored hosts. Using a commercial edition of the program, you can override the common settings and specify individual settings for hosts and groups. To enter individual settings for a host/group, you need to open it for editing and switch to **Monitor Settings**.

Pic 1. Monitor Settings

Monitoring settings allow you to change ping intervals and to check attempts used to detect Up/Down states. These settings were explained above. You can also change the ping packet size, the ping timeout and the TTL (time to live). Note that depending on the used edition of the program and the initial configuration set at the first start of the program, the default monitoring settings may vary, but you can change them anytime if required.

What settings should you use in different cases? There is no universal answer to this question, because the optimal settings depend on the case, but it makes sense to follow these recommendations:

- **Don't use too large and too small intervals**. Small intervals increase monitoring workload, which may matter if you monitor hundreds or thousands of hosts. For example, if you reduce the interval by 2 times, the program will send twice as many pings during the same interval. Large intervals make monitoring less responsive because it requires more time to detect state

changes. For example, it makes no sense to ping a host once per hour because a host state may change many times during an hour and these changes will not be detected.

- **Avoid false positive reports by increasing Up/Down check attempts**. If you set check attempts to just one ping, the host state can be changed on every ping. If the connection is unstable, you will constantly notice state changes and will not be able to react appropriately. By increasing the number of check attempts, one reduces the number of potential false-positive state changes; but at the same time, too large a number of check attempts makes monitoring less responsive. For example, if **State Check Interval** is set to 10 seconds and you set **Down Check Attempts** to 1000 pings, an outage will be detected 10.000 sec later at the earliest, i.e. over 2 hours after the onset of problems.

> How to estimate the monitoring responsiveness, i.e. the time required for the monitoring system to detect a host state change? The program sends ping requests on a regular basis, so it immediately detects that pings start to fail, but it isn't reported as a host state change to avoid false positives until the number of failed pings detected in a row reaches the **Down Check Attempts** value. In this case, pings are sent with a **State Check Interval**. To evaluate the minimum time required to report the Down state after the first failed ping, you need to multiply **State Check Interval** by **Down Check Attempts**. To evaluate the minimum time required to report the Up state after the first passed ping, you need to multiply **State Check Interval** by **Up Check Attempts**.

What settings should I use if I need to detect state changes no sooner than in 2 minutes after the problem onset (in other words, outages shorter than 2 minutes shouldn't be detected)?

In this case, first we need to decide how often the host should be pinged in the transitional state. If it should be pinged every five seconds (**State Check Interval** should be set accordingly), how many pings do we need to send to detect a state change? Let's calculate: 120 sec. (2 min.) / 5 sec. = 24, so we need 24 pings to detect a host change with this interval and can enter this number as **Up Check Attempts** and **Down Check Attempts**.

Note that the interval and the number of attempts are inversely related, so as one value is increased, the other one should be decreased if you wish to maintain the same monitoring responsiveness. In the above example, if we set **State Check Interval** to 3 sec., how many pings are required to detect a state change? This number can be calculated as 120 sec. (2 min.) / 3 sec. = 40, thus we need 40 pings to detect a host change with this interval and need to set **Up Check Attempts** and **Down Check Attempts** to 40 pings.

Local, Remote and Web Access to the Program

The program has a client/server architecture. The server works as a Windows service to monitor hosts, send notifications and generate reports. The client is a Windows application with a GUI that allows you to connect to the server and manage the monitored hosts, review statistics, change settings, etc. When installing the program, you can select to install the server, the client, or both. Thus, you can install the client and the server on the same PC or different PCs.

It is recommended to install the Ping Monitor server on a Windows server or another computer that is always on, so monitoring can run in the 24/7 mode. The Ping Monitor GUI client can be installed on the same or a different computer, since the program allows clients to connect to the server remotely over a LAN/WAN/VPN. You can install multiple clients that can connect to the same server and work concurrently. To be able to connect to the server remotely, you need to open ports *48030* and *48031* in the firewall on the computer where the server is installed.

When running the Ping Monitor client, you should specify if you would like to connect to a server installed locally or remotely `Pic 1`. If you wish to connect to a remote server, you should enter its host name or IP address.

> The program supports different numbers of simultaneous client connections depending on the used license. The Free edition of the program supports only one connection, the Professional edition supports two connections, and the Enterprise edition doesn't limit the number of simultaneous connections.

The server requires user authentication, so when using the default settings, you need to specify a Windows account that is a member of the Administrators group on the computer where the server is installed. If your current Windows session satisfies this condition, you can enable the **Use Windows session Credentials** option and skip entering the username and password.


Pic 1. The server connection dialog

The program allows you to configure who has access to the server. You can allow access for selected Windows users/groups and can assign different roles in the program to different users. For example, you can provide an administrative access with all permissions to a specific user group and a read-only access to all other users. You can learn more about using roles and permissions in the Access Control chapter.

> The program uses secure communication between the client and the server, so all the data traffic is encrypted. By default, the program uses a self-signed SSL certificate, and you get a warning that the used certificate isn't trusted when you connect to the server. If you have a SSL certificate, it's recommended to specify it in the program preferences to validate the identity of the server when connecting to it remotely.

Monitoring Web Interface

In addition to the GUI client, you can also use the monitoring web interface that offers features similar to those available in the GUI client. The web interface allows you to review the state and quality of the monitored hosts, get detailed host statistics and start/stop monitoring of hosts and groups **Pic 2**. The current version of the program doesn't allow managing hosts and settings through the web, so you need to use the GUI client to add/delete hosts and to change the program settings.
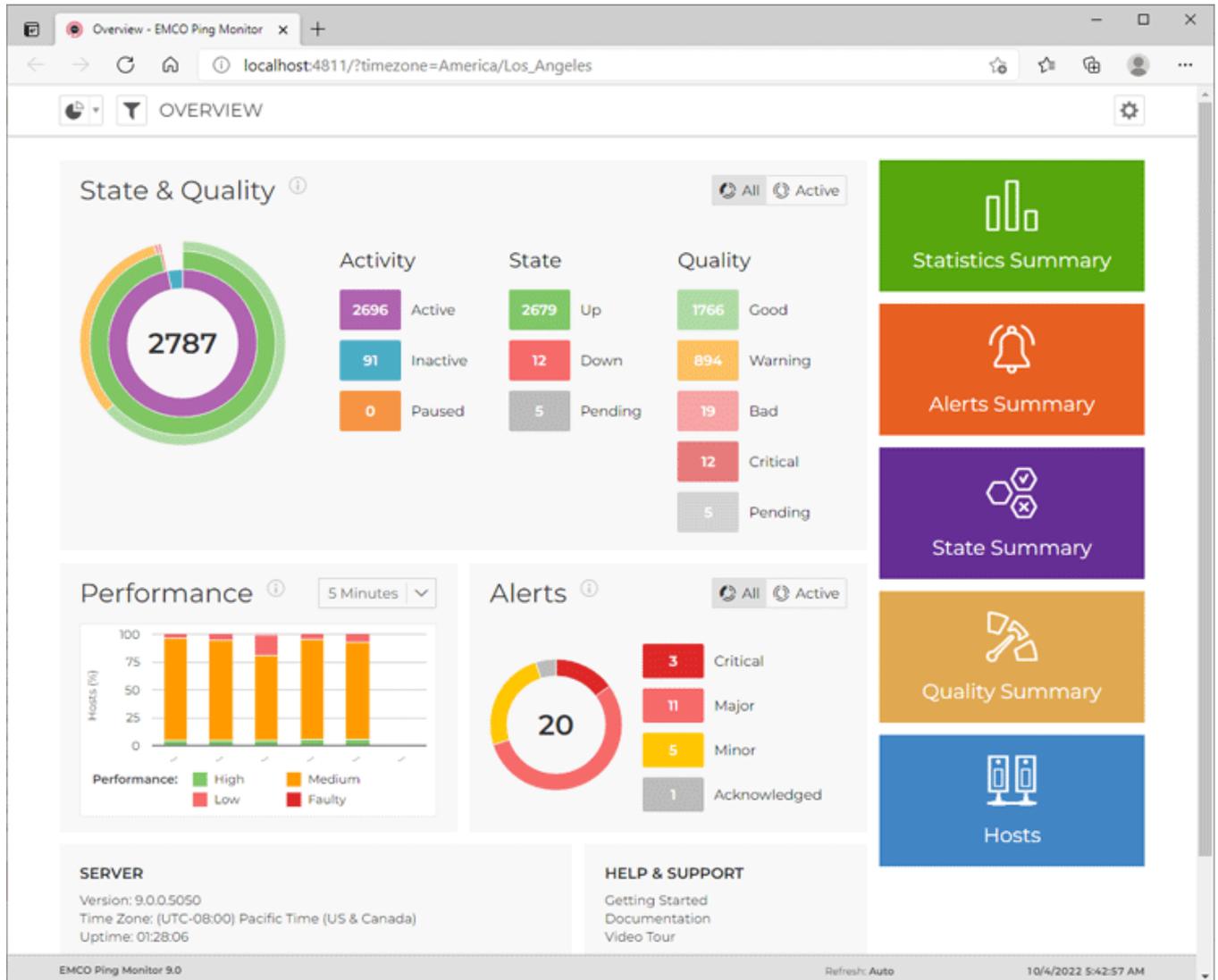
Pic 3. Monitoring web interface

The program uses Microsoft IIS to deploy the monitoring web interface. During installation of Ping Monitor, the program installer automatically activates Microsoft IIS and deploys the monitoring web interface if you choose to install it. When installed with default parameters, a corresponding shortcut appears in the Windows Start menu, and you can use it to open the monitoring web interface in a browser.

Managing and Configuring Hosts

At the first start of the program, you have an option to specify hosts that will be monitored by the program. After you have entered hosts, you can find them in the **Hosts** view located on the left of the main screen of the program. Using this view, you can see all the hosts added to the program and check if they are currently being monitored. In the **Hosts** view, you can add/delete hosts and manage their settings, so you need to open this view to add all the hosts that you plan to monitor.

Adding New Hosts

There are multiple ways for adding hosts to the program. You can use one of the following approaches depending on your needs:

- **Add a single host**. To add a single host you need to select **New > Host** in the context menu or on the toolbar of the **Hosts** view. In the dialog that appears, you can add a host by name or IP address. The program supports hosts with dynamic IP addresses: in this case, you need to enter the host name and turn on the option **This host uses a dynamic IP address**, so the program will resolve the host name to an IP address at every ping.

- **Add multiple hosts by an IP range**. This option can be used when you need to add multiple hosts at once and all of them are within the same IP range. To use this option, select **New > Host** in the context menu or on the toolbar of the **Hosts** view. You should add the start and end addresses of the IP range, and all IPs from this range will be added into the program `Pic 1`. By default, these hosts are added as IP addresses, but suppose you need to add them as host names. The program can resolve IPs and add them as host names if the option **Resolve address to host name** is turned on. There is also another useful option: **Do not add if not resolved**. When this option is enabled, the program skips the IPs of which cannot be resolved to host names.

- **Import hosts from a file**. This option is helpful when you have a list of hosts to be added into the program, and it isn't convenient to add them one-by-one or as an IP range. To use this option, select **Import** in the context menu of the **Hosts** view and follow the instructions available in the Importing and Exporting Hosts chapter.

Pic 1. Adding hosts

Note that the program automatically starts monitoring the added hosts because the **Start monitoring when added** option is enabled by default in the **Add Host** dialog. Disable this option if you don't need to monitor the added hosts immediately.

> If you need to add a list of hosts into the program, the easiest way to do so is to import them. Create a text file with the *.csv* extension and specify the host names or IPs in this file, where every line contains one host. Then select the **Import** option in the context menu of the **Hosts** view and follow the steps of the wizard that appears to import the created file.

Starting and Stopping Monitoring of the Hosts

When you add a host, the program starts monitoring it automatically. If you need to start or stop the hosts monitoring manually, you can do it in the **Hosts** view. To start or stop the monitoring, select the required host and choose the **Start Monitoring** or **Stop Monitoring** options in the context menu. The program also allows you to start/stop the monitoring of multiple hosts with a single click, for which you can select multiple hosts or groups and choose the corresponding context menu options.

14

The monitoring state is preserved even if you restart the computer running Ping Monitor server. The server works as a Windows service, so it runs on when you start the computer and can continue monitoring automatically. By default, the program preserves the same monitoring state of the hosts, so monitoring continues for the hosts that were monitored before the restart. If required, you can change that and configure the program to start or stop monitoring hosts regardless of their previous state, and set the hosts that should be monitored after the program restart. You can find these advanced options on the **Automation** page of the program preferences.

Deleting Hosts

To delete a host, you need to select it in the **Hosts** view and choose the **Delete** option in the context menu. It is possible to delete one or multiple hosts at once. Note that when you delete a host, all its collected statistics is deleted as well, and it isn't possible to restore it.

If the host deletion option is disabled, it means that it isn't possible to delete the host because it is currently being monitored. You need to stop monitoring the host to be able to delete it.

Configuring Host Settings

An addition to the name or IP address, every host can have various settings that allow customizing its monitoring options, notifications, performance estimation and other aspects. You can configure these settings when you add a host, or change them later by editing the host. On the left of the host configuring dialog, you can find the navigator, and on the right, you can apply the required changes `Pic 2`.

Pic 2. Host settings

The Professional and Enterprise editions of the program allow overriding the common settings used for all hosts and specifying individual settings for a selected host. For example, by default, all hosts use the monitoring settings specified on the **Monitor Settings** page of the program preferences, but you can override them for some hosts, and use custom ping intervals and check attempts.

> By specifying individual settings for hosts and groups, you can specify different e-mail notification recipients for different hosts and groups, so the program will send e-mails to the relevant recipients only.

Organizing Hosts in Groups

To organize hosts in the program, you can create groups and add the hosts into these groups. Why do you need to add hosts into groups? There are a few examples to consider:

- Using a group, you can start and stop monitoring all hosts in a group with a single click. If you have several different types of hosts that should be monitored differently, you can create several groups and add your hosts to those groups, so you can start and stop monitoring those groups independently.

- You can override the default monitoring and notification settings for multiple hosts at once by specifying custom settings for a group.

- When creating a report, you can configure it to include statistics for all the hosts in a group. Then you can update the hosts in the group, and the report will be updated automatically to provide statistics for the actual list of hosts in the group.

- For a group, you can see the total number of hosts with different state and quality characteristics.

To add hosts into a group, you need to create the group in the **Hosts** view and specify the hosts to be added into it.

Avoiding False Positive Outages Detection Using the Gateway Option

Let's analyze a typical situation: suppose you monitor a remote host located in the Internet, and pings to that host start failing, so the program reports an outage. An outage means that there is no connection between the computer where the Ping Monitor server is installed and the monitored host. Usually, there are two possible reasons for this problem. The first reason: the monitored host is down, so it isn't available for you and for other users. The second reason: you have lost the Internet connection, so the host isn't available only to you, but it is available to other users. By using a gateway in the program, you can distinguish between these cases.

In the program preferences, you can specify the gateway IP address to check and confirm the ping results. So, how does a gateway work in monitoring? If a ping to the host passes, the gateway check is skipped; but if the ping fails, the program pings the specified gateway. If the gateway ping passes, it means the problem lies with the monitored host, and the host ping is considered as failed. After the configured number of **Down check attempts**, the host state changes to Down if all the pings have failed. However, if the gateway ping fails together with the host ping, it means this isn't a host failure and a host outage isn't reported.

You can configure a common gateway to be used for all the hosts on the **Gateway Options** page of the program preferences. If required, you can override the common settings and specify an individual gateway in the host settings.

> What host can be used as a gateway? From the technical point of view, you can use any host with a static IP address, because the program allows using an IP address only as the gateway. It makes sense to specify an always-on host located on the route between the monitoring server and the monitored host. Note that you can specify multiple IPs as gateways, if required.

Program Navigation

The program allows you to work with the different types of data and perform the different operations. For example, you can manage hosts monitored by the program, review monitoring results, generate reports, etc. These operations can be performed in the different views described below.

Hosts Management

To start monitoring hosts you need to add them into the program. You can do it in the **Hosts** view that is displayed by default in the left side of the main screen.

The **Hosts** view allows adding and removing hosts to the program, exporting/importing hosts and configuring hosts settings. This view allows you to organize hosts into groups to create hosts hierarchy and for managing multiple hosts as a single entity.

In the **Hosts** view to can start and stop monitoring of the hosts and see hosts, which are monitored currently. Note that the view doesn't provide any information about host state, statistics or other results of monitoring. This information is provided by other views, described below. The **Hosts** view is used for managing hosts and activating their monitoring.

Working with the Monitoring Information

All hosts monitoring information collected by the program is represented in the document interface, displayed by default at the center of the main screen. A document contains all monitoring results and allows you to navigate through the monitoring data quickly and easily. When you open the program at the first time, you can see a default document, which displays the monitoring information for all hosts. If required, you can open additional documents to display monitoring results for selected hosts or to tune data representation within the document.

In the document you can navigate through the monitoring information using the navigation panel, located at the left side of the document `Pic 1`. By default the program shows **Overview**, that displays charts representing the current state of monitoring. You can click the buttons on the navigation panel to open the **Statistics Summary**, **Alerts Summary**, **State Summary** and **Quality Summary** pages.
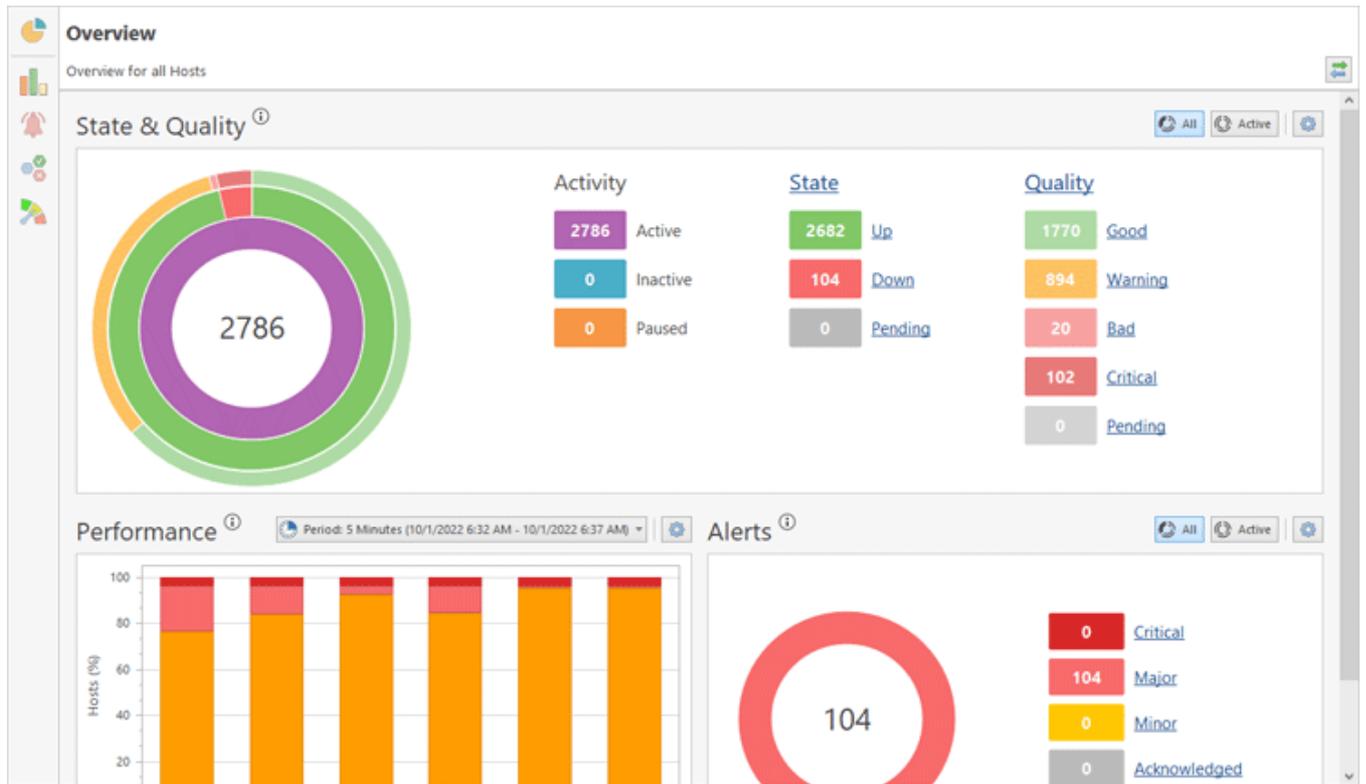
Pic 1. Navigation panel

You can use the navigation panel to navigate through specific characteristics of the monitoring data. For example, the **Alerts Summary** page displays current alerts and the **Statistics Summary** page displays states of hosts. The Overview page and the summary pages with statistics, alerts, state and quality, display information for all hosts on a single screen Pic 2.

Pic 2. Statistics summary view for all hosts

If you need to see detailed information about a specific host, you can click it in on a summary page. It works as a drill-down from a list of hosts to a selected host. For example, if you click on a host in **Statistics Summary**, you will navigate to the **Statistics** page of the clicked host. It displays all statistics collected for the host `Pic 3`.
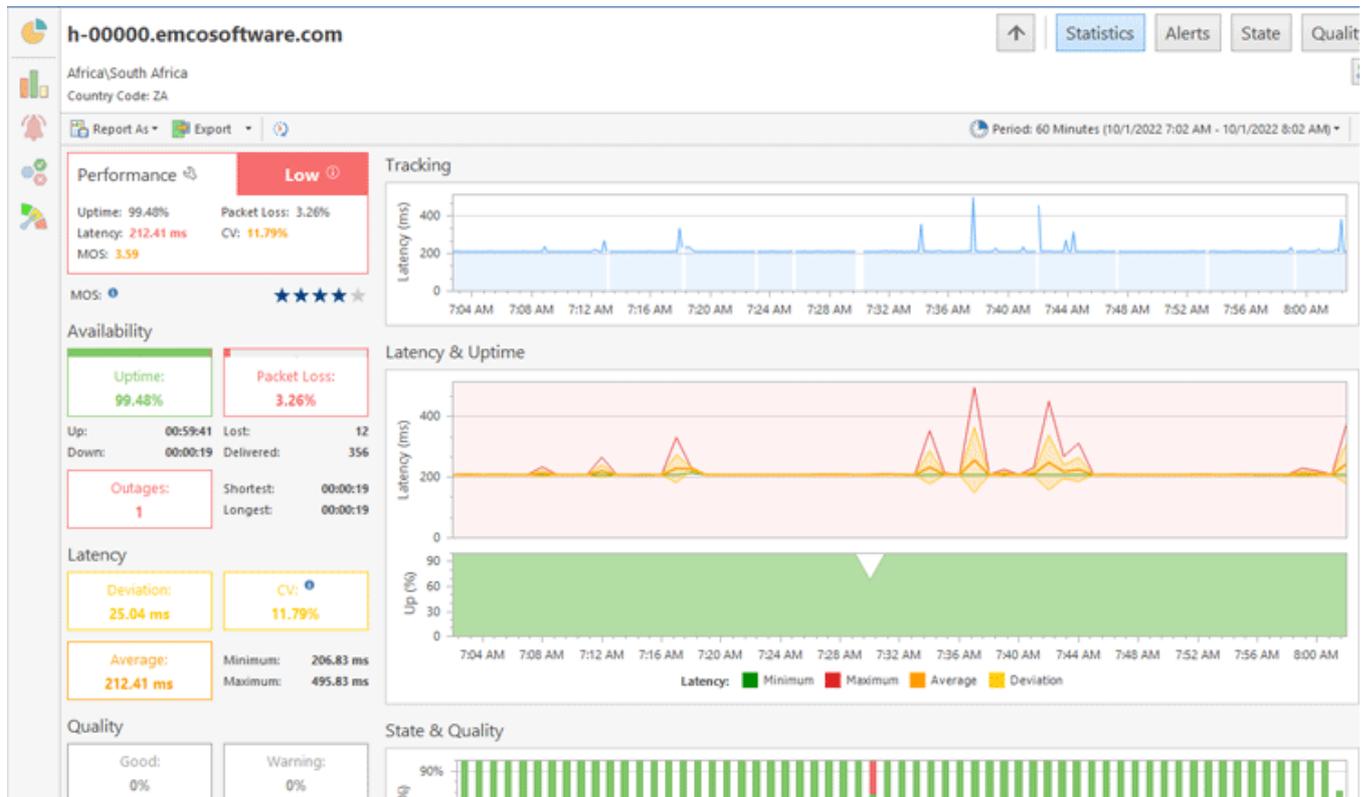
Pic 3. Host statistics

When you are on the host level, you can review all other information, available for the host. Use the navigation bar, located on the top right corner. It allows you to switch to **Statistics**, **Alerts**, **State** and **Quality** pages of the host. You can also use the **Up** button to navigate to the upper level `Pic 4`. On the left side of the navigation bar you can see a host name or a name of the current page, so you can always know your current location.

Pic 4. Navigation bar

You can use either the navigation panel or navigation bar to navigate through the hosts, but the navigation panel buttons allow you to open summary pages displaying information for all hosts with a single click. Using the navigation bar you can walk through hosts hierarchy and navigate through different pages of the host.

As mentioned above, the program allows you to work with multiple documents. For example, you can open documents with different hosts. To create a new document click on the **Document** button in the **New** group of the **Home** menu on Ribbon. In this case the program creates a new document with all hosts. To create a document with specific hosts select the hosts in the **Hosts** view, then right-click and choose **Show Overview In** and then **New Document**. You can change a list of hosts displayed in the view by enabling the **Link with Selection** option in the document and selecting hosts in the **Hosts** view.

Documents are displayed as tabs, so you can switch between them quickly. You can right-click a document tab to pin, rename or duplicate it. You can also undock a document by dragging its title and dropping to another location on the screen to reorganize visual layout of the program.

Managing Reports

You can configure and run reports using the **Reports** view. To open it, click the **Reports** tab, located by default at the left bottom corner of the main screen. The **Reports** view displays available reports, you can create a new report or run a report in this view.

## Access Control, Log and Operations Management

You can configure users, which can use the program, in the **Access Control** view. In the **Log** view you can see logging events generated by the program. The **Operations** view displays a list of running operations. All these views are displayed in the corresponding tabs that are located at the bottom of the main screen.

Monitoring Host State

Ping Monitor is designed to continuously monitor host states and notify you when the host state changes. As explained in the How the Program Works chapter, the program uses ICMP pings to monitor hosts and detects the host states as Up or Down. The Up state means that the monitored host is reachable and it replies to ping requests. The Down state means that the host is unreachable and it doesn't reply to ping requests. There is also the Pending state, which is reported when the host state detection is in progress and the state isn't detected as Up or Down yet.

Using the Overview and State Summary Pages

When the monitoring is started, you can find the general state of the monitoring system on the **Overview** page ⬚ Pic 1 ⬚. The groups of circles on the chart correspond to the groups of numbers displayed on the right. The first group shows hosts monitoring activity, the number of hosts that are Active (i.e. currently monitored), Inactive (i.e. currently not monitored) and Paused. The second group shows the number of monitored hosts that are Up or Down now. The numbers located on the right of the view are clickable, so you can navigate to the hosts with the selected characteristics.
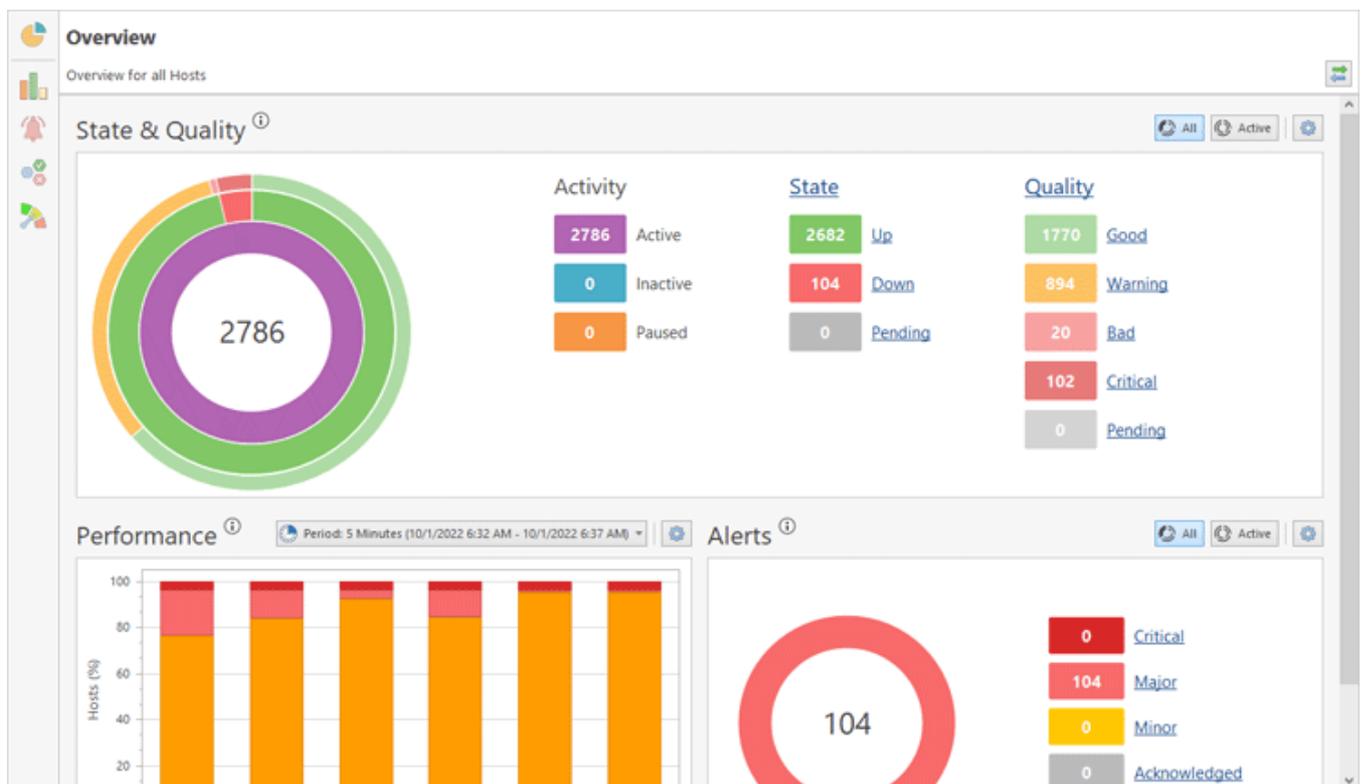
Pic 1. Hosts Summary

If you need to review the host states, you can open the **State Monitor** page by clicking the corresponding button on the navigation panel, located on the left side of the document. This page is designed for control rooms displays the state of all the hosts on a single screen and can use the sorting and filtering features to display the required hosts only. The **State Summary** page supports different modes of data representation.

Hosts can be displayed as tiles where the host state is indicated in different colors: green if the host is Up and red if the host is Down. You can change the size of the displayed tiles to fit all the entries into a single screen `Pic 2`.

Pic 2. State Summary displaying hosts as tiles

> 💡 If you select a small size for the tiles on **State Summary**, the host names aren't displayed so that a maximum number of entries could fit the screen. To see the name and other information, hover the mouse pointer over the box for the program to show the host data on the tooltip.

Alternatively it is possible to display hosts and their states as a table `Pic 3`.

Pic 3. The State Monitor view displaying hosts

To switch to the table presentation you need to click the **Table** button on the toolbar located above the displayed data.

Sorting, Grouping and Filtering Hosts

If you monitor hundreds or thousands of hosts, **State Summary** shows too many entries. How do you organize them? There are several options available, and you can find the corresponding controls on the toolbar of **State Summary**.

- **Sorting**. You can sort the displayed hosts by host name or by time. You may notice that for every host you can see the time when the current host state was detected. When sorting by time, on the top of the screen you can see the hosts states of which have recently been changed.

- **Grouping**. If you enable the **Group by Severity** option, the hosts in the Down state are displayed on the top of the screen.

- **Filtering**. Use **Filter Editor** to select the hosts that should be displayed. For example, you may choose to display only the hosts in the Down state.

Displaying Host Groups

You may notice that by default **State Summary** shows only hosts even if you organized hosts into groups. To see the groups, you may click on the **Groups** button available on the toolbar. As a result, only groups will be displayed, and you can see how many hosts in every group are Up, Down and Pending Pic 4 . If you click on a group, **State Summary** shows all the hosts that belong to this group. You can also click on the numbers that represent the quantity of hosts in different states to drill-down to those hosts.
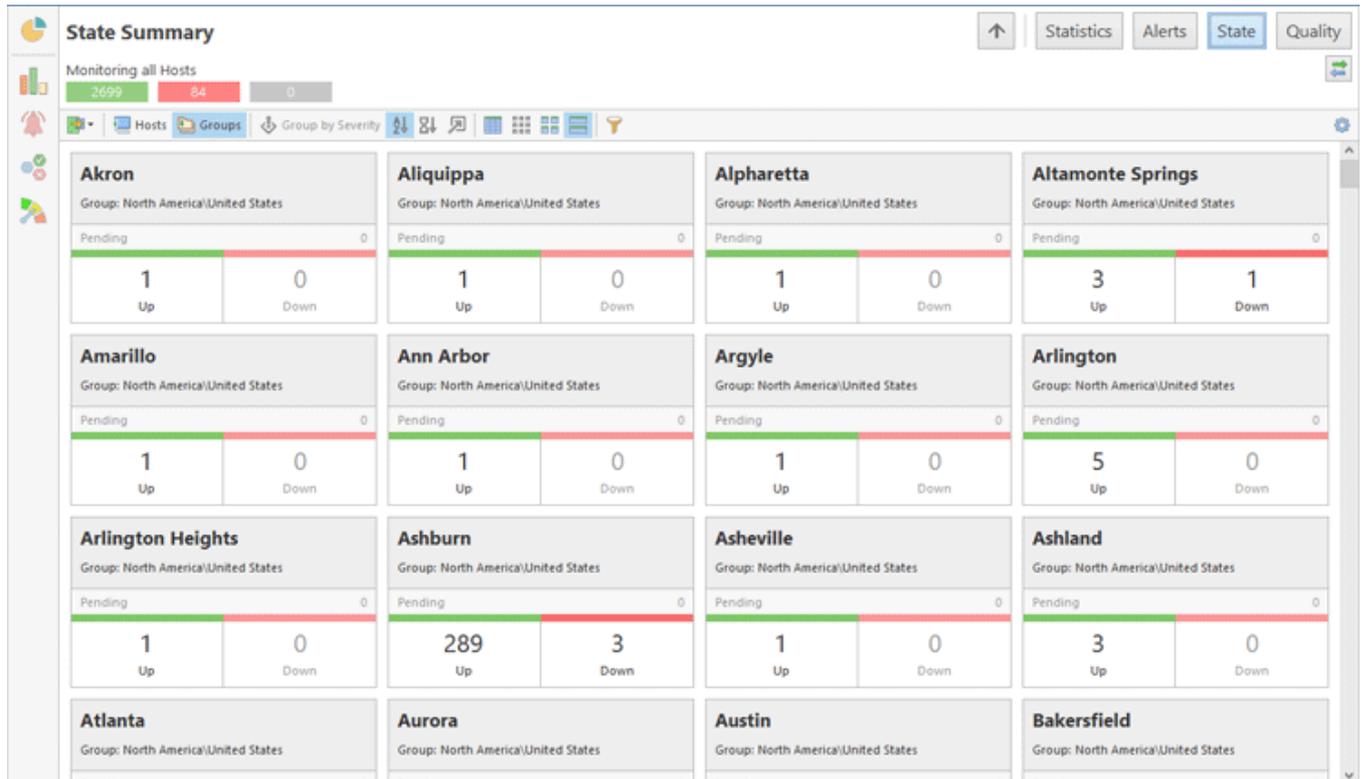
Pic 4. The State Monitor view displaying groups

> The hosts that don't belong to any group are displayed in **State Summary** in the special virtual group called *Individual Hosts*.

Host State Details

The **State Summary** page displays state information for multiple hosts. If you need to see details for a specific host, you can click the host to drill-down. As a result you navigate to the host and can review a real-time pings chart, which shows the result of the latest pings. You can use it to see whether the latest pings have passed of failed. Besides, on the same chart you can see how the host state is changing depending on the ping results. On the host you can see also the statistics of the last 20 pings and host state intervals for the last hour `Pic 5`.
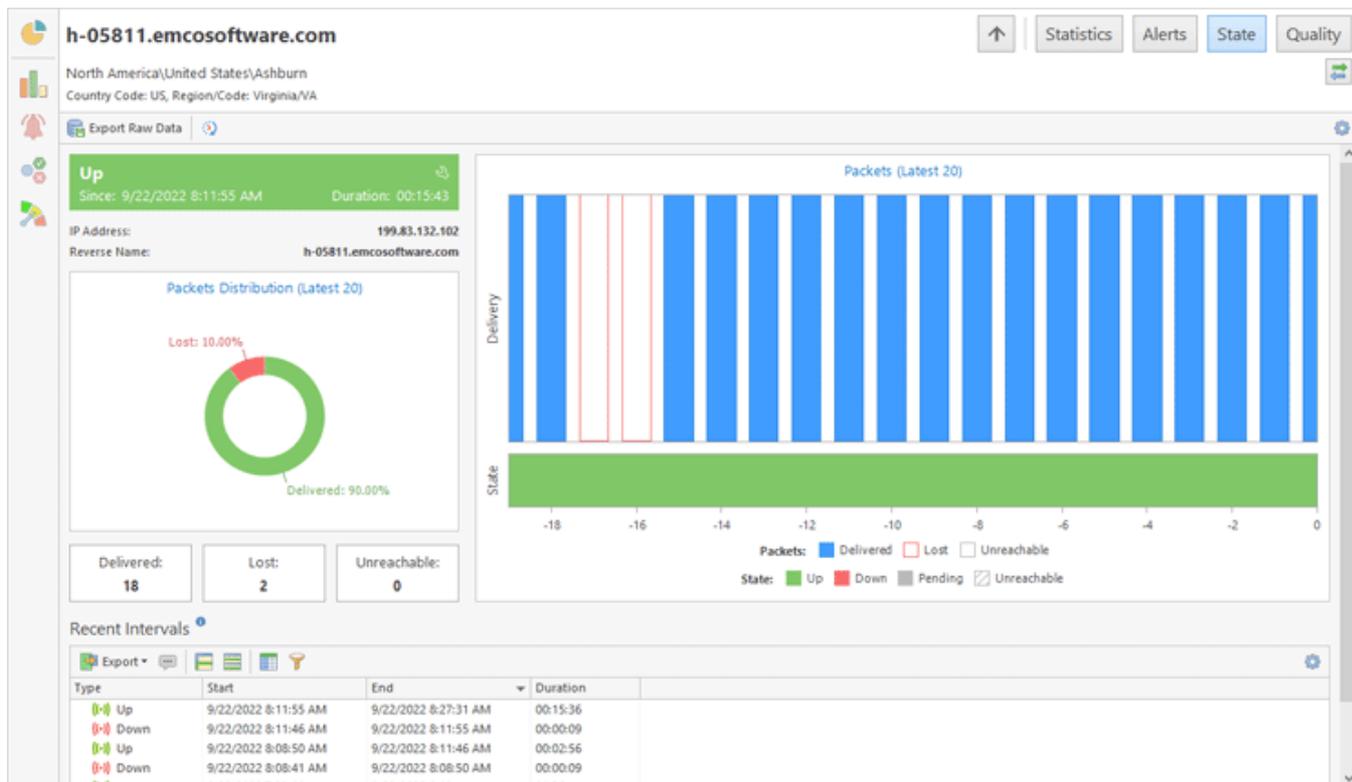
Pic 5. Host state details

To go back and see all the hosts again, click the **Up** button located on the navigation bar in the top right corner.

Best Practices in Host State Monitoring

You can organize hosts monitoring using different approaches and choose the right one depending on your needs. For example, you can rely on alerts and notifications, so when the monitored host goes Down or Up, you are notified about the state change. This approach requires that you configure notifications, and once this is done, you don't need to run the GUI client. All information required to troubleshoot the problem is delivered in notification messages. You can learn how to configure notifications in the Managing Notifications chapter.

If you plan to use the program in a control room to monitor hosts states, you may expand the **State Summary** page to the whole screen and monitor host state changes in real-time Pic 6. In this case, you may configure a filter to reduce the number of displayed hosts and show only the hosts that require your attention, for example the hosts that are Down.
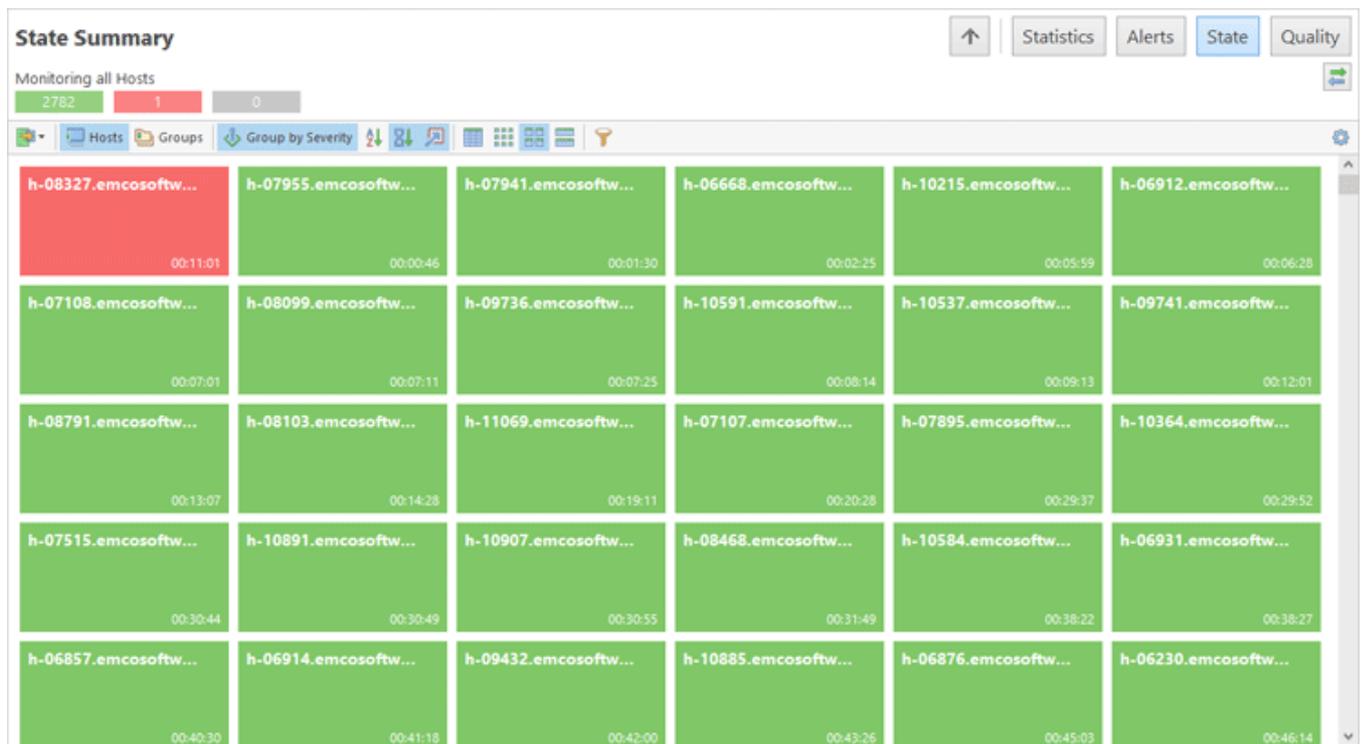
Pic 6. State Monitor displayed in a control room

> 💡 The user interface of the GUI client is customizable, so you may organize it as you need. You can undock the document with hosts statistics, drag it to a dedicated monitor, press F11 to hide the window title and occupy all the available space with it. Refer to the Main features of UI Elements chapter to learn how to reorganize UI elements.

Monitoring Connection Quality

The host state monitoring represented in the previous chapter is one of the main features of the program because it allows you to detect changes in the host state. It is very important to know when the monitored host goes Down, and when the host is Up, but it is also important to estimate its connection quality. Monitoring of the quality of the connection allows you to estimate its current, real-time characteristics and qualify it as Good, Warning, Bad or Critical. Connection quality monitoring allows you to quickly identify potential network problems and resolve them before they are escalated.

How Connection Quality is Detected

The program uses ping results to calculate the connection quality metrics of the monitored host. The connection quality is a real-time value detected at the current moment, so the program uses the latest ping results to calculate the quality metrics. By default, the program uses the packet loss and the latency to detect the connection quality, but it is possible to use the jitter metric as well. The quality metrics are configured on the **Connection Quality** page of the program preferences, where you can tune the settings used Pic 1 .
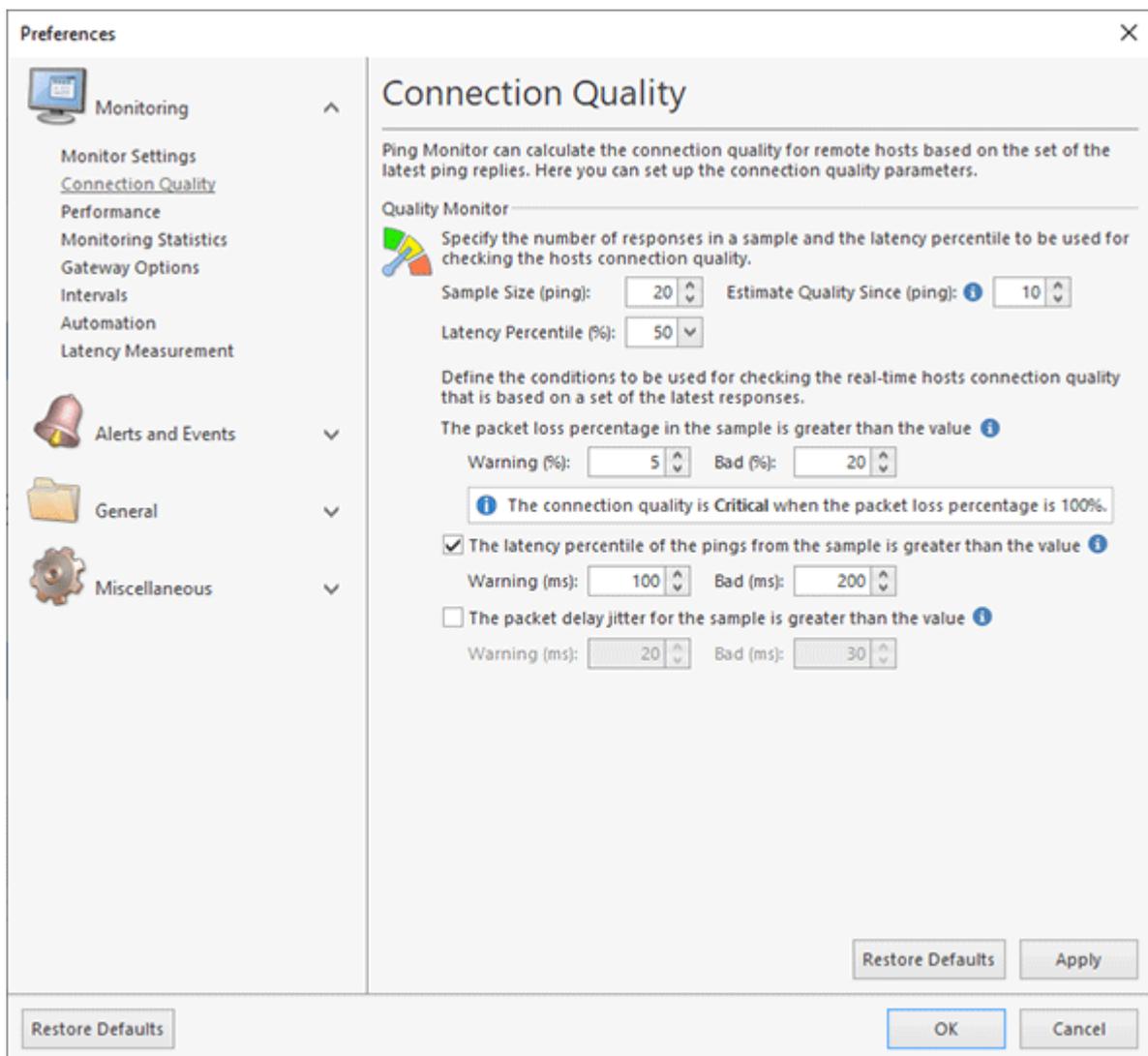
Pic 1. Connection Quality settings

By default, to calculate the packet loss, latency and jitter for a host, the program uses the last 20 ping results. To detect the connection quality, the program uses both the packet loss and the latency. With the default settings, the quality is reported as Good if the packet loss is below 5% and the latency percentile (50%-ile) is below 100 ms. The Warning or Bad quality is reported if any of the metrics exceeds the specified thresholds. For example, the Warning quality is reported if the packet loss for the monitored host is 10%. The Critical quality is reported when the packet loss is 100%, it means that the host doesn't reply to pings, so there is no connection between the monitoring server and the monitored host.

> **i** By default, the common settings configured in the program preferences are used to detect the quality of all the hosts. It is possible to override the common settings and specify individual settings for hosts and groups.

Using Quality Summary to Track the Quality of Hosts and Groups

After the hosts have been monitored, you can see the quality statistics displayed in the **Overview** view, where you can see the number of hosts with a Good, Warning, Bad and Critical quality. By clicking on the displayed numbers, you can navigate to the hosts with the selected characteristics.

To see the quality values of all the hosts, you can switch to **Quality Summary** by clicking the corresponding button on the navigation panel.

By default hosts are displayed as tiles. This representation is designed for control rooms and can show the connection quality of all the hosts on a single screen. The connection quality is represented in different colors, and the key quality metrics are displayed for every host. This view allows you to identify, for example, the hosts with a Bad quality and see the metrics used to define the quality as Bad `Pic 2`.
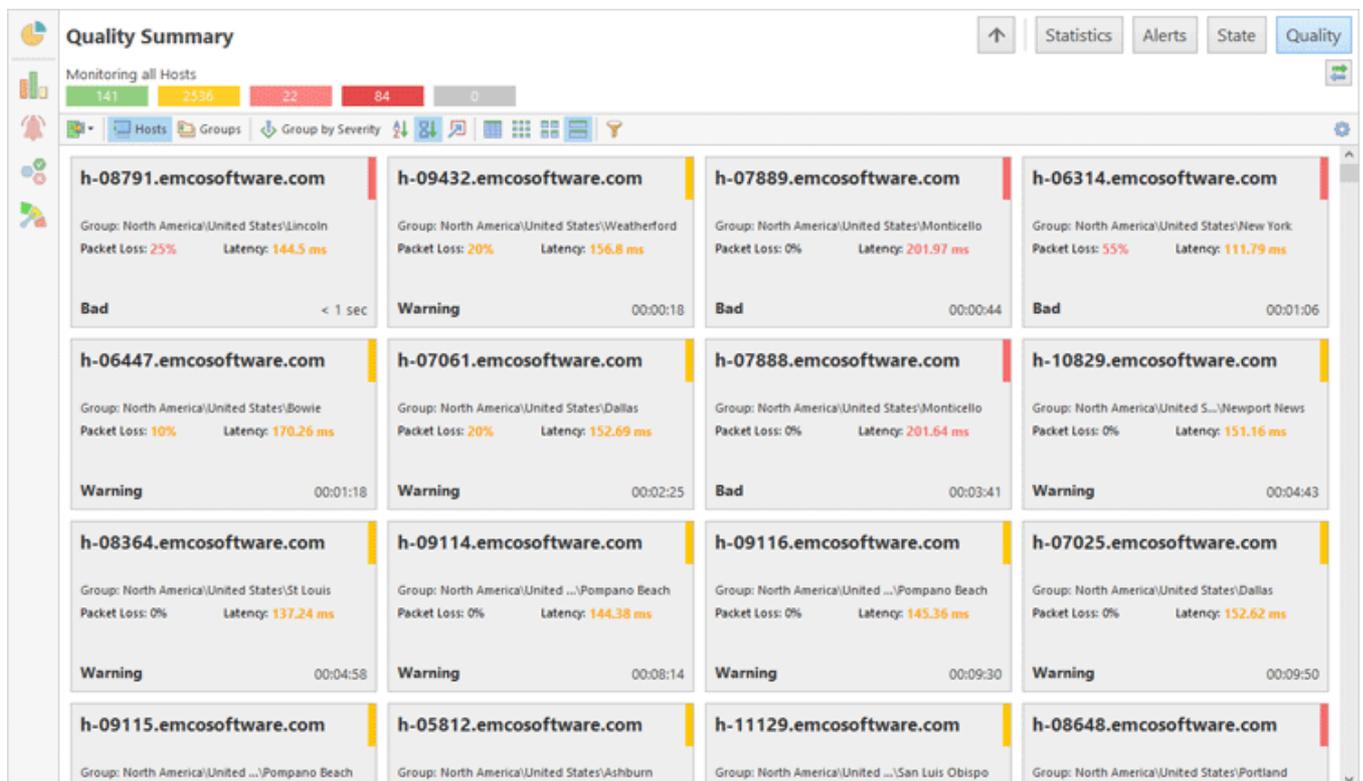
Pic 2. The Quality Summary displaying hosts as tiles

Alternatively you can display hosts and their quality as a table **Pic 3**. Click the **Table** button located on the toolbar above the displayed data to switch to the table presentation.

Pic 3. Quality Summary displayed as a table

The data visualization in **Quality Summary** is similar to the data visualization in **State Summary**, so you can use the same approaches to managing data. In particular, you can display hosts and groups in the view and use data sorting, grouping and filtering features, which are explained in the Monitoring Host State chapter.

In the **Quality Summary** page you can click a host to drill-down and see quality metrics for the host. The latest ping results used to calculate the quality metrics are displayed in a chart together with the latency percentile value. On the same screen, you can also see the packets distribution chart and the calculated metrics of the packet loss, latency and jitter.
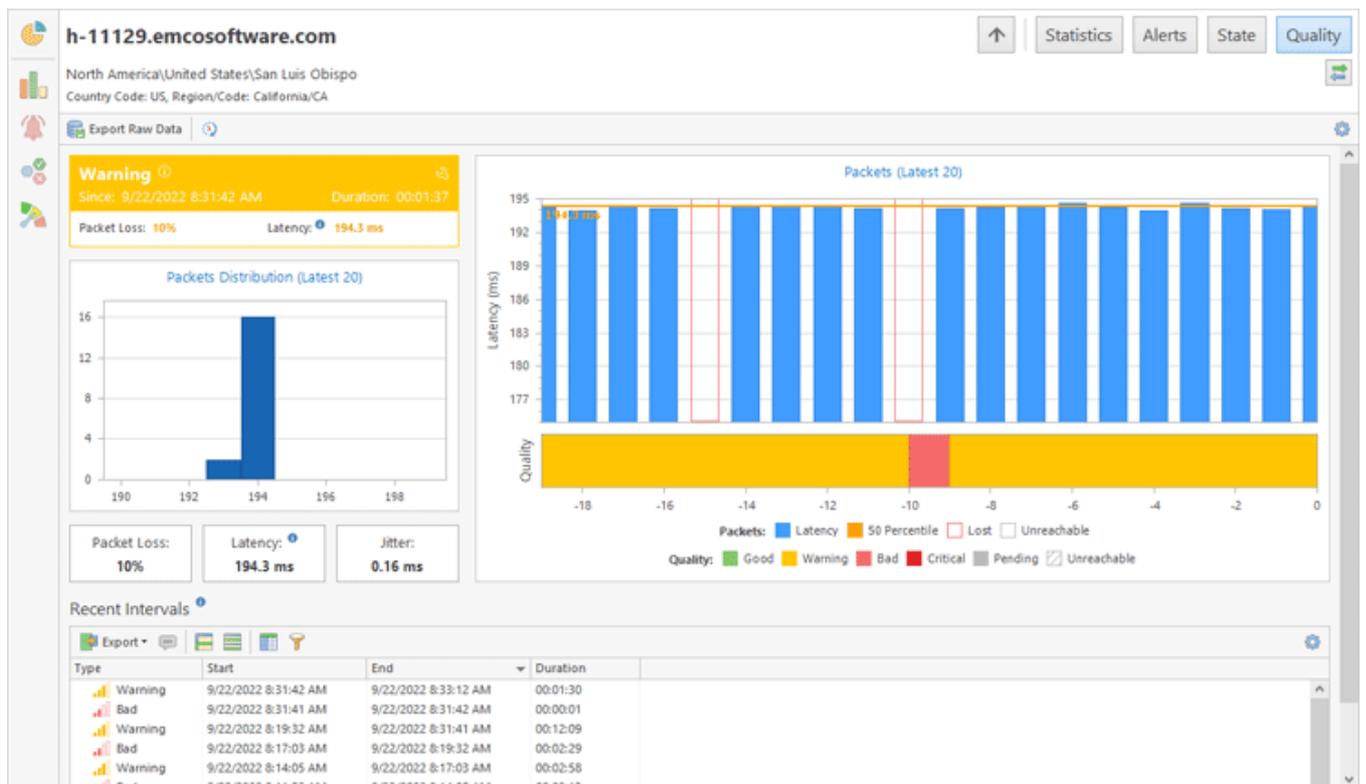
Pic 4. Quality metrics of a host

By navigating to host details, you can see the ping results for the host in real-time and track the quality changes.

Best Practices of Connection Quality Monitoring

To monitor the connection quality, you can use the same approaches as explained in the Monitoring Host State chapter. If you plan to use the program in a control room, you can open **Quality Summary** for a visual tracking of quality changes. For example, you can configure a filter to display hosts with a Critical, Bad and Warning quality only, so if any host with those characteristics appears on the screen, you will be able to take the required actions to resolve the problem.

Another approach is based on using notifications sent by the program when the quality of the connection to a host changes. For example, you can create an alert that will send you notifications when connection quality reaches a specified value. In this case, you don't need to open the GUI client because the program will notify you about all problems itself. The notification messages contain detailed information about the host and its metrics.

By default, connection quality notifications are turned off in the program preferences, so you need to enable them. This topic is described in the Managing Notifications chapter.

How Alerts Work

Alerts help you to detect problems with monitored hosts quickly and easily. An alert is real-time entity that is created by the program when host monitoring characteristics don't satisfy specified criteria. You can see the actual list of alerts in the program – it shows alerts for hosts that have monitoring problems at the current moment. The program can also notify you by sending e-mail messages, playing sounds and showing Windows Tray balloons when alerts are started and ended.

The program has two preconfigured alert types. It creates alerts when a host is down or when a host connection quality is unsatisfactory, i.e. when the quality is Bad or Critical. To review the actual state of monitoring system you can open **Overview** on the right side of the main screen. The **Alerts** section shows you how many alerts are in the monitoring system at the current moment. You can open the **Alerts Summary** page by clicking the corresponding button on the navigation panel to see the list of alerts for all hosts `Pic 1`.

Pic 1. A list of alerts

The alerts list shows the name of alert, host name for which this alert is reported, alert severity, duration of the alert and alert state. Each alert displayed in the list represents a problem with the host, because host monitoring parameters don't satisfy criteria configured for the alert. Alerts can be configured on the **Alerts and Notification** page of the preferences dialog. You can configure as many alerts as you need and each alert has its own condition. If this condition is satisfied, a problem is detected and an alert is reported by the program.

You can use simple or complex logical conditions for alerts. For example, one of the preconfigured alerts is reported when a host state is Down. You can create more complicated conditions and use any real-time characteristics detected for a host. For example, you can report an alert when packet loss or latency is over a specific value. You can combine criteria using logical operators to create complex conditions Pic 2 .
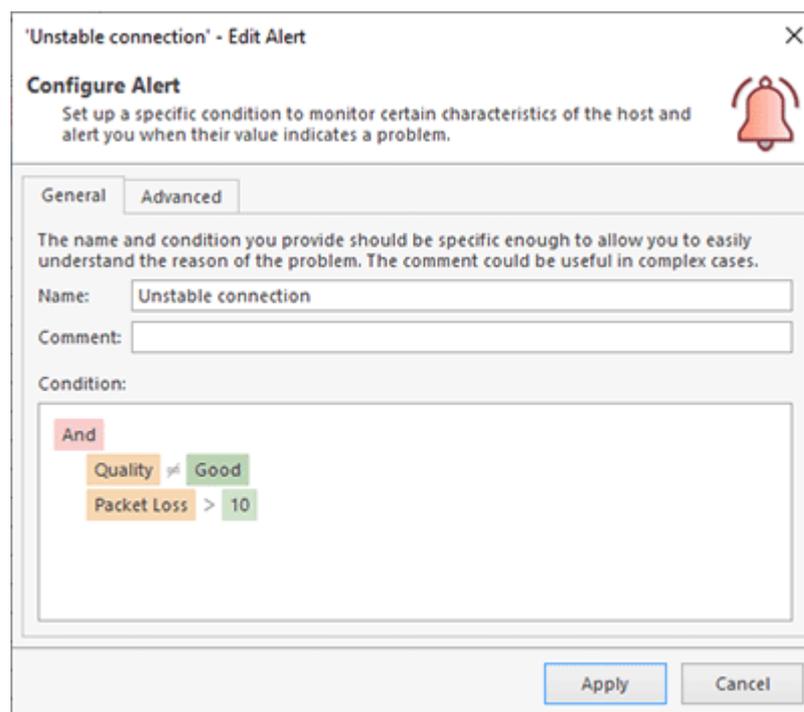
Pic 2. Alert configuration

The program allows you to create multiple alerts, if you need to check different monitoring characteristics. In this case multiple alerts can be reported for the same host. Set different severity for alerts to be able to filter and sort alerts. You can navigate to a host level by clicking the host name on the Alerts Summary page. In this case you can see alerts reported for the selected hosts only.

Alerts can be used for indication of the problems. If there are alerts reported, it means that there are some problems with the hosts for which the alerts are reported. You can acknowledge alerts when you work on a problem. To acknowledge an alert right-click it and select Acknowledge and a time period during with an alert will be acknowledged. Acknowledged alerts are displayed with the corresponding status in the list, so you can review active and acknowledged alerts separately. If an acknowledgment period is passed, but the alert condition is still satisfied, the program will change the alert state to active.

The program can automatically notify you by e-mail, sound or System Tray balloons when an alert is started and ended if notifications are configured for the alert in the program preferences. You can learn how notifications work in the **Managing Notifications** chapter.

Analyzing Hosts Statistics

The program allows you to access the detailed monitoring statistics for any host. While the host state and the connection quality are real-time characteristics, the statistics allows you to analyze the host metrics and performance during any historical period.

> When working with historical data, it's important to remember that the result depends on the selected period. In other words, statistics is always reported for a particular period. For example, the uptime metrics for yesterday and for the previous week will be different, so you need to select the required period first to work with statistical data.

Statistical data for all hosts collected by the program is available in the **Statistics Summary** page `Pic 1`. Click the corresponding button on the navigation panel to open **Statistics Summary**. First, you need to select the required period in the corresponding combo-box located on the view's toolbar.

Pic 1. Statistics for yesterday displayed for all hosts

The **Statistics Summary** page shows general data for all the hosts during a selected period, so that you can see what the uptime, the packet loss, the latency, the number of outages and other values are for every monitored host. The host statistics is displayed as a table, so you can sort and filter the displayed data, reorganize the displayed columns and use other standard features available for any grid view.

Reviewing Host Statistics

The **Statistics Summary** page shows data for all the hosts. To see the statistics for a particular host, you can click on its name to drill-down to the selected host `Pic 2`. The host statistics is displayed for a specific period selected in the header of the view.
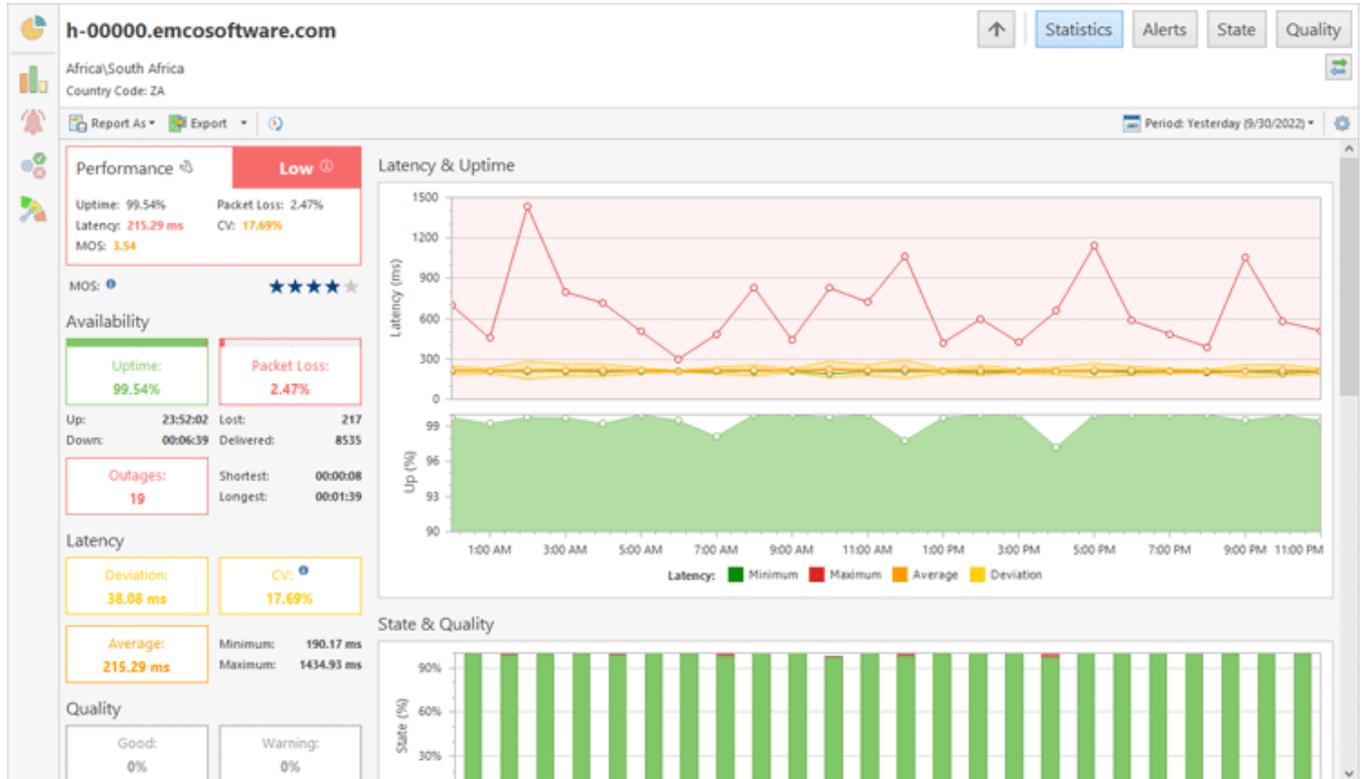
Pic 2. Host statistics for yesterday

The host statistics shows how various metrics change over time. The program displays aggregated information on charts, so that you can track the latency, uptime, state and quality changes. The program reports the number of detected outages and the time intervals during which the host had different state and quality characteristics.

Estimating Historical Host Performance

The host state and quality are real-time characteristics that constantly change. For example, the host quality may change many times during a day, so if we need to estimate the host performance for the entire day, we cannot use quality. For estimating the host performance during a historical period, we can use other metrics such as the uptime percentage, packet loss percentage, average latency, latency deviation, latency coefficient of variation (CV) and mean opinion score (MOS) calculated for the entire period.

To estimate the host performance, the program calculates metrics for the selected period and compares the metrics with the defined thresholds. For example, using the default settings, the host performance is considered as High if the uptime exceeds 99%, Medium if it is over 95% or Low if it is below 95%. Other metrics have different thresholds, for example, the host performance is considered as High if the packet loss is below 5%, Medium if it's below 20% and Low if it exceeds 20%. The program analyzes the metrics and sets the performance rank for the host as the lowest rank of all the metrics. The overall host performance during the selected time interval is displayed in **Statistics**, and the metrics that are considered Medium and Low, are highlighted, so that you can easily understand what the actual performance rank set for the host is based on.

If required, you can tune the thresholds used to estimate the host performance on the **Performance** page of the program preferences. Those settings are applied to all the hosts, but it is possible to override the common settings and specify custom settings for a host or group Pic 3.

Pic 3. Tuning performance thresholds for a host

> 💡 Host performance can be considered as the aggregate of all the metrics during a specific period. For example, when analyzing a weekly host performance, you may look into the daily host performance and see how it changed over time. It allows you to find the days when the performance was Low and check the detailed statistics for those days to identify the reason of the problem.

Reviewing Ping Data on the Timeline

The program stores all collected ping data, which allows you to see the latency chart for any host and any period. To open the timeline, click the on the **Timeline** button located on the header of the **Statistics** view displaying a host. The **Timeline** view allows you to choose the time range to be displayed on the chart, using the range selector located at the bottom. At the top, you can see charts showing the ping latency and the host state and quality during the selected period `Pic 4`.
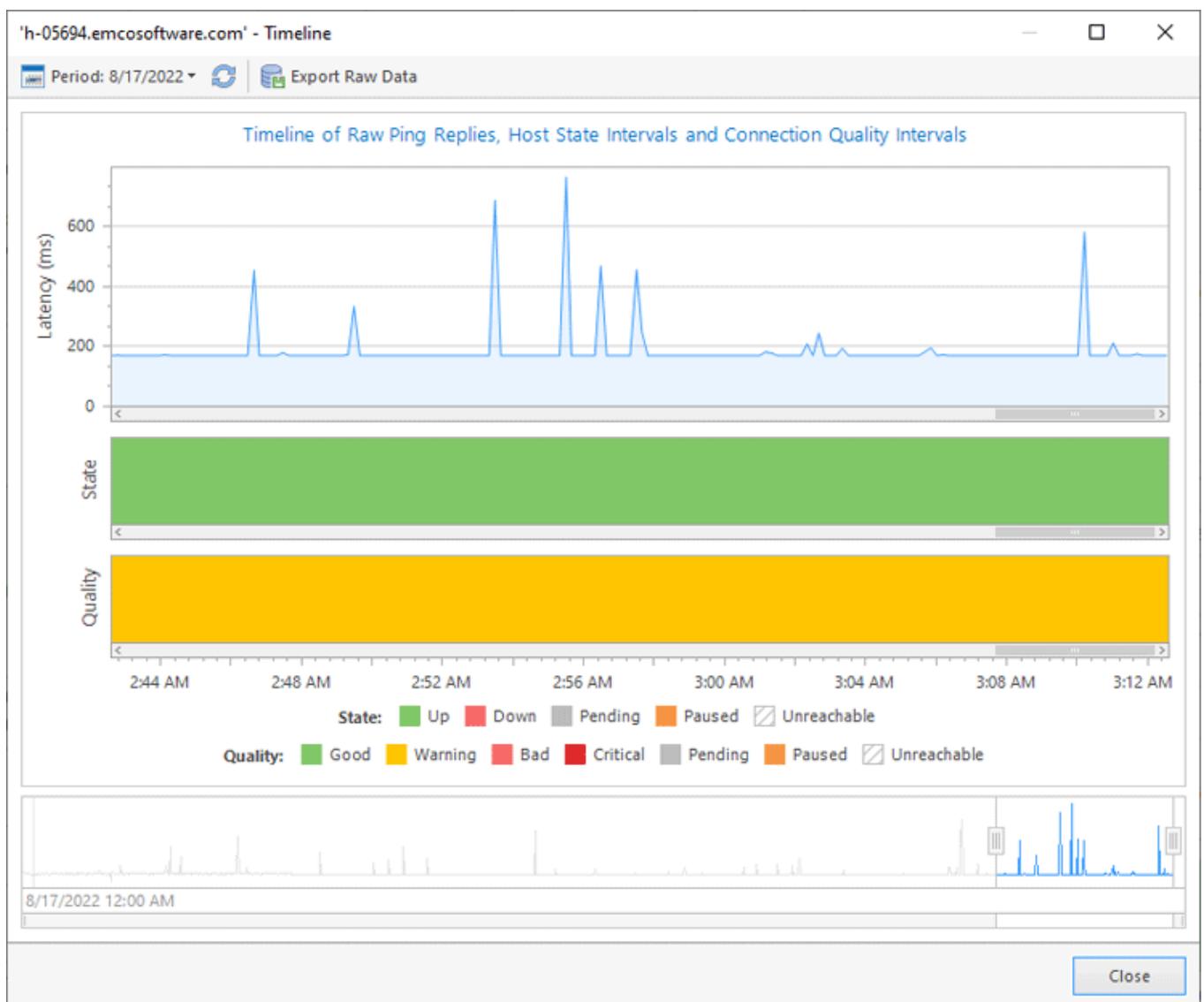
Pic 4. Timeline view

> When reviewing data displayed in the **Statistics** view, you can click on values represented in the charts to open **Timeline** for a specific time range. For example, when reviewing statistics for a day, you can see data aggregated by hours in the **Latency & Uptime** and **State & Quality** charts. You can click on any hour value displayed in the charts to see pings for that hour in the **Timeline** view.

In the **Timeline** view, you can see the results of every ping sent to the monitored host. To see the latency value, read the data displayed in the tooltip that appears when you hover the mouse pointer over the chart. It is possible to export the ping data displayed in the **Timeline** view by clicking on the **Export Raw Data** button. The ping results are exported as a CSV file that can be opened in external programs.

Practical Examples of Using Statistics

How to use statistics to find and analyze problems? For example, we need to analyze the network outages that happened yesterday to find problematic hosts. So how can we use the program in this case?

In this task, we need to analyze data in the historical period and work with statistics that is available in **Statistics Summary**. We need to analyze the data for yesterday, so we should select this period. As a result, we can see the statistics of all the hosts for yesterday displayed as a table. How can we find problematic hosts? There are multiple approaches to this, and we can use one depending on our needs.

For example, we can sort the displayed data by the **Perf** (i.e. performance) column, so the hosts with a Low performance are displayed at the top, and we can easily find problematic hosts. It is helpful, but it isn't sufficient, because hosts with a Low performance can have no outages (some hosts have a high latency, so they show a Low performance, but they work stably and with no outages). So how can we find hosts with outages?

To show the hosts with at least one outage that took place yesterday, we can use a filter. When we press the **Filter Editor** button on the toolbar, the editor appears and we can specify a filter condition `Pic 5`. After the filter is applied, the displayed data change and we can see only hosts with outages.
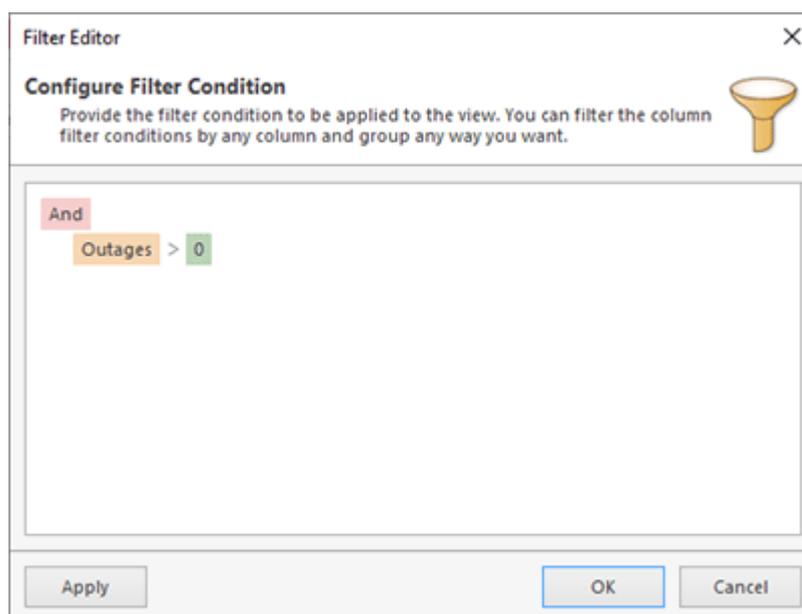
Pic 5. Configuring filter in Statistics

> 💡 If you apply a filter, it is saved until you reset it. The current filter condition is displayed at the bottom of the grid. To reset the filter and display all the hosts, you need to click on the **Close** button located to the left of the filter.

After applying the filter, we can see all the problematic hosts and start to analyze them one by one. The hosts with the maximum number of outages should be analyzed first, so we can sort the displayed data by the **Outages** column and click on the host displayed at the top to open its statistics.

To analyze the host statistics, first we need to know when the outages happened. Therefore, we can scroll down to the **Intervals** table and switch it to display state intervals. It shows a list of host state intervals detected during yesterday, but we need to analyze the Down intervals only, so a corresponding filter should be applied. As a result, we can only see the Down intervals and their start and end time and duration. We can sort the displayed data by duration to display the longest outages at the top of the list `Pic 6`.

Pic 6. List of the host outages that happened yesterday

To get detailed information on the host performance, we can review the **Latency & Uptime** chart to see how the host metrics changed during the day. Note that the latency chart shows the host performance as highlighted backgrounds, so if the host performance was Low during a particular time interval, you can see that it is highlighted with a red background on the chart. You can hover the mouse pointer over the chart to see the latency minimum, maximum, average and deviation displayed for every hour.

The latency, uptime, state and quality charts in **Statistics** show aggregate metrics. In particular, when we check the statistics for yesterday, the displayed data is aggregated by hours. It helps you to identify the hour when the problem happened and drill-down to see detailed information for this hour. For example, the **State & Quality** chart displays hourly quality values, so we can easily find the hour when the quality was Bad. It is possible to click on this chart value for the program to open **Timeline** for the selected hour, so that you can see all the ping results during that hour.

What is State, Quality, Performance and Statistics

In the previous chapters, you could learn how the program detects the host state, the connection quality, and the host performance and how to use different views of the program to assess the required characteristics. In this chapter, you can learn what features of the program you can use in different cases and how to interpret the reported data.

You can use Ping Monitor for the following tasks:

- **Track real-time changes**. Host state and connection quality monitoring deals with the current real-time status of the monitored host.

- **Analyze statistics for a historical period**. Host statistics and host performance deal with historical information for a specific time range.

Tracking the real-time status and detecting its changes are the main features of monitoring systems. Ping Monitor allows you to track the host state and the connection quality. At the same time, Ping Monitor can be used as an analytical tool that collects statistics and allows auditing collected data for any historical period.

> To decide what feature of the program you should use, you need to understand first whether you have to work with real-time or historical data. The host state and quality indicate the real-time status of the monitored host, whereas host statistics and host performance operate with historical data for a specific time range.

Below you can find a brief explanation of the main concepts of the program.

State

The host state is a real-time characteristic of a host used to determine if the host is reachable or not. If the host is Up, it means that it works and replies to ping requests. If the host is Down, it means that the host doesn't reply to ping requests, so it is unreachable. The program monitors the states of all the hosts in real-time and displays the states on the **State Summary** page. The program can send you notifications when the host states change. Learn more about the host states in the Monitoring Host State chapter.

Quality

The connection quality is a real-time characteristic of the host used to estimate the quality of the connection between the monitoring server and the monitored host. When a host is Up, the connection quality allows you to assess how good the connection to the host is, using various real-time metrics. When the host is Up, the quality can be Good, Warning or Bad depending on its metrics. When the host is Down, the quality is Critical, which means the host is unreachable. The host quality is measured based on real-time metrics such as the packet loss percentage, latency percentile and jitter. The program detects real-time changes in the connection quality to send notifications and display the current status on the **Quality Summary** page. Learn more about the connection quality in the Monitoring Connection Quality chapter.

> 💡 Which one do you need to track: the state or the quality? It depends on your goal. If you want to know whether a host is Up or Down, you should monitor the host state. In other cases, it makes sense to monitor the connection quality because that would give you more detailed information and enable you to resolve problems proactively before they are escalated to the next level. For example, you can start resolving the problem when the quality becomes Warning, whereas the monitored host is still reachable.

Statistics

The host statistics is a set of collected ping results and aggregate data for a historical period. Having this information available, the program allows analyzing the host performance during any historical time interval. For example, you can analyze the host statistics during the last week, look into the daily performance of this host day by day and find time intervals during which problems occurred.

Performance

The host performance is a characteristic that allows you to assess how the host worked during the selected historical period. The host performance can be High, Medium, Low and Faulty. The host performance is evaluated using different statistical metrics calculated for the selected period. These metrics are the uptime percentage, packet loss percentage, average latency, latency deviation, CV (latency coefficient of variation) and MOS (mean opinion score). Learn more about the host statistics and performance in the Analyzing Host Statistics chapter.

> 💡 What is the difference between the host quality and the host performance? The host quality is a real-time characteristic calculated using the current ping results. The host performance is a historical characteristic calculated for a selected historical period. Therefore, if you need to assess the real-time status of a host to understand how it works right now, you should use host quality. If you need to estimate the host characteristics for yesterday, for example, you should use the host performance.

Managing Notifications

When an alert is started or ended and when the host state or quality change, the program can notify you accordingly by sending e-mails, executing custom commands/scripts/executables, playing sounds and showing balloons in Windows Tray. You can configure notifications on the **Alerts and Notifications** and **Balloons and Sounds** pages of the program preferences `Pic 1`.
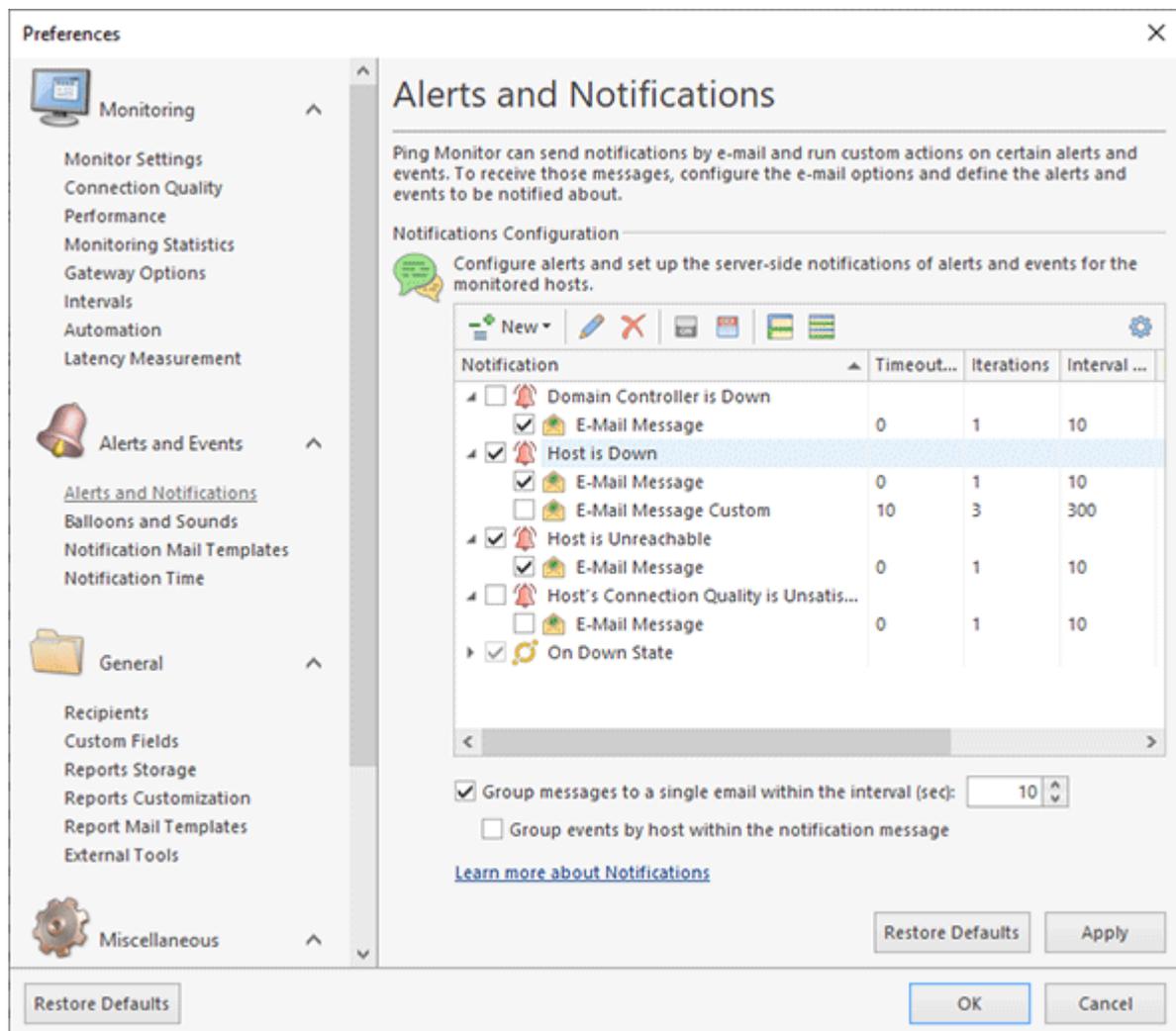
Pic 1. Alerts and Notifications page

There are two types of notifications: server and client notifications. Server notifications are implemented by sending e-mail messages and executing custom actions. The server sends such notifications regardless of the availability of connected GUI clients. Server notifications are managed on the **Alerts and Notifications** page of preferences. Client notifications are implemented by GUI clients; so sounds and Windows Tray notifications are initiated only when there are clients connected. Thus, sounds are played and Windows Tray balloons are displayed on the computers where GUI clients are running. Client notifications are managed on the **Balloons and Sounds** page of preferences.

⚠️ It makes sense to enable Windows Tray notifications and sounds only if you monitor a small number of hosts, otherwise those notifications can be very annoying.

Notifications are triggered subject to different conditions:

- **On Alerts**. These notifications are sent when alerts are started and ended. By default e-mail message notification is enabled for the preconfigured alert that is created when a host goes Down.

- **On Events**. These notifications are sent when a host state or quality are changed. You can configure events on which notifications should be sent.

On the **Alerts and Notifications** page of preferences you can configure when notifications should be sent. To add a notification you need to select an alert and use the context submenu **New** to add an e-mail notification or a custom action. When an e-mail notification is added to an alert you can use checkbox to enable and disable assigned notification. You can also add notifications for specific events, such as On Up State, On Down State and On Critical, Bad, Warning and Good Quality. You can add these notifications from the New submenu of the context menu.

Each notification has configuration parameters. You can change the parameters by editing a notification using the context menu. The default list of recipients used for all notifications is configured on the **Recipients** page of preferences. You can override default preferences and set custom recipients for each notification. The default notification time parameters are configured on the **Notification Time** page of preferences. Notifications can be sent at the configured days of the week and period only. You can configure the program to repeat notifications and delay notifications if required. You can override these settings and specify custom settings for each notification by editing the notification `Pic 2`.

Pic 2. Notification settings

When you enable e-mail notification for an alert you will receive e-mails twice – when an alert is started and when it is ended. You can delay notification by specifying a timeout for notification. In this case the program will send you a notification about created alert after specified timeout. If an alert is ended earlier than the specified timeout, no e-mails are sent.

E-mail notifications of the host state changes are enabled by default, but you need to activate them by specifying SMTP settings on the **E-Mail Options** page of the program preferences. On the **Notification Mail Templates** page of the preferences, you may find templates used for e-mail notifications and change them, if required.

If you use e-mail notifications, you may configure them to group messages into a single e-mail. It allows you to reduce the number of e-mails that the program sends in case of a massive outage of the monitored hosts. In addition, the program allows grouping events by host within a notification message.

If required, you can configure the program to execute custom actions, such as commands, scripts or executables, on the server when the host state or quality change. This may be helpful, for example, for integrating Ping Monitor with other systems. This option is explained in the Integration with Other Programs chapter.

Using Custom Notifications for Hosts/Groups

All notifications configured in the program preferences are common and used for all hosts. For example, e-mail recipients configured on the **Recipients** page of the preferences are used for all hosts.

Now let's assume you need to send e-mails to different addresses for a specific group of hosts. Ping Monitor allows overriding common settings and using individual settings for hosts and groups. You may open a host or a group for editing and specify custom notifications settings and e-mail recipients `Pic 3`.
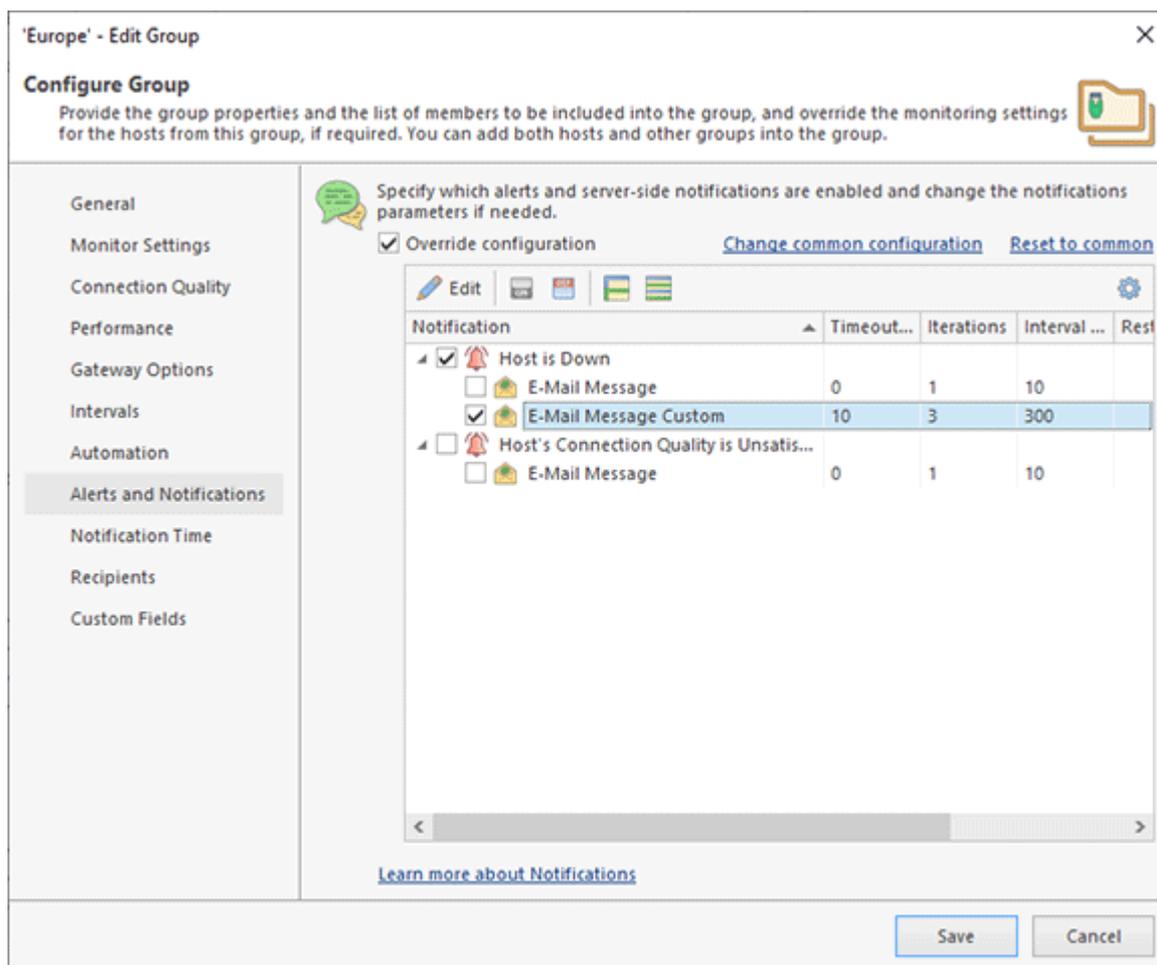
Pic 3. Overriding common notification settings for a group

Using this feature, you may, for example, enable notifications on state change events for all hosts in a specific group, while no notifications of state changes will be sent for other hosts. Or you may specify a list of e-mail recipients for all hosts, override it for a specific group that will use different recipients, and specify still different recipients for a host in the group.

Generating Reports

Ping Monitor includes built-in reporting features, so the program can automatically generate reports for you. Reports can be managed on the **Reports** view, where you can create reports of two types: summary and detailed. What is the difference between those types of reports?

- **Summary report**. This report includes main statistical metrics for multiple hosts. It is represented as a table, with one raw per host. The report includes basic metrics such as the

number of outages, uptime, packet loss, performance, MOS, latency average, deviation and CV. This report is similar to information displayed in the **Statistics** view for all hosts.

- **Detailed report**. This report includes all available statistics for multiple hosts. The report includes detailed statistics for a host such as the latency, uptime, state and quality charts, state and quality intervals and other data. This report is similar to information displayed in the **Statistics** view for a host, but it can include data for multiple hosts.

You can manage reports in the **Reports** view. When creating a new report, you should decide whether it should be a summary or a detailed report, then configure the report settings accordingly **Pic 1**.

Pic 1. Configuring a report

To configure a report, you need to specify the following settings:

- **Generation type and recurrence**. A report can be generated on demand, when you initiate its generation manually, or it can be generated automatically. For automatically generated reports, you need to specify the recurrence settings. For example, reports can be generated daily, weekly or monthly.

- **Members**. You need to configure a list of hosts and groups to be included into the report.

- **Filter**. You may filter hosts based on specified conditions.

- **Output format**. The program can generate reports as PDF and HTML files and send them by e-mail, if required. The program can also upload the generated reports to a specified FTP server.

Reports are designed to include information about multiple hosts. So how do you manage the reported data? You can use a filter based on the entered condition, for instance Pic 2. When you configure a daily report, which is generated automatically every day, you should include all hosts that you need to track into this report. For example, you need to include hosts with downtime to analyze problematic hosts only. The list of those hosts can be different every day depending on the monitoring results, but it will always meet the entered condition and be up-to-date.
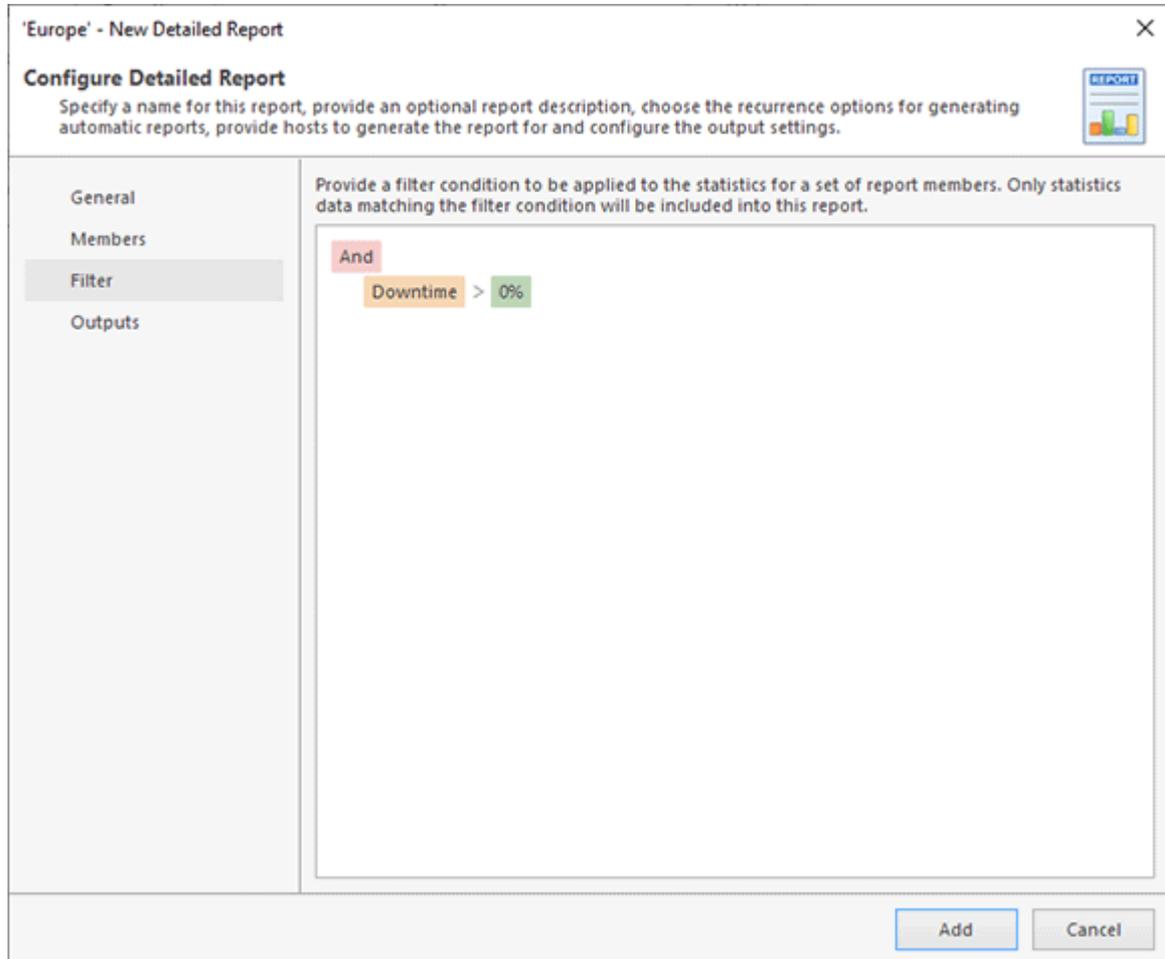
Pic 2. Filter configuration in a report

The reports generated by the program include a preconfigured header and footer. You can customize them and include your own logo and text. This can be configured on the **Reports Customization** page of the program preferences.

Integration with Other Programs

The program includes several features that may help you to integrate it with other systems and programs. For example, you can use Ping Monitor as a tool that registers various events, such as host state and connection quality changes, and integrate Ping Monitor with other systems such as event managers or help desks to notify them about those events. As another example, you can use ping data collected by Ping Monitor and export them for processing into external tools.

Using Custom Actions to Integrate with other Programs

Ping Monitor tracks alerts, the host state and the connection quality to detect their changes, so that the program can notify you of such events. The Managing Notifications chapter provides an overview of the available notification types, including Custom Actions. So, what are Custom Actions and how can you use them?

A Custom Action allows you to run a command, script or executable on the server after a host state or connection quality change. You can configure one or multiple actions for every event on the **Alerts and Notifications** page of the program preferences. You can use Custom Actions to send custom notifications in form of, for example, SMS messages on alerts. Thus, if you have software that can send mobile text messages, you can integrate it with Ping Monitor using Custom Actions. Custom Actions can also be used to integrate the program with third-party event management systems and help desks. Thus, when an alert is created by the program or when the host state or quality change, the program runs the configured Custom Actions that create events and tickets in external systems.

A **Custom Action** should be assigned to an alert or event that will initiate it. On the **Alerts and Notifications** page of the preferences select an alert or event and choose **Custom Action** in the **New** context submenu. The configuration dialog allows you to specify certain actions and commands to be executed. Note that the command will be executed on the computer where Ping Monitor server runs, so the specified script or executable file must be available on the server. You may test the entered command to make sure it works as expected. All other settings are the same as for the other notifications and are explained in the **Managing Notifications** chapter.
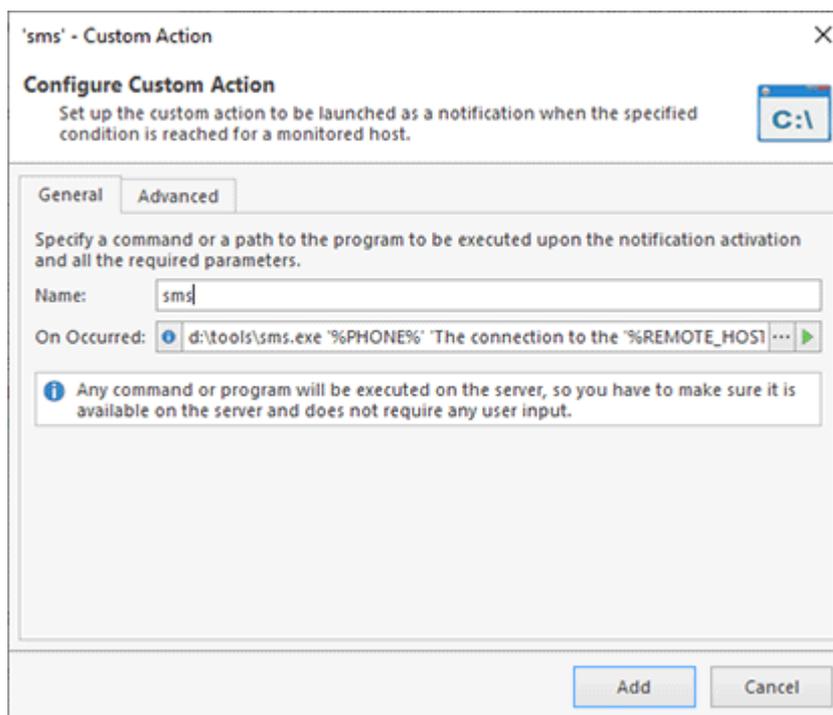
Pic 1. Configuring a Custom Action

> 💡 Custom Actions can be executed on alerts and various events, for example, on host Up or Down and on quality changes. If required, you may configure different scripts or executables to process them. Alternatively, you may use a single script or executable and pass the type of event as a command-line parameter.
>
> Note that a Custom Action configured in the preferences will be executed for all the hosts, but how do you know what host triggered the event? In the command-line of Custom Actions, you can use placeholders. For example, the *"%REMOTE_HOST_ADDRESS%"* placeholder will be replaced by the host name. You can use placeholders to pass information on the host into a Custom Action script or executable as command-line parameters. Learn more about this topic in the Using Placeholders chapter.

As for any notification, Custom Actions configured in the program preferences are used for all the hosts. The program allows overriding the common settings to use individual settings for hosts and groups, if required. It means that you may configure different Custom Actions for hosts and groups.

Exporting Ping Data

Ping Monitor saves ping results for all hosts, so it is possible to export raw ping data and use it in external tools. Ping data exporting options are available in **Statistics** when a host is selected. Open the **Timeline** dialog and use the export option available there. When you initiate ping data export, the program opens the exporting wizard where you can select the scope of the exported data and the export format. The program exports ping data as a .csv file.

Chapter 3: Program Interface Overview

The main window of Ping Monitor **Pic 1** displays the **Hosts** view **A**, the **Reports** view **B**, the **Document** view **C**, the **Log** view **D**, the **Access Control** view **E**, the **Operations** view **F** and the **Ribbon** bar **G**.
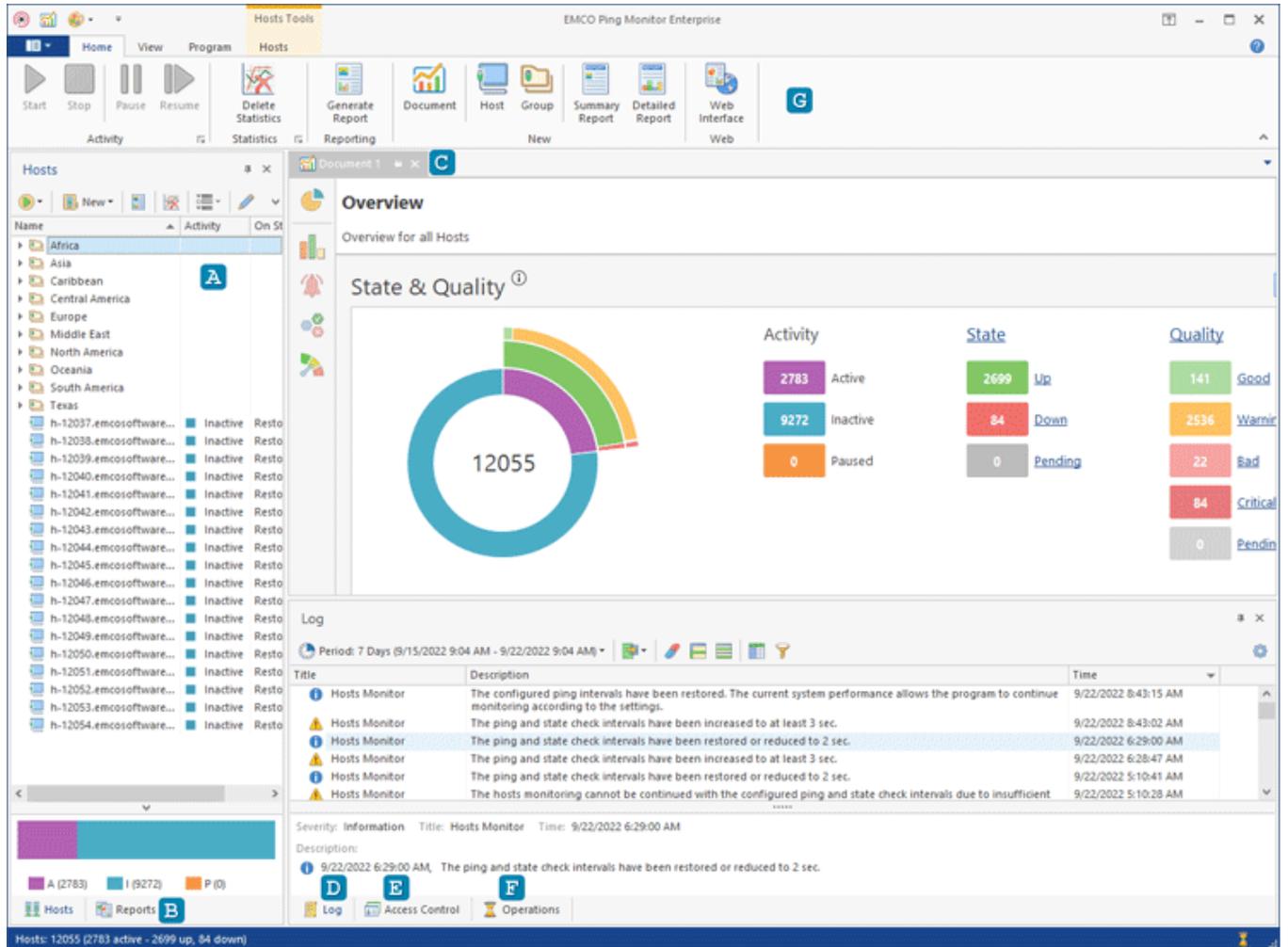
Pic 1. The main program window

The **Hosts** view displays the hosts and groups of hosts in the hierarchical structure and is primarily designed for performing hosts management and monitoring activity management. The **Reports** view is designed to display and manage preconfigured monitors performance and availability reports to be generated either on demand or on a regular basis.

The **Log** view shows those events not connected to hosts availability and monitoring activity, such as messages from supplementary operations, reports generation problems, etc. Within the **Access Control** view, you can define the roles and permissions for the users to access the server. If you would like to review and/or cancel the currently running operations, you can use the **Operations** view.

The **Document** view provides you with access to host monitoring information and statistics Pic 2. You can open multiple documents, if required, to display monitoring information for different hosts. On the left side of the document you can find the navigation panel H that allows you to switch the pages in the document to work with the different types of the data.
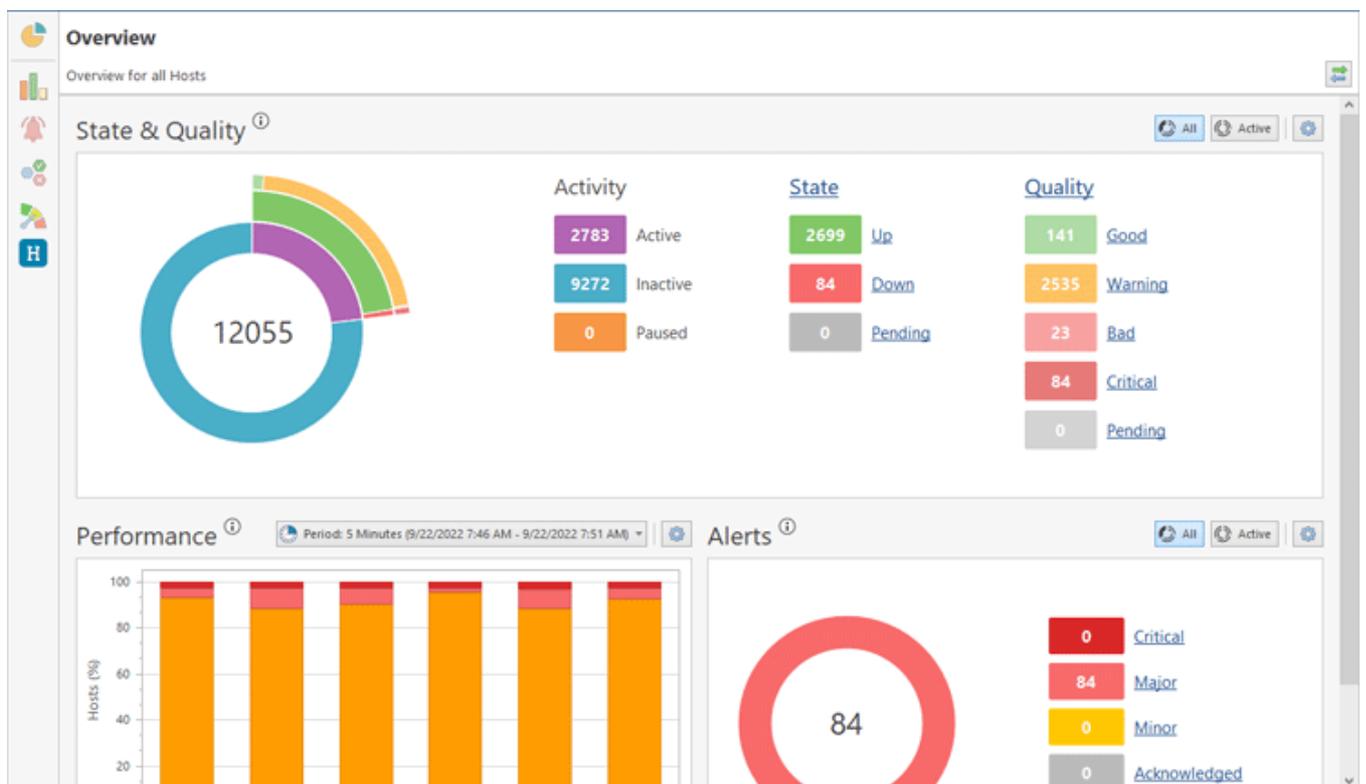
Pic 2. The Document view

Use the navigation panel to work with the following pages. **Overview** provides you with the brief information on the hosts being monitored and their actual state and quality. **Statistics Summary** displays the hosts monitoring statistics for the specified time interval. **Alerts Summary** displays alerts for hosts. You can review all current active alerts and can acknowledge alerts, if you need. **State Summary** can be used to monitor current state of remote hosts. **Quality Summary** allows you to focus on the connection quality to the hosts.

The summary pages allow you to review statistics, alerts, state and quality for multiple hosts at once, but to get details for a specific host, you can click the host name and drill-down to this host to review its characteristics **Pic 3**. You can switch between host characteristics using buttons, located on the navigation bar **I**.
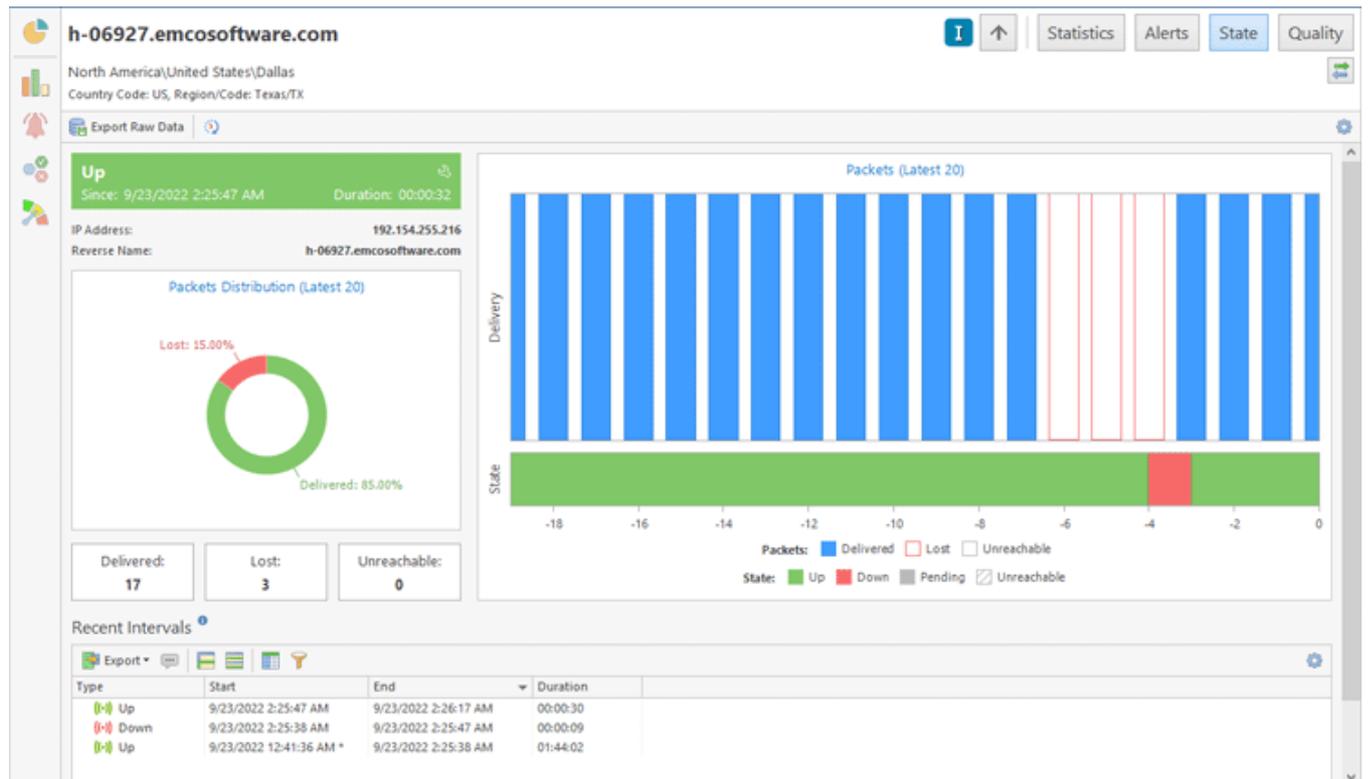
Pic 3. Host monitoring data

Use the **Up** button to navigate to the upper level. You can switch between host monitoring data pages using **Statistics**, **Alerts**, **State** and **Quality** buttons.

The Document View

The **Document** view provides you with access to all monitoring and statistical information collected by the program. By default it is located at the center of the main screen. The program automatically creates a document with the Document 1 name when you run the program at the first time. It is displayed as a tab. If you need, you can create new documents that will appear on the main screen as new tabs. You can open a document on a screen by switching to the corresponding tab.

You can navigate within a document using the navigation bar **A**, located at the left side **Pic 1**. It allows you to switch to the different pages: **Overview**, **Statistics Summary**, **Alerts Summary**, **State Summary** and **Quality Summary**. These pages provide you with the details of the particular aspects of the monitoring data. The summary pages display information about all hosts in the document, but you can also navigate to the host level to see the host details. In the following chapters you can find more information about these pages.
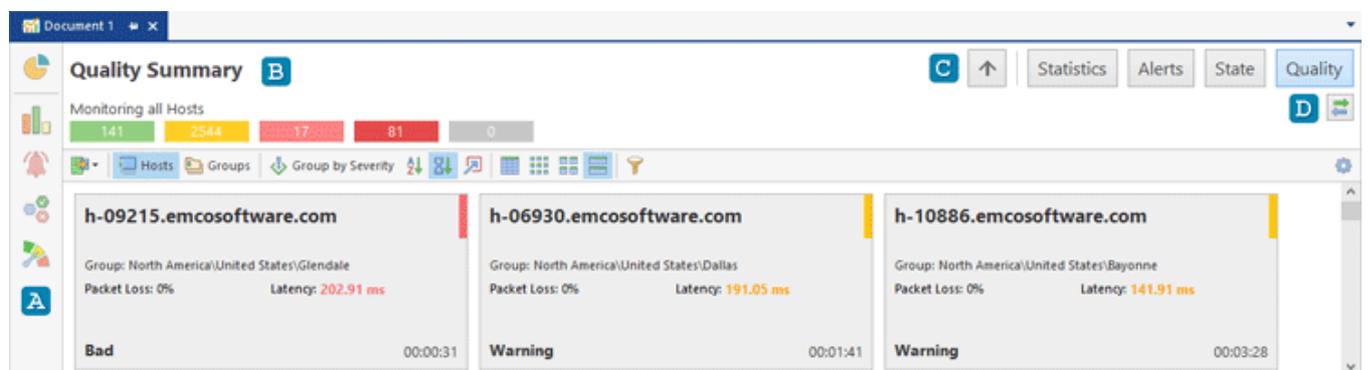
Pic 1. The Document view

The information about the current page opened in the document is displayed in the information panel **B**. There you can see a name of the opened page or a name of a host if you navigated to the host level. The navigation bar **C** allows you to switch the pages within document and navigate through hierarchy. The **Up** button allows going to the upper level, i.e. if you currently is on the host level, so that you can navigate to the summary page displaying information for all hosts. The **Statistics**, **Alerts**, **State** and **Quality** buttons allow switching to the corresponding pages. If you are on the summary level, by pressing these buttons you can switch to the corresponding summary pages. If you are on the host level, these buttons allow you to switch to the corresponding page of the same host.

The **Document** view can be linked to the **Hosts** view to display only the hosts that are selected in the **Hosts** view or that are in the groups selected in the **Hosts** view. This functionality is enabled using the **Link to Hosts View** button on the navigation bar **D**.

By default the **Document** view shows information for all hosts, but it is possible to narrow down to specific hosts in the document. When the document is opened, you can click the **Link to Hosts View** button on the navigation bar and select required hosts in the **Hosts** view. To switch back to all hosts you can click the **Display All** link or toggle out the **Link to Hosts View** button.

You can open a new document by clicking the **Document** button located in the **New** group of the **Home** tab of Ribbon. Alternatively you can select hosts to be added to the document in the **Hosts** view and select the **New Document** option in the context menu items **Show Overview In**, **Show Alerts In** or **Show Statistics In**. When a new document is opened, a new tab with the auto-generated document name is appeared.

You can use the following context-menu actions displayed when the document tab is clicked by the right button of the mouse. These actions allow you to manage a document.

	Close **Close** the document, so that the document tab is closed
	Close All But This **Close all** documents except of the current one
	Close All **Close all** documents, including the current one
	Float Switch the document to the floating mode, that allows moving the document to any place on the screen
	Pin Tab **Pinned** tabs are moved to left and displayed before other tabs
	New Horizontal Tab Group Split the screen horizontally and organize tabs (documents) into groups located one under another

	New Vertical Tab Group
	Split the screen vertically and organize tabs (documents) into groups located one next to another
	Duplicate
	Make a copy of the current document
	Rename
	Set a custom name for a tab (document)

The **Document** view allows you to organize monitoring data as you need. For example, you can open a few documents to review data for specific hosts or groups. Each document has its own UI controls layout, data filters, sorting and other visual presentation settings, so if you need to represent the same data differently, you can do that using different documents.

Overview

The **Overview** `Pic 1` is designed to provide you with the brief information on monitored hosts and their states. It is located within a document, in the middle of the main program window and can be opened using the document navigation panel. You can either overview the entire monitoring system or focus on specific host and/or groups.

Pic 1. The entire monitoring system overview

In the **State & Quality** area of **Overview** the information is summarized in a doughnut chart, so you can easily see the distribution of hosts with different states and quality. Inside a doughnut itself, you can find the total number of host you are focusing. The first column of the legend displays the count of active, inactive and paused hosts – this distribution is represented with the inner doughnut. For the hosts the monitoring is active for, you can find the information on how many of

them are up and down, as well as how many hosts the state is being determined for. This distribution is displayed in the second column of the legend and the middle doughnut respectively. The last column is used to describe the connection quality to monitored hosts. The distribution is reflected in the outer doughnut on the chart. If you would like to focus on host states and connection quality distribution for active hosts, click the **Active** radio button in the right top corner of the area. To switch back to all hosts use the **All** button.

The **State & Quality** part is interactive. You can click the values for states and qualities to drill down to the hosts with the corresponding quality and state.

The **Performance** chart shows historical characteristics of the monitored host and displays how many hosts had particular performance characteristics during the selected period. You can switch the period to see the overall performance change over time.

The **Alerts** chart shows the number of alerts that are active or acknowledged at the current moment. The alerts are grouped by severity, so you can see how critical these alerts are. You can click the displayed numbers of alerts to navigate to these

To refresh the **Overview** pertaining to the selection within the **Hosts** view, you can enable the **Link to Hosts View** item in the toolbar.

Statistics

The **Statistics** page of a document displays the monitoring statistics for specific periods of time. You can open it by clicking the **Statistics Summary** button on the navigation panel of the document.

Statistics Summary

The monitoring statistics summary is represented in a form of a table **Pic 1** where each row stands for a single host. The statistics is displayed for the period chosen on the view toolbar. You can choose between live intervals, which are configured on the **Monitoring Statistics** preference page, a set of predefined historical intervals and custom historical interval. You can apply grouping, sorting and filtering operations for all available hosts at once.

Pic 1. Statistics summary for all hosts

Along with the statistical values, on the **Statistics** page you can find the performance characteristics, calculated on a basis of these values. The conditions for calculating the performance are provided on the **Performance** preference page. By default, the performance values are highlighted due to their severity, as well as the values that affect the performance. This behavior is controlled with the **Highlight** button on the toolbar.

> ℹ️ Please note that not all of the available data columns are displayed on this page by default, but you can always choose the columns you really need and remove the unwanted ones by using the column chooser. For example, you can display the **Uptime Interval** and **Downtime Interval** columns to see how exactly the uptime percentage was calculated.

For the statistics table, you can choose from the following set of columns.

Column	Description	Visible by Default
Host properties		
Host Name	The combination of host address and label provided during host configuration.	Yes
Host Address	The host address.	No
Host Label	The label provided to the host during configuration.	No
Group	The hosts group the current host belongs to.	Yes
Activity characteristics		
Activity Time	The time interval during which the monitoring process has been running.	Yes
Pause Time	The time interval during which the monitoring process has been paused.	No
Monitoring statistics for the specified interval		
Uptime	The percentage of time with the up state.	Yes
Uptime Interval	The time interval during which the host was up.	No
Downtime Interval	The time interval during which the host was down.	No
Outages	The number of outages.	Yes
PL (Packet Loss)	A ratio of the number of lost packets to the number of packets being sent.	Yes
PD (Packet Delivery)	A ratio of the number of delivered packets to the number of packets being sent.	No
Delivered Packets	The absolute number of delivered packets.	No
Lost Packets	The absolute number of lost packets.	No
Dev (Latency Deviation)	A standard deviation from the average latency value for all round-trip times of packets successfully delivered.	Yes
CV (Latency CV)	A percentage ratio of the latency deviation to the average latency calculated for all round-trip times of packets successfully delivered.	Yes
Avg (Average Latency)	An arithmetic mean for all round-trip times of packets successfully delivered.	Yes
Min (Minimum Latency)	A smallest value from all round-trip times of packets successfully delivered.	Yes
Max (Maximum Latency)	A largest value from all round-trip times of packets successfully delivered.	Yes
Performance characteristics		
Perf (Performance)	The performance calculated on a basis of monitoring statistics.	Yes
MOS	A well-established metric to obtain the quality of VoIP on a basis of the latency characteristics and packet loss percentage for all packets sent.	Yes

Column	Description	Visible by Default
Connection quality characteristics		
Good Quality	The percentage of time with the good connection quality.	No
Warning Quality	The percentage of time with the warning connection quality.	No
Bad Quality	The percentage of time with the bad connection quality.	No
Critical Quality	The percentage of time with the critical connection quality.	No
Good Quality Interval	The time interval during which the connection quality was good.	No
Warning Quality Interval	The time interval during which the connection quality was warning.	No
Bad Quality Interval	The time interval during which the connection quality was bad.	No
Critical Quality Interval	The time interval during which the connection quality was critical.	No

You can collapse or expand all the groups using the **Full Expand** and **Full Collapse** buttons on the view area toolbar.

Toolbar Overview

	Period The **Period** button from the **Statistics** view toolbar allows you to choose the time period the summary statistics is displayed for.
	Delete The **Delete** button from the **Statistics** view toolbar is used to delete all monitoring statistics for the selected hosts.
	Export The **Export** button from the **Statistics** view toolbar is intended to export the displayed monitoring statistics to a CSV file.
	Generate Report The **Generate Report** button from the **Statistics** view toolbar can be used to generate a monitoring statistics report for the selected hosts, having specified the required report type, output options and a period of time.
	Highlight The **Highlight** button from the **Statistics** view toolbar enables and disables highlighting the performance cell and cells in the statistics table that affect the performance with the performance mark color.

Full Expand

The **Full Expand** button from the **Statistics** view toolbar should be used to expand all grouping rows.

Full Collapse

The **Full Collapse** button from the **Statistics** view toolbar should be used to collapse all grouping rows.

Group By Box

The **Group By Box** button should be used to configure the data grouping for the table within the **Statistics** view.

Choose Columns

The **Choose Columns** button should be used to choose the columns to be displayed in the table within the **Statistics** view.

Filter Editor

The **Filter Editor** button should be used to define the custom filter criteria to be applied to the data displayed in the table within the **Statistics** view.

Advanced Options

The **Advanced Options** button from the **Statistics** view toolbar opens the view configuration menu where you can reach the settings of storing and displaying monitoring statistics and reset the layout of the view.

Detailed Statistics

To see detailed statistics for a host you can click the host name in **Statistics Summary**. The host statistics page `Pic 2` is used to provide you with the integral monitoring statistics gathered during the specified period, graphically visualized and grouped by categories. The information on this page is grouped in several categories.
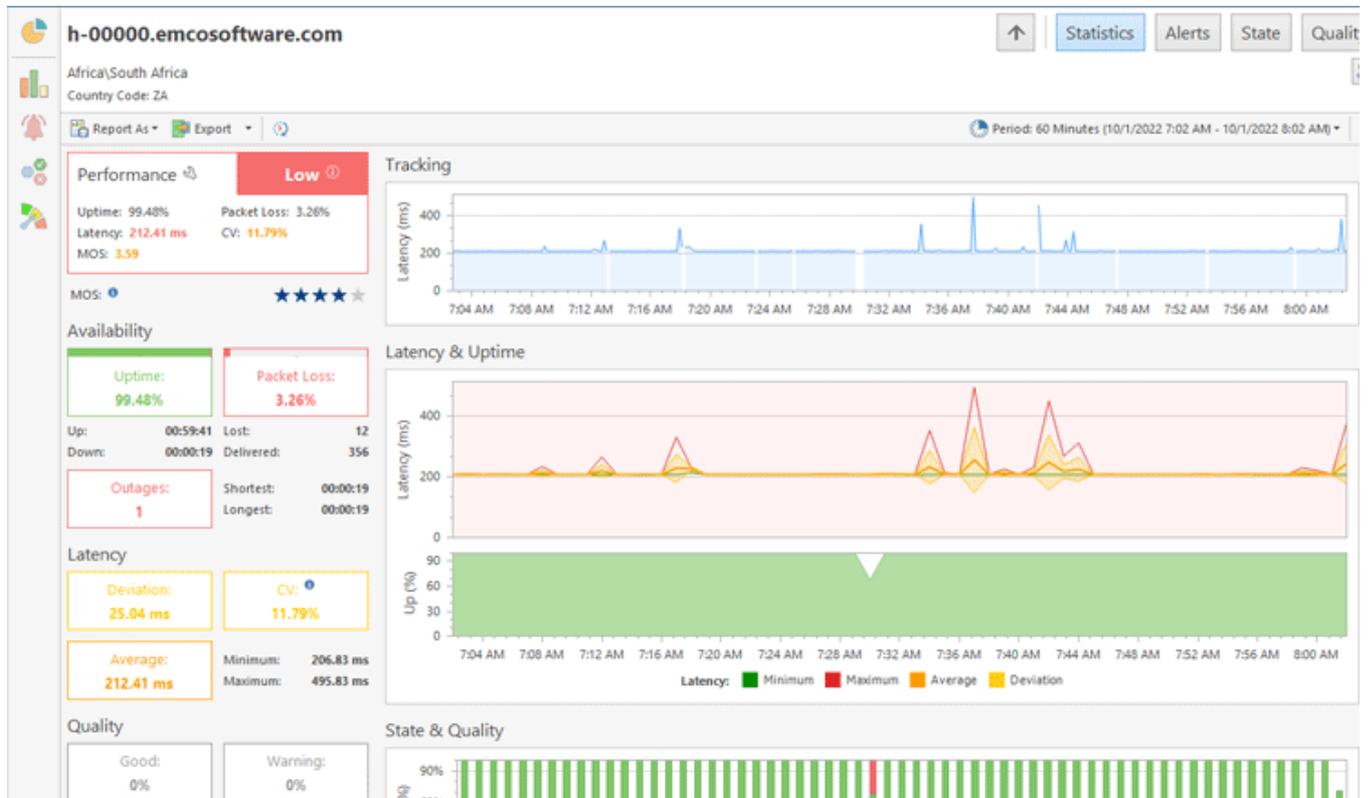
Pic 2. The detailed statistics view for a single host

On the toolbar you can find the buttons for selecting statistics display period, opening the detailed timeline, exporting raw data and publishing the statistics report.

Toolbar Overview

	Period The **Period** button allows you to choose the time period the detailed statistics is displayed for.
	Timeline The **Timeline** button allows you to open the timeline graph of raw ping responses together with host state and connection quality intervals.
	Export Raw Data The **Export Raw Data** button allows you to export raw ping replies data to a CSV format.

	Report As
	The **Report As** button can be used to report the detailed monitoring statistics to a PDF, HTML or MHT file.

	Print
	The **Print** button should be used to print the displayed monitoring statistics.

In the left top corner, you can find the performance characteristics. Below the performance characteristics, you can find the information on host availability during the specified interval. It consists of an uptime percentage, uptime and downtime intervals, a packet loss percentage, lost and delivered packets counts and outages information.

The next category to follow is the information on latency: minimum, maximum, average, deviation and coefficient of variation. The next category is showing you the percentage and intervals of different connection quality during the specified period. The last within the left column comes the category, displaying information on monitoring activity – you can find the activity time interval and pause time interval.

On the right side of the page you can find charts with statistical information. The **Tracking** chart `Pic 3` is aimed to display the real-time information with the latest host responses time. This information is displayed only when reviewing live statistics and, in case the selected interval is longer than an hour, only the data for the latest hour is displayed due to performance reasons.
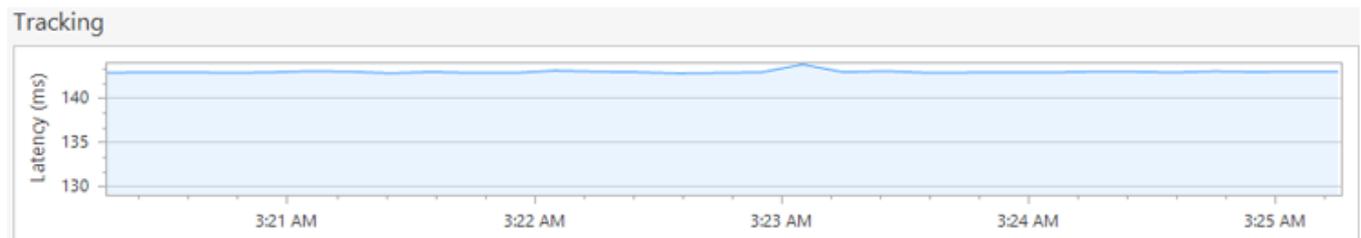
Pic 3. Tracking latency

The **Latency & Uptime** chart `Pic 4` is used to focus on the latency and uptime analysis. You can see latency minimum, maximum, average and latency deviation as well as uptime percent. The level of aggregation in the chart is adjusted automatically for the specified period.
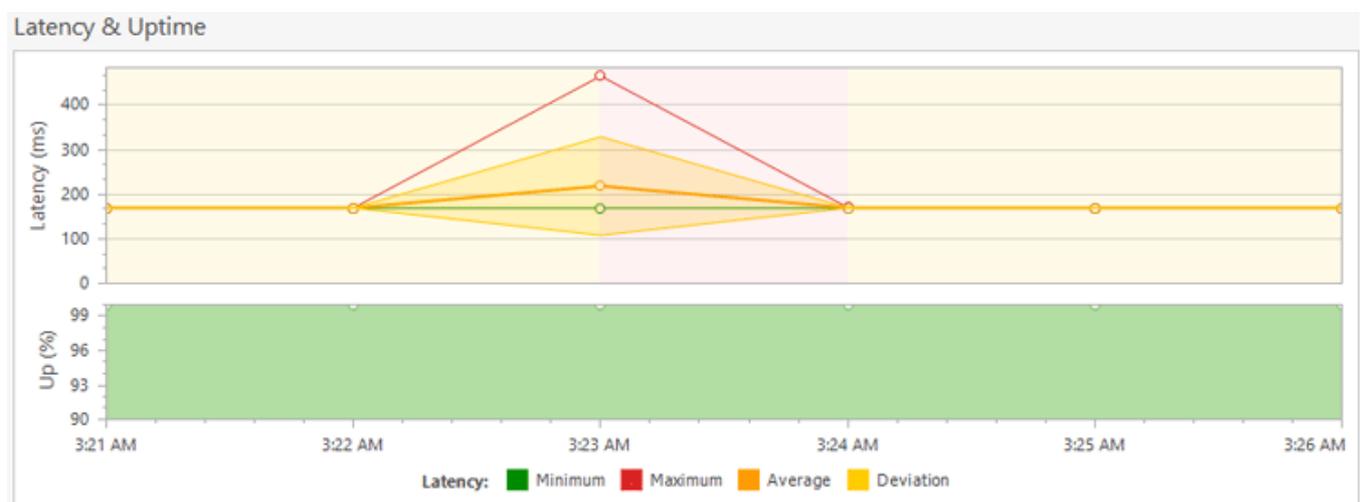
Pic 4. Analyzing latency and uptime

The **State & Quality** chart `Pic 5` is used to focus on the host state and connection quality intervals distribution analysis. It shows a percent of each state and quality values the host had in each of the time intervals. The level of aggregation in the chart is adjusted automatically for the specified period.
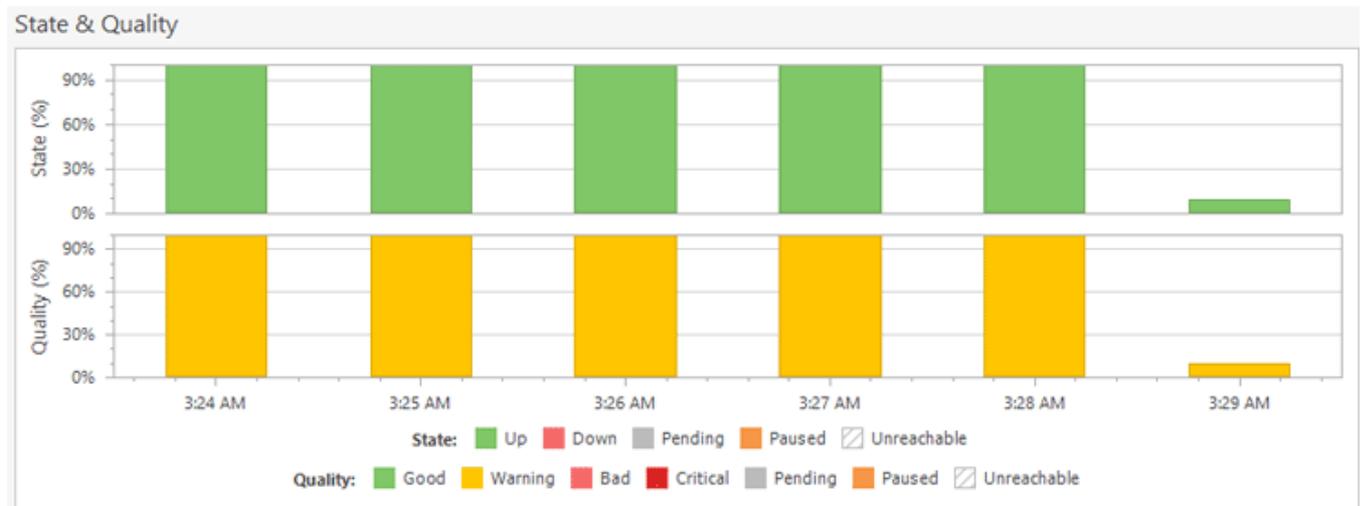
Pic 5. Analyzing state and quality

The **Intervals** table displays the list of all host state and quality intervals for the selected period of time. For each state and quality interval you can see its start and end date and duration `Pic 6`.

Pic 6. Reviewing intervals

The list of intervals is displayed in a form of a tree, where the root nodes represent the specific state. In case the host has been unreachable during any interval, it can be expanded to review when the host was reachable and when not. In case the comment is provided for the interval, it is displayed under the root node. For each interval, along with its type, you can find the start time, end time and duration. In case the interval is exceeding the selected period, the exceeding time is marked with a star.

Toolbar Overview

Export

The **Export** button from the toolbar allows you to export the displayed intervals list to a CSV format.

💬	**Set Comment** The **Set Comment** button can be used to provide a comment for the selected interval.
((•))	**State** The **State** button allows you to display state intervals in the table.
▁▃▅	**Quality** The **Quality** button allows you to display quality intervals in the table.
▤	**Full Expand** The **Full Expand** button from the toolbar should be used to expand all nodes in the intervals tree.
☰	**Full Collapse** The **Full Collapse** button from the toolbar should be used to collapse all nodes in the intervals tree.
▦	**Choose Columns** The **Choose Columns** button should be used to choose the columns to be displayed in the intervals tree.
▽	**Filter Editor** The **Filter Editor** button should be used to define the custom filter criteria to be applied to the data displayed in the intervals tree.
⚙	**Advanced Options** The **Advanced Options** button from the toolbar opens the view configuration menu where you can reset the layout of the view.

For each state or quality interval, it is possible to provide a comment. The comment can, for example, describe the reason for the outage, or something else. To provide a comment, select the interval and choose the **Set Comment** item in the pop-up menu or click the corresponding button on the toolbar. The dialog will be displayed on the screen to let you provide the comment. Either the selected or all intervals can be exported to a CSV file using the **Export** button on the toolbar and the **Export All** and **Export Selected** menu items. At any point, you can reset the view layout to defaults using the **Reset Layout** option from the **Advanced Options** menu.

The **Events** table contains all monitoring events for the host and can be used as a monitoring log. If you are facing some problems during monitoring or would like to know when the monitoring process was started and stopped, you should refer to this page.

Pic 7. The host events for a single host

The events are displayed in a form of a table where each row represents a single event. You can sort, group and filter the events by any column as well as change the columns set. By default the table consists of the event type represented by an icon, the event title, the logging time and the event description itself, with or without a troubleshooting hint. The description and hint for any event is by default wrapped, so that you can easily read it. If you would like to have more events visible at the same time, you can configure the **Events** page to display only one line per event by disabling the **Wrap Description** option from the **Advanced Options** menu. If required, it is possible to add the **Error Code** column to the view using the **Column Chooser**.

The following icons are used to display the event types:

- the blue icon with an 'i' character means that everything is OK;

- the brown circle icon with a cross-cut line is used to identify that the operation was canceled by user or due to shutdown of the underlying system;

- the yellow icon with an exclamation mark is the warning icon. It means that the special attention should be payed to this event;

- the red icon with a white cross is the error sign: it stands for a failure event.

If required, you can add a column containing the text representation for the severity, that can be used for grouping and filtering data.

Toolbar Overview

	Export The **Export** button from the toolbar is intended to export the displayed events to a CSV file.
	Full Expand The **Full Expand** button from the toolbar should be used to expand all the grouping rows in the view.
	Full Collapse The **Full Collapse** button from the toolbar should be used to collapse all the grouping rows in the view.

▦	**Group By Box** The **Group By Box** button should be used to configure the data grouping for the **Events** page.
▦	**Choose Columns** The **Choose Columns** button should be used to choose the columns to be displayed on the **Events** page.
▽	**Filter Editor** The **Filter Editor** button should be used to define the custom filter criteria to be applied to the data displayed on the **Events** page.
⚙	**Advanced Options** The **Advanced Options** button from the **Events** page toolbar opens the view configuration menu where you can enable/disable automatic scroll and messages wrapping, and reset the layout of the view.

If it is really important for you to see the newly arrived events as soon as possible, you can enable the **Autoscroll** option in the **Advanced Options** menu. In case this option is enabled, the view will automatically scroll to new events as soon as they arrive.

Using the toolbar or pop-up menu it is also possible to export all or selected events to a CSV file for future analysis, sharing with colleagues or sending problem reports to your ISP.

The layout of the **Events** page, including all the grouping and sorting settings and the details pane visibility, can be easily reset to factory settings by choosing the **Reset Layout** option from the **Advanced Options** menu.

Timeline

Ping Monitor can show you the timeline of raw ping reply data along with host state and connection quality intervals. You can open the timeline using the **Timeline** button in the detailed statistics view. You can focus on specific interval of the timeline by clicking the point within **Latency & Uptime** or **State & Quality** charts.
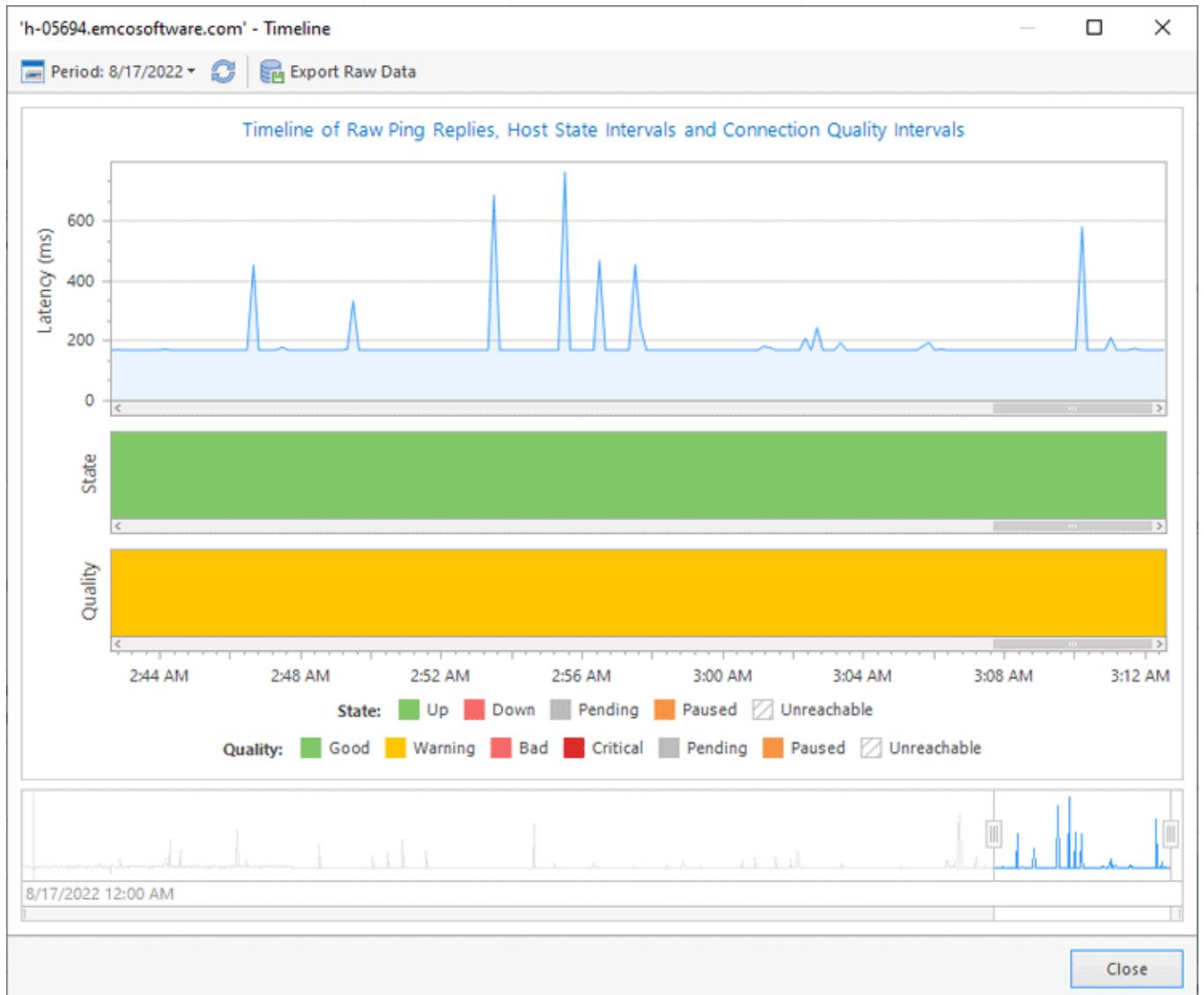
Pic 8. Timeline

Within the **Timeline** dialog , you can find the timeline graph and the sliders to be used for navigation through the timeline. The timeline graph consists of three parts, those are **Latency**, **State** and **Quality**. The **Latency** part is used to display the ping replies data, the **State** part reflects the state intervals on the timeline and the **Quality** part is used for displaying the quality intervals.

Toolbar Overview

Period

The **Period** button allows you to choose the interval the timeline is displayed for.

	Refresh The **Refresh** button allows you to actualize the data on raw ping replies, state and connection quality for the specified period.
	Export Raw Data The **Export Raw Data** button allows you to export raw ping replies data to a CSV format.

Along with using the sliders for navigation, it is also possible to swipe the chart itself for navigation and use mouse wheel for zooming. The timeline range is limited to 30 days due to performance reasons. You can change the timeline range using the **Period** button on the dialog toolbar. To actualize ping replies data along with state and quality intervals, use the **Refresh** button on the toolbar. The **Export Raw Data** button can be used to export raw ping replies data to a CSV format.

Alerts

The **Alerts** page of a document displays the current alerts for monitored hosts. You can open it by clicking the **Alerts Summary** button on the navigation panel of the document.

Alerts Summary

The **Alerts Summary** page displays a list of current alerts detected for monitored hosts. Alerts are displayed in a table, where a row represents the alert and the columns show the host for which the alert is detected, alert name, severity, duration and state Pic 1. The summary page shows a list of alerts for all hosts represented in the document.

Pic 1. Alerts summary

You can use data grouping, filtering and sorting options available for the table interface to represent data according with your needs. You can switch between different modes of **Alerts Summary** using the corresponding buttons on the toolbar.

Toolbar Overview

	Edit
✏️	The **Edit** button allows editing a selected alert, so you can change the alert severity or acknowledge the alert.
	Export
📤	The **Export** button allows exporting alerts information displayed on the screen.

All

The **All** button allows you to display all current alerts, including the alerts in the Active and Acknowledged states.

Active

The **Active** button allows you to display alerts with the Active state only.

Acknowledged

The **Acknowledged** button allows you to display alerts with the Acknowledged state only.

Highlight

The **Highlight** button turns on coloring of the alert severity text in the table, so you can find alerts with the critical problems easier.

Full Expand

The **Full Expand** button expands all grouping nodes, if grouping is turned on for the table.

Full Collapse

The **Full Collapse** button collapses all grouping nodes, if grouping is turned on for the table.

Group By Box

The **Group by Box** button enables data grouping in the table by the values of the selected columns. When this option is enabled you can drag & drop a column to the appeared area to group data by values of this column.

Choose Columns

The **Choose Columns** button allows you to select columns that should be displayed or hided on the displayed table.

Filter Editor

The **Filter Editor** button should be used to define the custom filter criteria to be applied to the monitored entries.

The alerts reported by the program allow you to discover the current problems with the monitored hosts. To help you managing the problems there are two types of alerts – active and acknowledged alerts. Active alert means that there is a new problem. If you know about the problem and work on resolving it, you can acknowledge the alert permanently or for a specific period of time. Acknowledged alerts are displayed with the corresponding state, so you easily identify them and don't mix with active alerts.

You can acknowledge alerts by editing them and enabling the acknowledge options. To manage an alert use the actions available in toolbar or on the **Alerts** tab of the contextual **Alerts Tools** menu on Ribbon. Alternatively you can use context menu for alerts to acknowledge them with just a single mouse click.

Host Alerts

In the **Alerts Summary** page you can see all current alerts for all monitored hosts. Note that alerts can be detected by different conditions that you can configure and customize, so the list of alerts can contain different alerts for the same host and alerts for the different hosts as well. For each alert **Alerts Summary** reports the name of the host where the alert is detected. These names work as hyperlinks, so you can click them to navigate to the host level and see all alerts for a specific host.

The list of alerts for a host is identical to the **Alerts Summary**. It is represented with the identical table with the same actions available, but on the host level you can see alerts reported for a specific host only.

State

The **State** page of the document is mainly designed to be used for focusing on hosts states monitoring, where you can easily detect any problematic situations just in time. You can open it by clicking the **State Summary** button on the navigation panel of the document.

State Summary

State Summary displays the actual states of hosts. It shows only those hosts the monitoring is currently active for. It is organized with the help of tiles representing the objects being monitored, that are colored to indicate of the hosts states. Let us take a closer look at the data representation.
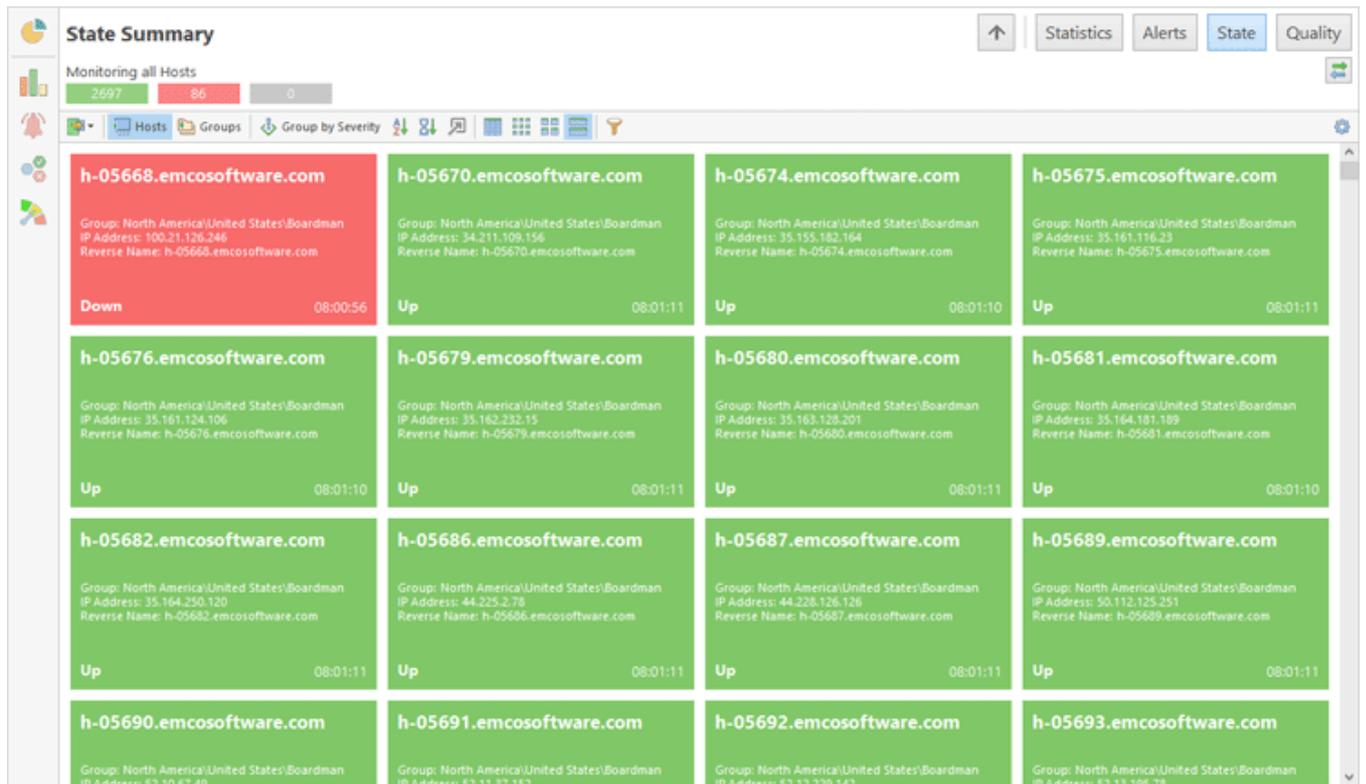
Pic 1. Monitoring hosts state

The first mode of the **State Summary** is the per-host state monitoring Pic 1. This is the default mode, where each tile in the view represents a single host that is currently monitored and is colored with the host state color: green – for up, red – for down, and gray – for pending. In case the host is currently unreachable, thus the state is represented with the latest reachable one, the tile is hatched.

Together with the state, for each host you can find out how long has the host been in this state, the group the host is located in, the host IP address and resolved reverse name. All these information is available in the tool-tip and on the tile itself, when the large tiles are used. For medium tiles, you can see the host name and label on the tile together with the state time stamp. The small tiles are simply filled with the host state color; any information is available in the tool-tip only.

Pic 2. Monitoring state for groups of hosts

Along with per-host state monitoring, it is possible to monitor state for host groups. The group tile can either represent the group or the set of individual hosts (selected individually or not belonging to any group) Pic 2. The group tile is displaying the number of hosts within the group that are currently in specific states. When monitoring state in grouped mode, you can click on the group to focus on hosts from that group, or click on the specific state part within a group to focus on hosts with that specific state.

Pic 3. Hosts states represented as a table

Tiles representation of host state us useful for control rooms where all hosts are displayed on a screen. In other cases you may need to use a table representation Pic 3. It shows host names, host states, state duration and other useful information as table columns.

You can switch between different modes of the **State Summary** page using the corresponding buttons on the view toolbar.

Toolbar Overview

Export	**Export** The **Export** button allows exporting hosts state information displayed on the scree.
Hosts	**Hosts** The **Hosts** button is used to configure the view for monitoring each host individually.
Groups	**Groups** The **Groups** button is used to configure the view for monitoring groups of hosts.

Group by Severity	**Group by Severity** The **Group by Severity** button allows you to group the view the way that the problematic nodes are always displayed on top.
	Sort by Name When monitoring hosts, the **Sort by Name** button enables the view sorting by entry name.
	Sort by Time When monitoring hosts, the **Sort by Time** button enables the view sorting by state change time stamp.
	Focus on Problems The **Focus on Problems** button allows you to configure the view to be automatically scrolled to entries that go down, when grouped by severity and sorted by time.
	Highlight The **Highlight** button from the **Statistics** view toolbar enables and disables highlighting the performance cell and cells in the statistics table that affect the performance with the performance mark color.
	Table The **Table** button switches the view to the table representation, where each host and its data is represented as a table row.
	Small The **Small** button switches the view to the mode where each monitored host is represented just with a pictogram describing its state. Any other information on the entry is available in the tool tip only.
	Medium The **Medium** button is used to switch to the mode where each entry is represented with a tile containing only the summary information on the entry. The detailed info is available in the tool tip.
	Large The **Large** button enables the view mode where a tile representing each entry contains maximum information on the entry being monitored.
	Full Expand The **Full Expand** button is available in the table mode only. It expands all grouping nodes, if grouping is turned on for the table.
	Full Collapse The **Full Collapse** button is available in the table mode only. It collapses all grouping nodes, if grouping is turned on for the table.

	Group By Box The **Group by Box** button is available in the table mode only. It enables data grouping in the table by the values of the selected columns. When this option is enabled you can drag & drop a column to the appeared area to group data by values of this column.
	Choose Columns The **Choose Columns** button is available in the table mode only. It allows you to select columns that should be displayed or hided on the displayed table.
	Filter Editor The **Filter Editor** button should be used to define the custom filter criteria to be applied to the monitored entries.

All entries within **State Summary** can be grouped by severity so that the problematic entries are always on top. To enable such grouping, use the **Group by Severity** button on the toolbar. For example, when enabled, the hosts, that are in the down state, will be displayed on top, then hosts that are in the up state will follow and then there will be the hosts with the pending state.

The Filter Editor button allows you to filter out entries with specific state. To switch between tiles of different size, use the Small, Medium and Large buttons. You can switch to the table data representation using the Table button.

Host State

On the **State Summary** page you can click on a host to navigate to the host details. It allows you to review the detailed information for a single host Pic 4 .
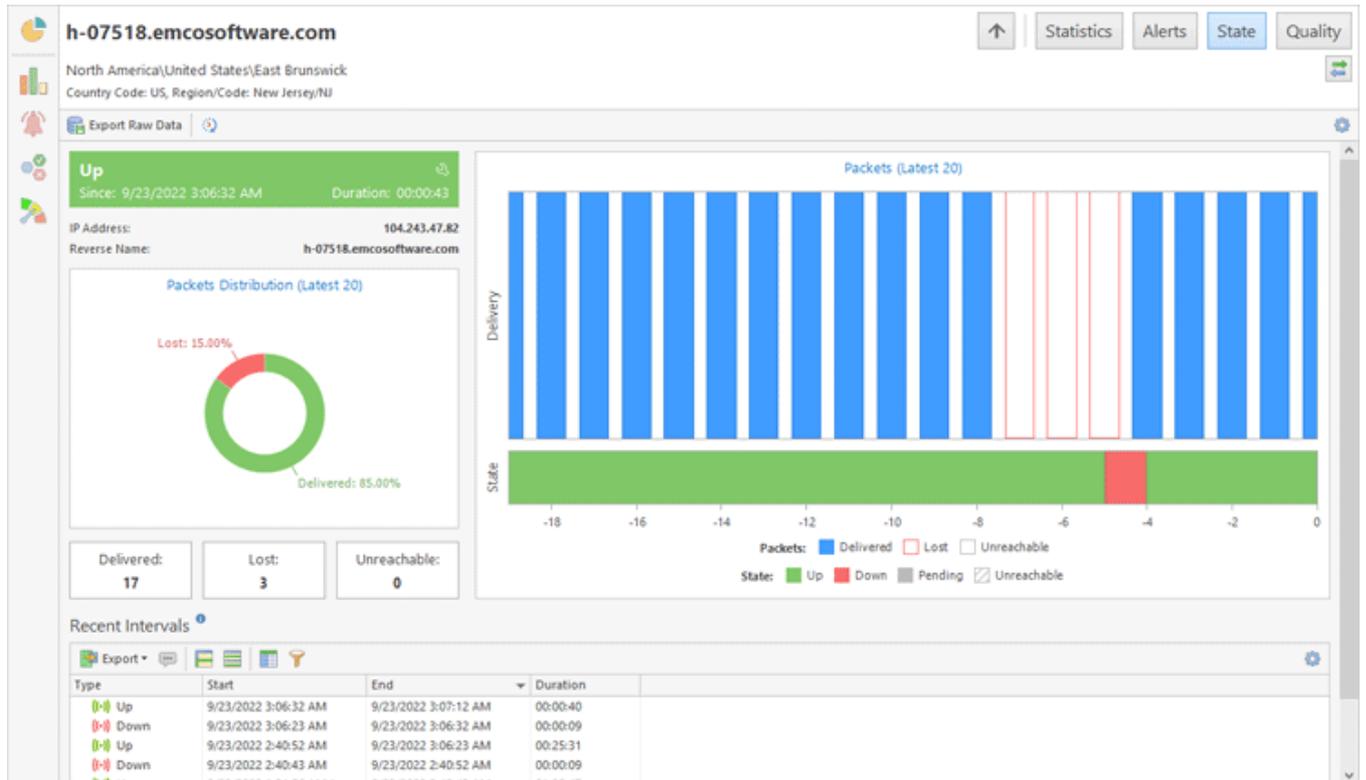
Pic 4. Monitoring state for a single host

On the host state page, in the left top corner you can find the block that is quite similar to the large tile representing the host and contains the same information. Below this block, you can view the information on the distribution for the twenty latest packets. To the right those latest packets are displayed in the chronological order as well as the host state that is reached after each response.

On the bottom on the page you can find the area with recent state intervals. It is used to display the most recent intervals that occurred during the last hour.

Quality

The **Quality** page of the document is designed to be used for focusing on connection quality monitoring, where you can easily detect any problematic situations just in time. You can open it by clicking the **Quality Summary** button on the navigation panel of the document.

Quality Summary

Quality Summary displays real-time quality metrics of the monitored hosts. It displays only those hosts the monitoring is currently active for. It is organized with the help of tiles representing the objects being monitored. Let us take a closer look at the data representation.
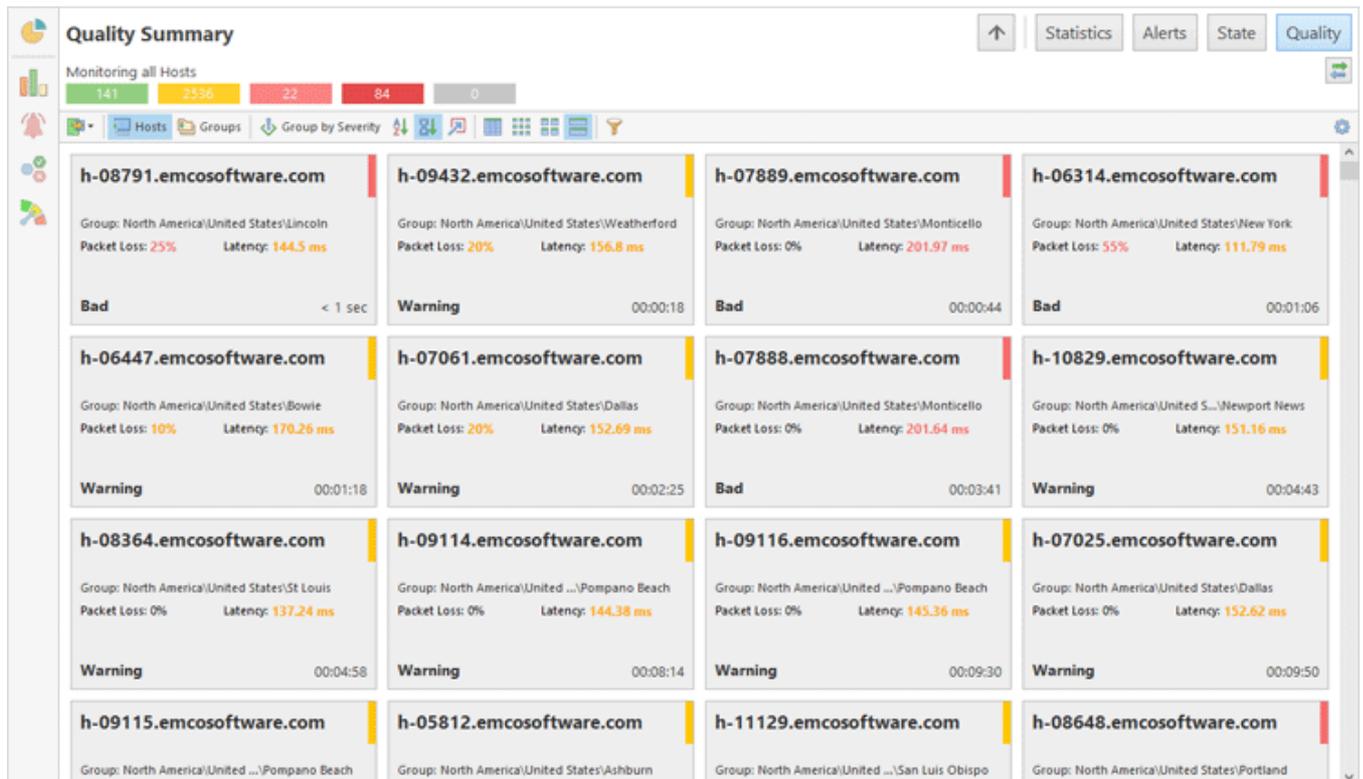
Pic 1. Monitoring hosts connection quality

The first mode of **Quality Monitor** is the per-host connection quality monitoring Pic 1 . This is the default mode, where each tile represents a single host. For the hosts that are monitored, the connection quality is calculated based on the rules defined in the program preferences and/or host settings. The tile is filled with red color in case all packets from the sample used to calculate the connection quality are lost, thus the quality is critical. In other cases, the quality value is displayed with the help of the colored tag on the right of the tile: green – for good quality, yellow – for warning, red – for bad, and gray – for pending. In case the host is currently unreachable, thus the quality is represented with the latest reachable one, the tile is hatched.

On the large tiles, you can find the parameters for each host used to calculate the quality and see which parameter is leading to the warning or bad-quality value. The same way as for the state, you can see how long the host connection quality has had this or that value. The smaller the tile the less information is available immediately, but there is still a whole set of values in the tool-tip.

Pic 2. Monitoring connection quality for groups of hosts

Along with per-host connection quality monitoring, it is possible to monitor connection quality for host groups. The group tile can either represent the group or the set of individual hosts (selected individually or not belonging to any group) **Pic 2**. The group tile is displaying the number of hosts within the group having specific connection quality. When monitoring connection quality in grouped mode, you can click on the group to focus on hosts from that group, or click on the specific connection quality part within a group to focus on hosts having that specific connection quality.

80

Pic 3. Connection quality displayed as a table

Tiles representation of quality may be helpful for control rooms where all hosts are displayed on a single screen. In other cases you can switch to the data representation as a table. In this case hosts are displayed as table rows and quality metrics are displayed as table columns `Pic 3`.

You can switch between different modes of **Quality Summary** using the corresponding buttons on the view toolbar.

Toolbar Overview

Export	**Export** The **Export** button allows exporting hosts quality information displayed on the screen.
Hosts	**Hosts** The **Hosts** button is used to configure the view for monitoring each host individually.
Groups	**Groups** The **Groups** button is used to configure the view for monitoring groups of hosts.
Group by Severity	**Group by Severity** The **Group by Severity** button allows you to group the view the way that the problematic nodes are always displayed on top.

	Sort by Name When monitoring hosts, the **Sort by Name** button enables the view sorting by entry name.
	Sort by Time When monitoring hosts, the **Sort by Time** button enables the view sorting by connection quality change time stamp.
	Focus on Problems The **Focus on Problems** button allows you to configure the view to be automatically scrolled to entries where connection quality goes critical, when grouped by severity and sorted by time.
	Highlight The **Highlight** button is available in the table representation mode only. It turns on coloring of the host quality text in the table, so you can find hosts with the problems easier.
	Table The **Table** button switches the view to the table representation, where each host and its data is represented as a table row.
	Small The **Small** button switches the view to the mode where each monitored host is represented just with a pictogram describing its connection quality. Any other information on the entry is available in the tool tip only.
	Medium The **Medium** button is used to switch to the mode where each entry is represented with a tile containing only the summary information on the entry. The detailed info is available in the tool tip.
	Large The **Large** button enables the view mode where a tile representing each entry contains maximum information on the entry being monitored.
	Full Expand The **Full Expand** button is available in the table mode only. It expands all grouping nodes, if grouping is turned on for the table.
	Full Collapse The **Full Collapse** button is available in the table mode only. It collapses all grouping nodes, if grouping is turned on for the table.

	Group By Box The **Group by Box** button is available in the table mode only. It enables data grouping in the table by the values of the selected columns. When this option is enabled you can drag & drop a column to the appeared area to group data by values of this column.
	Choose Columns The **Choose Columns** button is available in the table mode only. It allows you to select columns that should be displayed or hided on the displayed table.
	Filter Editor The **Filter Editor** button should be used to define the custom filter criteria to be applied to the monitored entries.

All entries within **Quality Summary** can be grouped by severity so that the problematic entries are always on top. To enable such grouping, use the **Group by Severity** button on the toolbar. For example, when enabled, the hosts, that are in the down state, will be displayed on top, then hosts that are in the up state will follow and then there will be the hosts with the pending state.

The **Filter Editor** button allows you to filter out entries with specific connection quality. To switch between tiles of different size, use the **Small**, **Medium** and **Large** buttons. To display data as a table you use the **Table** button.

Host Quality

On the **Quality Summary** page you can click on a host to navigate to the host details. It allows you to review the detailed information for a single host Pic 4.
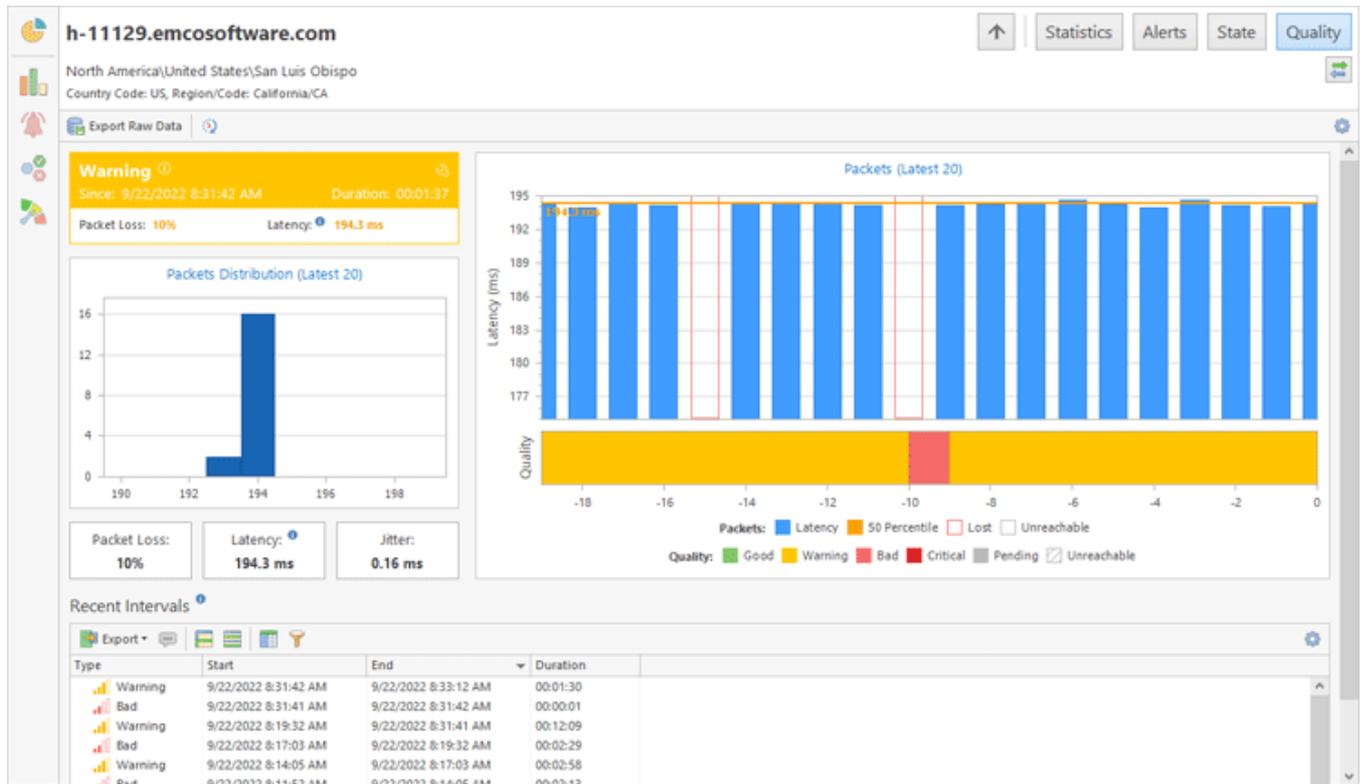
Pic 3. Monitoring connection quality for a single host

On the host quality page, in the left top corner you can find the block that is quite similar to the large tile representing the host and contains the same information. Below this block, you can view the information on the distribution for the packets from a sample used to calculate the connection quality. Below the packets distribution, you can find the connection quality characteristics. To the right those latest packets are displayed in the chronological order as well as the connection quality that is reached after each response.

On the bottom on the page you can find the area with recent quality intervals. It is used to display the most recent connection quality intervals that occurred during the last hour.

Hosts View

The **Hosts** view is by default located on the left of the main program window and displays the hosts and groups of hosts in the hierarchical structure `Pic 1`. This view was primarily designed for performing hosts management, so you can add and remove hosts there, and start and stop monitoring of the hosts.
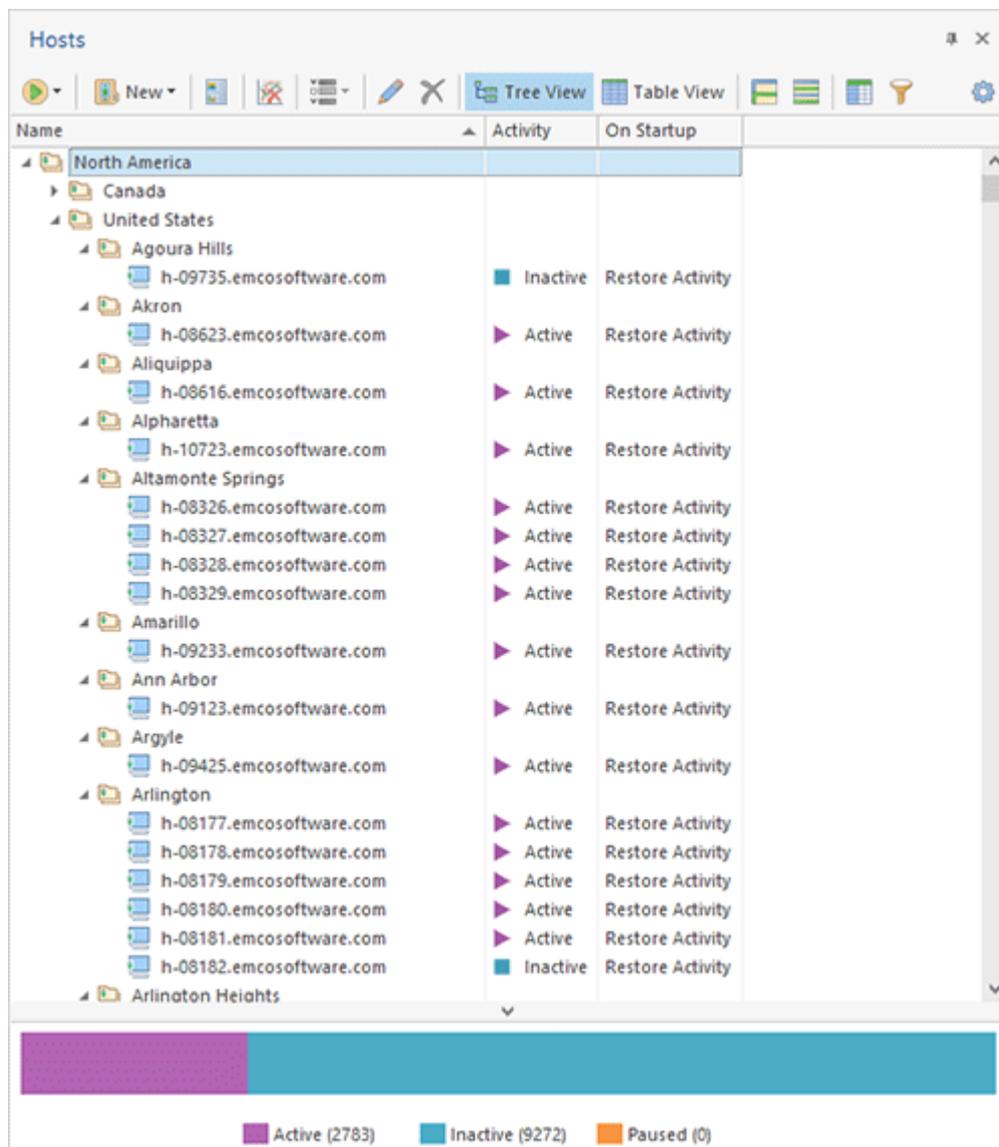
Pic 1. The Hosts view

You can switch from the tree structure representation to the table one to be able to apply grouping, sorting and filtering operations for all available hosts at once. The icon next to every item is used to describe of the item's type. The following set of icons is used:

- the group of hosts;

- the host;

- the host with duplicate address.

In the **Hosts** view you can find the current monitoring activity for each host, so for each host you can see whether it is monitored or not. If a host is currently monitored, it is displayed as **Active**. If monitoring of a host is stopped, the host is displayed as **Inactive**. If monitoring is paused, the host is displayed as **Paused**.

At the bottom of the **Hosts** view you can find an interactive chart that displays how many hosts are **Active**, **Inactive** or **Paused**. It gives you a quick overview of monitoring activity of all your hosts. The chart is interactive, so you can click the chart bars or the chart legend entries to apply a filter and display hosts with a selected type of activity only, for example, display **Inactive** hosts only. To switch the view and display hosts with all types of activity you need to click the **Back to All Hosts** link displayed above the list of hosts.

> Please note that not all of the available data columns are displayed in this view by default, but you can always choose the columns you really need and remove the unwanted ones by using the column chooser.

In the **Hosts** view you can choose from the following set of columns.

Column	Description	Visible by Default
Name	The combination of host address and label provided during host configuration.	Yes
Activity	The current monitoring activity: either Active, or Paused or Inactive.	Yes
Description	The description provided for the host during its configuration.	No
IP Address	The IP address of the host being monitored, as resolved during monitoring.	Yes
Reverse Name	The DNS name of the host being monitored, as resolved during monitoring.	No
Dynamic IP	The indication that the host has a dynamic IP address, thus the address must be resolved before each ping.	No
On Startup	The sign either the monitoring should be activated for this host on startup, or the host monitoring should stay inactive, or the previous activity should be restored.	Yes

From the **Hosts** view, you can manage a set of hosts and groups of hosts, control the monitoring process activity for specific hosts and generate statistical reports for custom periods of time. All these actions are available from the view pop-up menu and on the toolbar.

The other useful features of this view are an ability to use copy/paste and drag/drop to copy and move hosts between groups and the ability to import/export hosts and groups. The corresponding actions are available in the pop-up menu, **Organize** Ribbon group and **Clipboard** Ribbon group on the **Program** page.

Toolbar Overview

▶▾	**Manage Activity** The **Manage Activity** button from the **Hosts** view toolbar can be used to start, stop and pause the monitoring process for the selected hosts.
New ▾	**New** The **New** button from the **Hosts** view toolbar allows you to create hosts and groups of hosts having provided the required properties.
	Generate Report The **Generate Report** button from the **Hosts** view toolbar can be used to generate a monitoring performance and availability report for the selected hosts and groups of hosts, having specified the required report type, output options and a period of time.
	Delete Statistics The **Delete Statistics** button from the **Hosts** view toolbar is used to delete all monitoring data for the selected hosts.

	Auto-start The **Auto-start** drop-down button from the **Hosts** view contains the actions for the selected hosts to be included to and excluded from the auto-start list.
	Edit The **Edit** button from the **Hosts** view toolbar should be used to edit the selected host or group of hosts.
	Delete The **Delete** button from the **Hosts** view toolbar allows you to permanently delete the selected hosts and/or groups of hosts.
	Tree View The **Tree View** button from the **Hosts** view toolbar switches the view to the hierarchical representation of groups and hosts.
	Table View The **Table View** button from the **Hosts** view toolbar switches the view to the flat representation of groups and hosts.
	Full Expand The **Full Expand** button from the **Hosts** view toolbar should be used to expand all nodes in the view.
	Full Collapse The **Full Collapse** button from the **Hosts** view toolbar should be used to collapse all nodes in the view.
	Choose Columns The **Choose Columns** button should be used to choose the columns to be displayed in the **Hosts** view.
	Filter Editor The **Filter Editor** button should be used to define the custom filter criteria to be applied to the data displayed within the **Hosts** view.
	Advanced Options The **Advanced Options** button from the **Hosts** view toolbar opens the view configuration menu where you can reach the monitoring settings configuration and reset the layout of the view.

It is possible to switch between hierarchical and flat representation of groups and hosts using the **Tree View** and **Table View** items on the toolbar and in the popup menu. You can collapse or expand all the groups using the **Full Expand** and **Full Collapse** buttons on the view toolbar.

Now you are familiar with the **Hosts** view and should be able to use its benefits during the everyday work.

Reports View

The **Reports** view `Pic 1` is by default located on the left of the program main window. It is designed to display and manage preconfigured monitors performance and availability reports to be generated either on demand or on a regular basis.

Pic 1. The Reports view

The icon next to every item represented in the **Reports** view is used to describe of the item's type and state. Below is the list of icons used:

- the detailed report that is enabled for generation;

- the summary report that is enabled for generation;

- the detailed report that is disabled for generation;

- the summary report that is disabled for generation.

As for the problematic situations, the following overlays are used:

- the report is incorrectly configured and won't be generated;

- the report won't be generated, because there no enabled report outputs.

For the detailed information on different report types and states, you can refer the **Preconfigured Reports** section of this document.

The **Reports** view initial state displays the report name, recurrence, next automatic generation time (for regular reports) and the sign if the report is enabled. You can customize the **Reports** view by choosing other columns to be displayed and filter data to make it feet your needs best – see the **Grouping and Filtering Data** topic for details. It is always possible to roll back to the default view layout using the **Reset Layout** item from the **Advanced Options** menu.

Toolbar Overview

	Generate
	The **Generate** button from the **Reports** view toolbar should be used to immediately generate the output for the selected enabled reports.

New ▾	**New** The **New** button from the **Reports** view toolbar allows you to create a new preconfigured monitoring performance and availability report having provided the required properties.
	Enable The **Enable** button from the **Reports** view toolbar should be used to turn on an ability of generating the selected reports both manually and on a regular basis.
	Disable The **Disable** button from the **Reports** view toolbar should be used to turn off an ability of generating the selected reports both manually and on a regular basis.
	Open Storage The **Open Storage** button from the **Reports** view toolbar allows you to open the local reports storage for the selected preconfigured report.
	Edit The **Edit** button from the **Reports** view toolbar should be used to edit the selected preconfigred report.
	Delete The **Delete** button from the **Reports** view toolbar is used to permanentrly deleted the selected reports.
	Full Expand The **Full Expand** button from the **Reports** view toolbar should be used to expand all the grouping rows in the view.
	Full Collapse The **Full Collapse** button from the **Reports** view toolbar should be used to collapse all the grouping rows in the view.
	Group By Box The **Group By Box** button should be used to configure the data grouping for the **Reports** view.
	Choose Columns The **Choose Columns** button should be used to choose the columns to be displayed in the **Reports** view.
	Filter Editor The **Filter Editor** button should be used to define the custom filter criteria to be applied to the data displayed in the **Reports** view.

⚙   **Advanced Options**

The **Advanced Options** button from the **Reports** view toolbar opens the view configuration menu where you can reset the layout of the view.

From the **Reports** view, it is possible to create new preconfigured reports to be generated either on demand or on a regular basis, control reports enablement, generate, edit and delete reports, etc. All these actions are available on the **Reports** view toolbar and in view popup menu. The **Reporting** contextual Ribbon page from the **Reporting Tools** category is displayed when the **Reports** view is active and also contains the actions for reports generation and management.

The **Reports** view fully supports the drag/drop and copy/paste techniques. Via those techniques you can add groups and hosts to the reports members set and duplicate reports. From this view it is also possible to export preconfigured reports, and import them to the program. The corresponding actions are available in the pop-up menu, **Organize** Ribbon group and **Clipboard** Ribbon group on the **Program** page.

Log View

The log is designed to store information on the events taking place during the program execution. The larger part of this information consists of events generated by the operations. The purpose of this chapter is to help you understand the log.
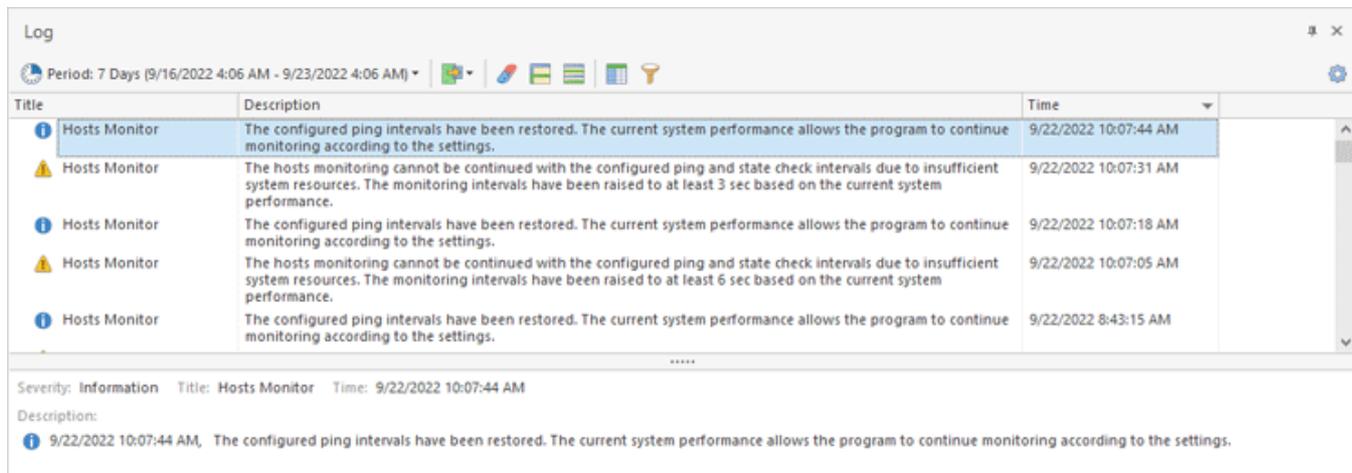
Pic 1. The Log view

The **Log** view is located by default at the bottom of the Ping Monitor main window and displays the log in form of a tree and a pane that shows details of a selected event **Pic 1**. The description for any logged event is by default wrapped, so that you can easily read it. If you would like to have more events visible at the same time, you can configure the **Log** view to display only one line per event by disabling the **Wrap Description** option from the **Advanced Options** menu, after which a detailed description will only be shown in the event details pane. If you do not need the event details pane and would like to review the events only within the tree, you can hide the event details pane by disabling the **Show Event Details Pane** option from the **Advanced Options** menu. Also, it is possible to enable the automatic scrolling feature to always see new log events as soon as they arrive, using the **Autoscroll** item from the **Advanced Options** menu.

The logged events are selected only for the specified period. This approach is used to optimize memory usage and performance as there may be lots of events in the entire database. The display range for events is by default set to the **7 Days** value and can be changed with the range drop-down button on the view toolbar. The text on the button shows you the currently applied range. You can choose between the predefined ranges or provide a custom one.

Every event in the log is assigned a severity level represented by a certain icon. The icon allows you to see if any problem has occurred without reading the description. The following icons are available:

🛈 - the blue icon with an 'i' character means that everything is OK;

🚫 - the brown circle icon with a cross-cut line is used to identify that the operation was canceled by user or due to shutdown of the underlying system;

⚠ - the yellow icon with an exclamation mark is the warning sign: it tells you that some errors have occurred, but they are not critical. In such a case, there is no guarantee that the operation has actually succeeded;

❌ - the red icon with a white cross is the error sign: it means that the operation execution has failed.

Analyzing the log can help you a lot in your everyday work with Ping Monitor, because it contains all the information on the executed tasks and provides you with troubleshooting recommendations in case any problems are detected.

Toolbar Overview

🕐 ▾	**Period** The **Period** button from the **Log** view toolbar allows you to choose the time interval to display the logged events for.
📤 ▾	**Export** The **Export** button should be used to export the log to a CSV file.
🧽	**Clear** The **Clear** button should be used to delete all the logged events from the program database.
🗒	**Full Expand** The **Full Expand** button from the **Log** view toolbar should be used to expand all nodes in the table of logged events.

	Full Collapse The **Full Collapse** button from the **Log** view toolbar should be used to collapse all nodes in the table of logged events.
	Choose Columns The **Choose Columns** button should be used to choose the columns to be displayed in the table of logged events.
	Filter Editor The **Filter Editor** button should be used to define the custom filter criteria to be applied to the data displayed within the table of logged events.
	Advanced Options The **Advanced Options** button enables you to configure the **Log** view, manage the visibility of the event details pane and reset the view layout.

The options of clearing the log, expanding nodes in the tree of logged events and collapsing them are also available from the pop-up menu of the Log view.

The layout of the **Log** view, including the visible columns, the column widths, the sorting settings, the descriptions wrapping and the details pane visibility, can be easily reset to the initial defaults by choosing the **Reset Layout** option from the view menu.

Access Control View

The **Access Control** view `Pic 1` is by default located at the bottom of the main program window.

> The Access Control view is available in the Enterprise Edition of the program only.

Its purpose is to define user roles and assign those roles to users and groups thus allowing granting or denying specific privileges to clients. For detailed information on configuring the privileges, refer to the **Access Control** section of this document.
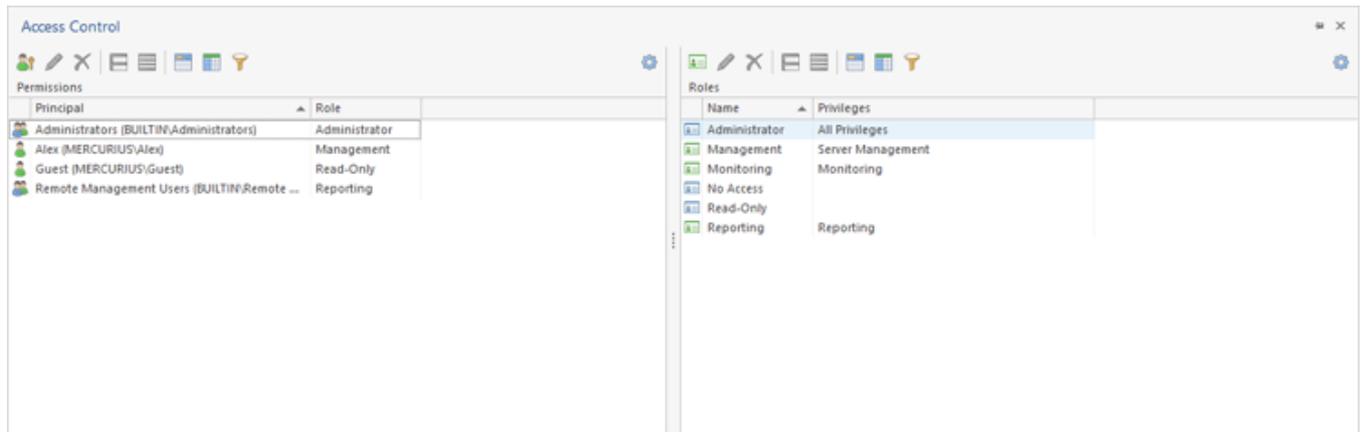
Pic 1. The Access Control view

The **Access Control** view is split in two parts, which are **Permissions** and **Roles**. Within the **Permissions** part, you can review and manage the currently effective associations between accounts and roles. The following icons are used within the **Permissions** group for displaying the type of the principal:

👤 - the role is assigned to a user;

👥 - the role is assigned to a group.

Toolbar Overview

👤	**Assign Permissions** The **Assign Permissions** button allows you to assign roles to users and groups thus defining their privileges when they access the Ping Monitor server.
✏	**Edit** The **Edit** button is used to reassign the access role for a selected user or group.
✗	**Delete** The **Delete** button allows you to delete the selected access role assignments.
▤	**Full Expand** The **Full Expand** button should be used to expand all the grouping rows in the table.
▤	**Full Collapse** The **Full Collapse** button should be used to collapse all the grouping rows in the table.

	Group By Box
	The **Group By Box** button should be used to configure the data grouping for the table.
	Choose Columns
	The **Choose Columns** button should be used to choose the columns to be displayed in the table.
	Filter Editor
	The **Filter Editor** button should be used to define the custom filter criteria to be applied to the data displayed within the table.
	Configuration
	The **Configuration** button provides access to the option of resetting the view layout.

The **Roles** part is used for reviewing and managing roles. For the **Roles** part, the following icons are used to define the type of the role:

- a build-in role;

- a user-defined role.

Toolbar Overview

	Add Role
	The **Add Role** button is used to create a new Ping Monitor server access role to be assigned to users and groups.
	Edit
	The **Edit** button allows you to change the name and/or the set of enabled privileges for the selected user-defined access role.
	Delete
	The **Delete** button is used to delete the selected user-defined access roles.
	Full Expand
	The **Full Expand** button should be used to expand all the grouping rows in the table.
	Full Collapse
	The **Full Collapse** button should be used to collapse all the grouping rows in the table.
	Group By Box
	The **Group By Box** button should be used to configure the data grouping for the table.
	Choose Columns
	The **Choose Columns** button should be used to choose the columns to be displayed in the table.

	Filter Editor
🔻	The **Filter Editor** button should be used to define the custom filter criteria to be applied to the data displayed within the table.
⚙	**Configuration**
	The **Configuration** button provides access to the option of resetting the view layout.

You can regroup the layout of this view any way you want it using the **Group Layout** item from the **Configuration** menu. Both parts of this view fully support all the grouping and filtering features.

Operations View

The **Operations** view `Pic 1` shows the detailed progress of each operation being performed at the moment and allows canceling a particular operation or all running operations. By default, it is located at the bottom of the Ping Monitor main window.
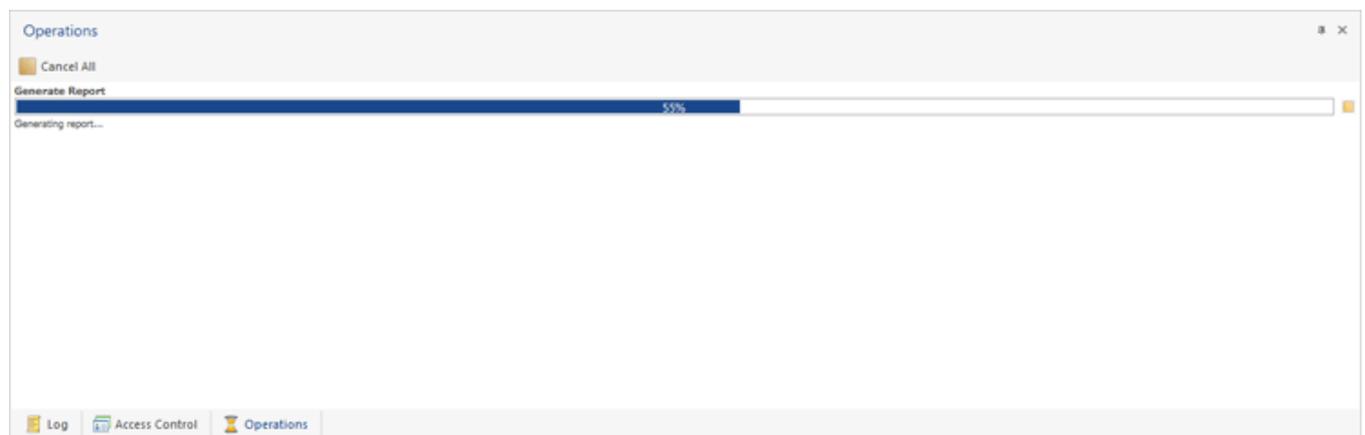
Pic 1. The Operations view

Progress information for every operation is shown in the pane with the progress bar, the operation information text and the **Cancel** button. The **Cancel** button is used to cancel individual running operations, whereas if the grouping operation is canceled, all the sub-operations are also canceled.

	Cancel All
🗔 Cancel All	The **Cancel All** button from the **Operations** view toolbar can be used to cancel all the operations running in the application.

You can cancel all the running operations by clicking the **Cancel All** button on the toolbar of the **Operations** view.

Graphical User Interface features

EMCO Software provides you with a modern and intuitive graphical user interface, because we appreciate the users of our products and would like them to feel glad that they have EMCO programs installed on their PCs. Lots of resources were involved in creating this kind of an interface for you, and now we are proud we have done it. Custom DPI settings are fully supported, so that you can use EMCO programs on any display with any resolution you like. The *'Microsoft User Interface Guidelines on Layout, Icons and Sizing'* have been a powerful base for this work, and we are glad to tell you that they are fully complied with and supported. With the help of the skinning support and the Ribbon UI interface, every customer can configure the program UI to feel comfortable during each working day. EMCO also provides you with the **High Contrast** skin along with the bonus skins pack, which is an accessibility feature designed for people with vision impairment. The High Contrast color scheme can increase legibility for some users by heightening the screen contrast with alternative color combinations.

This chapter gives you a detailed description of how to fully enjoy the graphical user interface features, the skinning mechanism and the Ribbon bar features.

Skinning

Ping Monitor provides you with a wide range of custom skins with unique look and feel, so that you can choose any skin you like most. If you are a fan of the Microsoft Office interface, you have no reason to complain either, since Ping Monitor also gives you an option of choosing this type of skin. There are not only formal skins but also some informal ones.

All the skins can be divided into four groups: Office Skins, Custom Design Skins, Bonus Skins and Skins for Fun. The following skins are available:

Office Skins:	"Office 2019", "Office 2019 Black", "Office 2019 Dark", "Office 2019 White", "Office 2016", "Office 2016 Dark", "Office 2016 Black", "Office 2013", "Office 2013 Silver", "Office 2013 Black".
Custom Design Skins:	"Bright Style", "Dark Style", "Blue Vision", "Blue Vision 2013", "Light Vision 2013", "Dark Vision 2013", "High Contrast", "Metropolis", "Metropolis Dark", "Seven", "Seven Classic", "McSkin", "Blue", "Black".
Bonus Skins:	"Lilian", "iMaginary", "Caramel", "Money Twins", "Sharp", "Sharp Plus", "Foggy", "Darkroom", "Dark Side", "Liquid Sky", "London Liquid Sky", "The Asphalt World", "Glass Oceans", "Stardust", "Coffee", "Blueprint", "Whiteprint".
Skins for Fun:	"Christmas", "Valentine", "Summer", "Springtime".

Let us take a brief look at some of the skins:

Default skin look and feel example
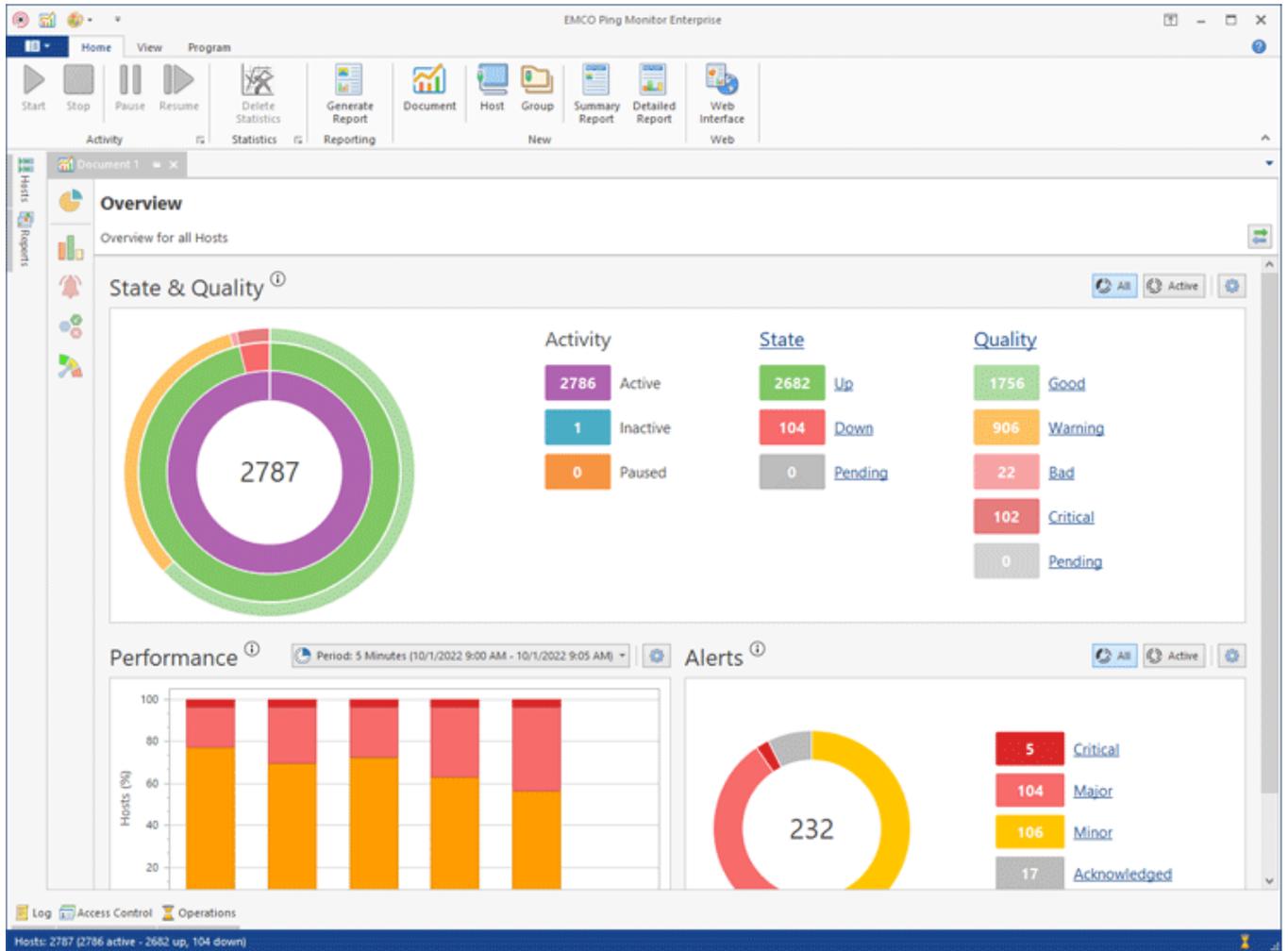
Custom Design Skin look and feel example
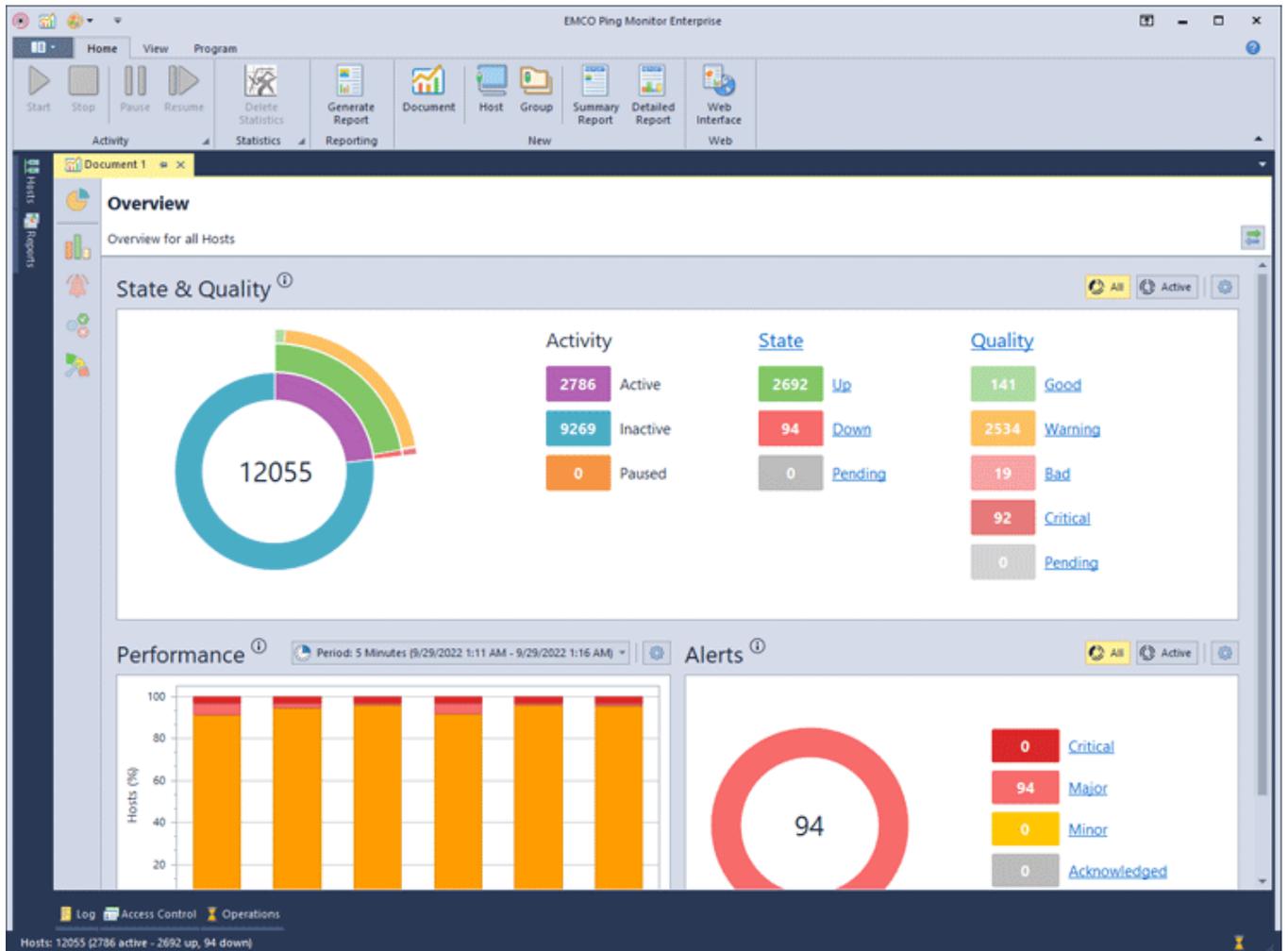
Skins for Fun look and feel example
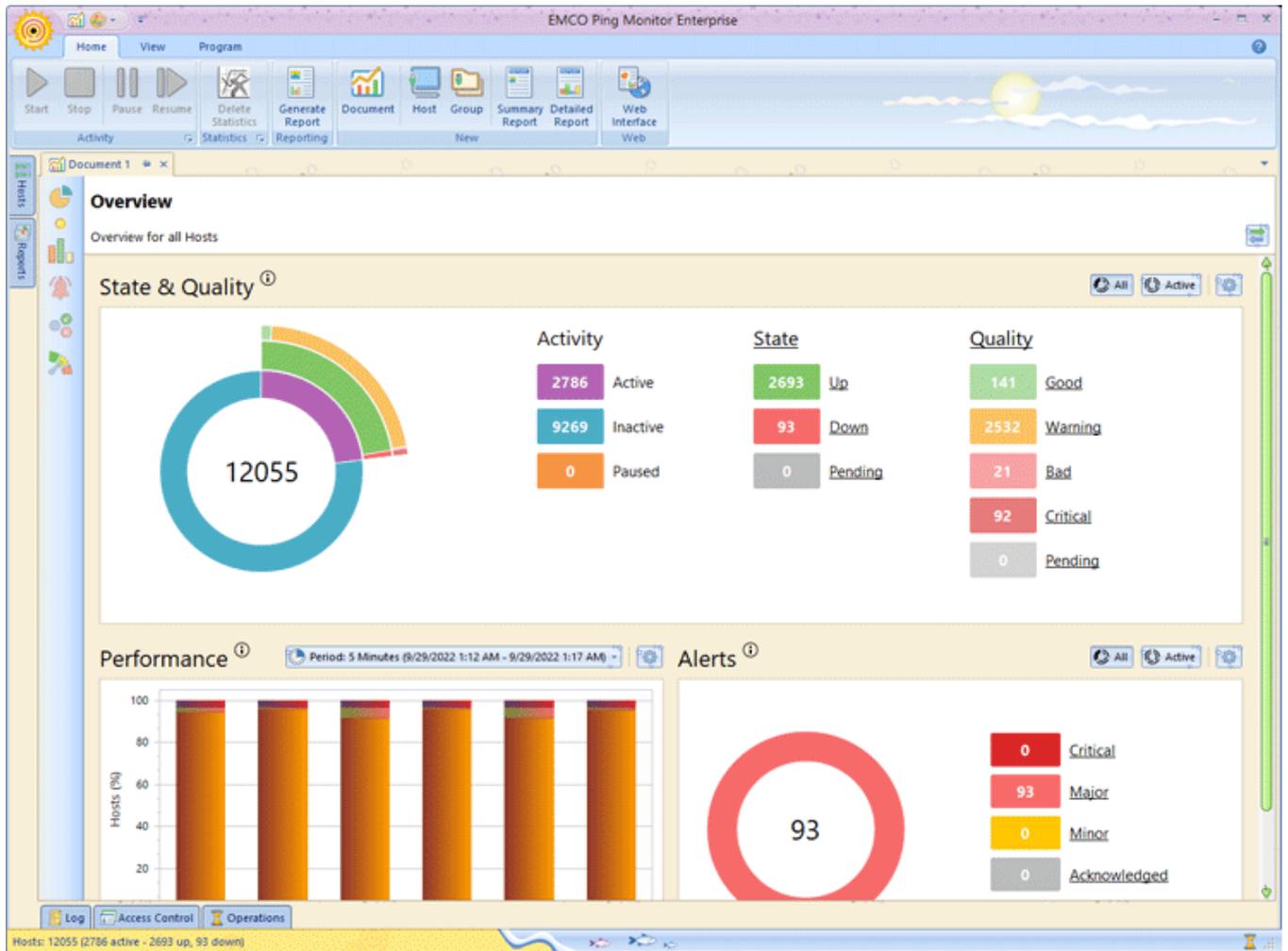
High Contrast Skin look and feel

Ribbon

Ribbon is a tool that presents commands organized into a set of tabs. The tabs on the Ribbon represent commands that are most relevant for each of the task areas in the program `Pic 1`. For example, in Office Word the tabs group commands by activities such as inserting objects like pictures and tables, doing page layout, working with preferences, doing mailings, and reviewing. The Home tab provides an easy access to the most frequently used commands. Office Excel has a similar set of tabs that make sense for spreadsheet work including tabs for working with formulas, managing data, and reviewing. Those tabs simplify access to the program features, because they organize the commands in a way that reflects the tasks people perform in those programs.

Pic 1. The Ribbon bar

We are delighted to let you know that we fully conform with *Microsoft® Ribbons Guidelines* and would like to introduce some Ribbon features to you. To learn more about Ribbon, the story of its development and its usability features, you may visit *'The Story of the Ribbon'* article from the MSDN blogs.

Application Menu

The **Application Menu** invoked using the **Application** button `Pic 2` is somewhat similar to the File menu in most programs that use a classic user interface, but it gives you more.
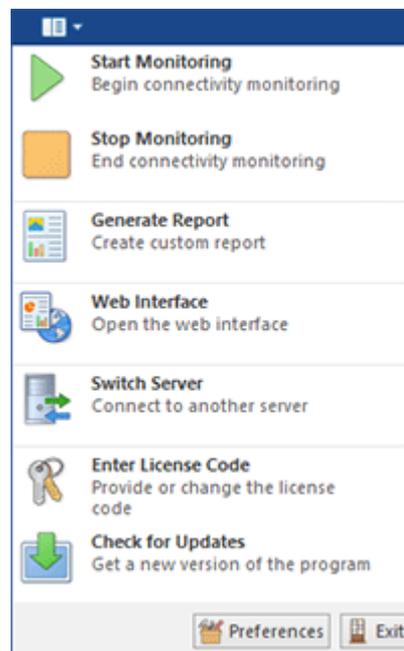
Pic 2. Application Menu

It contains links to the most helpful actions located under different tabs but made available from one access point.

Quick Access Toolbar

The **Quick Access Toolbar** `Pic 3` is an end-user customizable bar located near the **Application Menu** or below the Ribbon bar depending on the configuration. It can contain links to both Ribbon items and Ribbon groups.
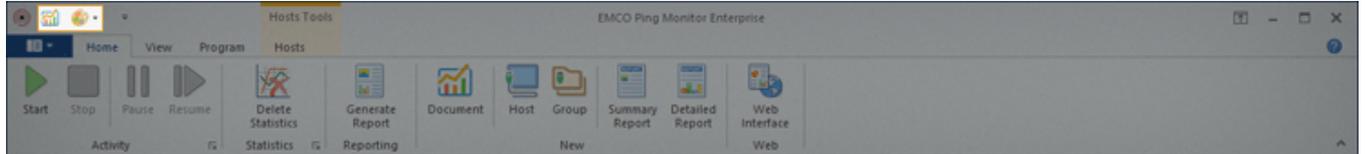
Pic 3. Quick Access Toolbar

To add an action link to the quick access toolbar, right click this action and select **Add to Quick Access Toolbar** from the pop-up menu. The groups can be added in the same way, the only difference being that to add a group you should right click its caption.

Representation and Navigation Features

The representation of the Ribbon bar can also be configured to make your work more comfortable. You can minimize Ribbon so that the tab's content is only shown when the tab is clicked on, thus extending the program workspace. Also, if it is not convenient for you to have the **Quick Access Toolbar** next to the **Application Menu**, you may place it below the Ribbon bar, so that it will look just like a simple toolbar. This configuration can be accessed from the pop-up menu of the Ribbon bar `Pic 4`.

Pic 4. The Ribbon customization menu

Navigation between the Ribbon tabs can be performed not only with a mouse click on a tab but also with the help of the mouse wheel. Just place the cursor over any tab and scroll the wheel – scrolling up will switch the tabs from right to left, and scrolling down will switch the tabs in the opposite direction.

Main features of UI Elements

The graphics shell used for Ping Monitor is aimed at providing a high level of usability to everyone. This topic covers main features of the graphical elements used in this program, and here you can find what puts EMCO GUI a step ahead of the others.

Docking

The Ping Monitor user interface is built using the ultimate docking technology which provides for the maximum use of the program working area. It allows docking the windows that are used less often than the main one to the sides, auto hide them or even close and then open again when required. The dock panels can be docked both to the main window and to each other, thus enabling you to build such a subsidiary window layout that makes you feel comfortable while working with Ping Monitor `Pic 1`.
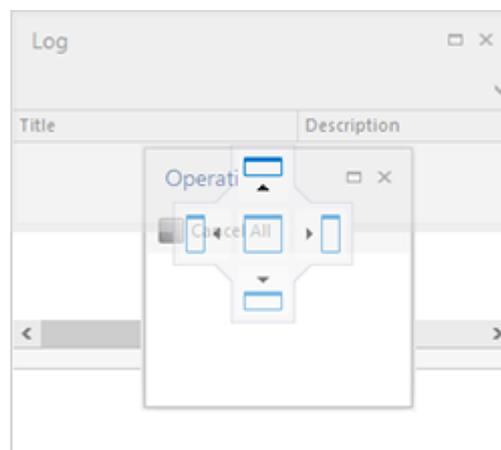
Pic 1. Docking preview

To change the position of any dock window, you should click its header and move the mouse pointer while holding the left mouse button down. Hint windows are shown to help you understand where you can drop the window dragged. When you are dragging it over another dock window, it is possible to dock both windows to each other or display them in different tabs of the same dock window. When a dock window is floating, you can expand it to full screen by either clicking the **Full Screen** button in the windows title bar or pressing **F11** on the keyboard. To exit the full screen mode, just press **F11**.

To enable the auto hide feature for a window attached to any side of a main window, click the pin button in the dock window header. Clicking the cross button results in closing of the dock window. Each view can also be closed and opened again using the checkboxes in the **Show** Ribbon group accessible from the **View** page.

Grouping and Filtering Data

The Ping Monitor user interface is designed so as to make its usage as flexible as possible. The tables available in every EMCO program provide you with an easy-to-use data filtration and grouping mechanism. To group data by one of the columns, you should drag its header to the grouping box displayed over the table or choose an appropriate item from the column header pop-up menu `Pic 2`.
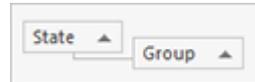
Pic 2. The grouping box of a table grouped by two columns

To group or ungroup data by any column when **Group By Box** `Pic 2` is not visible, you can have it displayed by selecting the **Show Group By Box** item from the pop-up menu of any column header.

Data filtration can be performed in two ways: by using the quick filter or the filter editor. To use the quick filter feature, just click on the glyph in the right top corner of any column header. A drop-down list appears offering you to choose one of the predefined filters or select the custom one from the filtering dialog `Pic 3`.
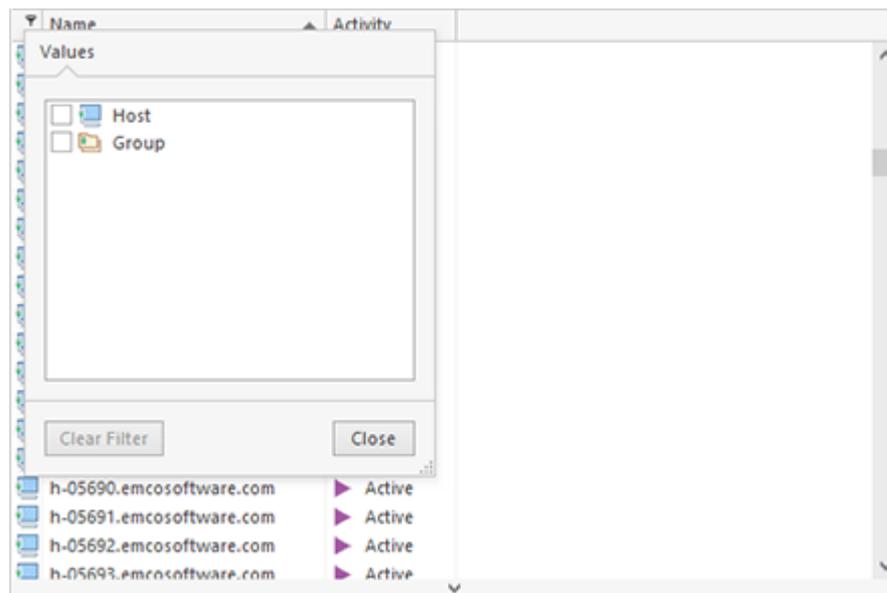
Pic 3. Accessing the quick filter abilities

The **Filter Editor** shipped with Ping Monitor is easy to use and allows you to build your own complex filters quickly and easily `Pic 4`. To open the filter editor, choose the **Filter Editor** item from the column's pop-up menu.
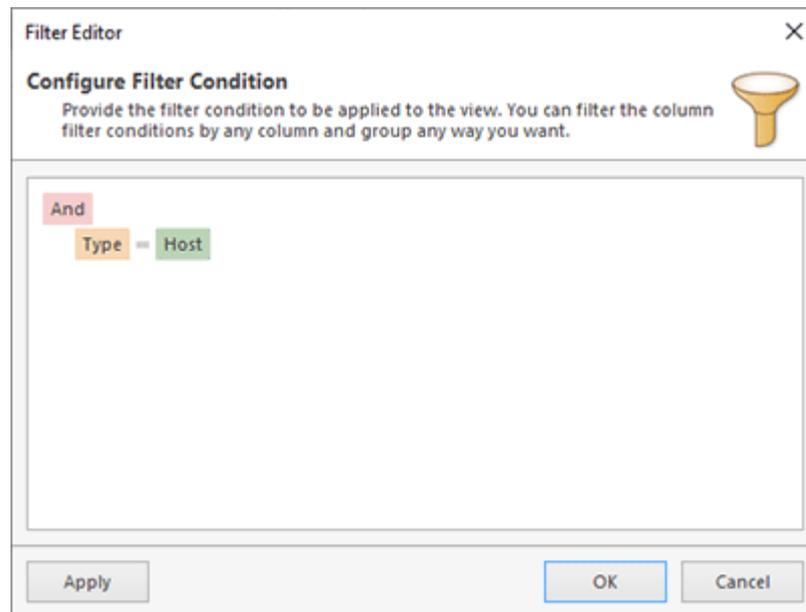
Pic 4. Using the filter editor

You can enable and disable the currently applied filter condition using the checkbox displayed next to the filter condition in the bottom of the view, inside the filter info pane `Pic 5`.
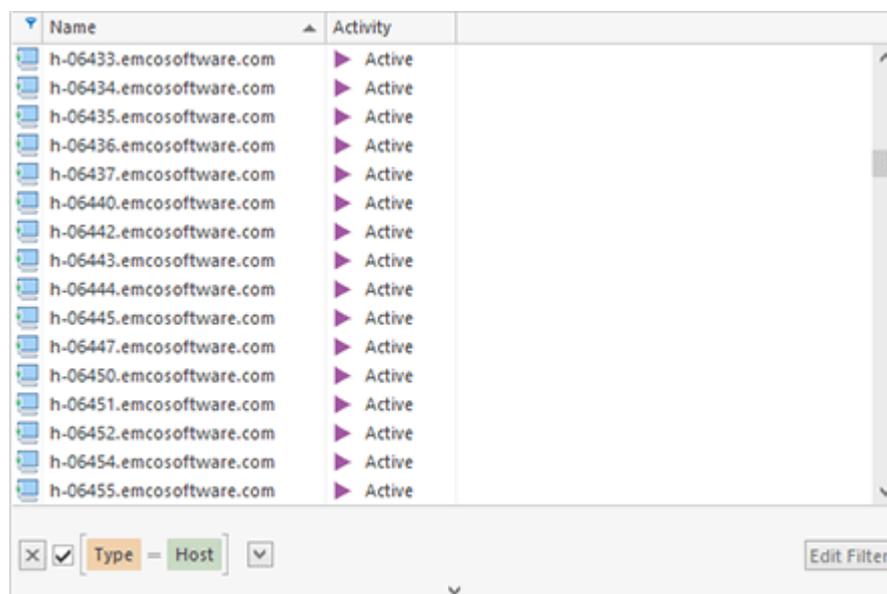
Pic 5. The filter info pane

To reset the currently applied filter use the ⊠ button from the filter info pane, and to customize it use the **Edit Filter** button from this pane.

108

Managing Columns in Trees and Tables

You can customize almost every table and tree in EMCO programs by moving and removing columns to make the control most informative for you. To move a column, drag it over the control's header and drop between other columns to its new position `Pic 6`.
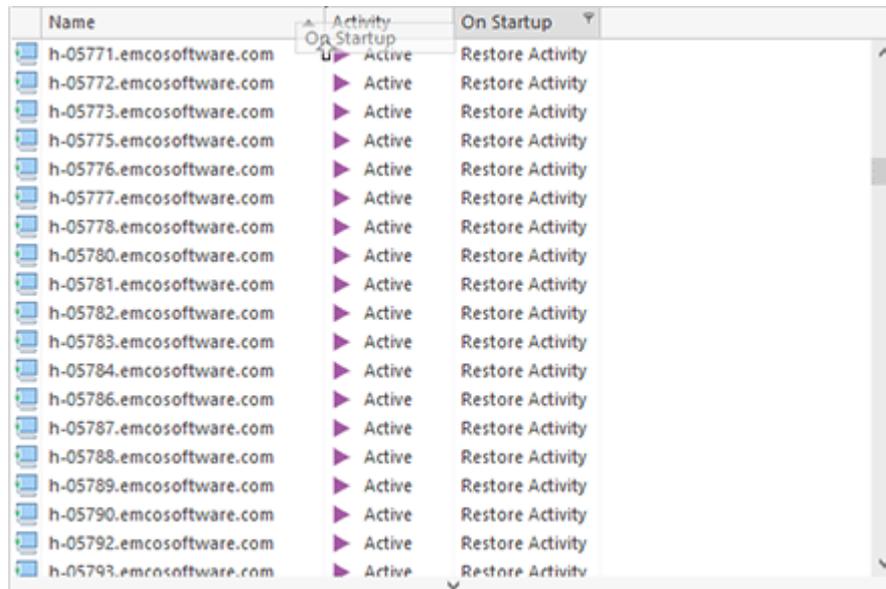
Pic 6. Moving a column

To remove a column that is of no use for you, right click the control's header and select the **Remove This Column** item from the pop-up menu. Also, you can control columns availability using the column chooser `Pic 7`.
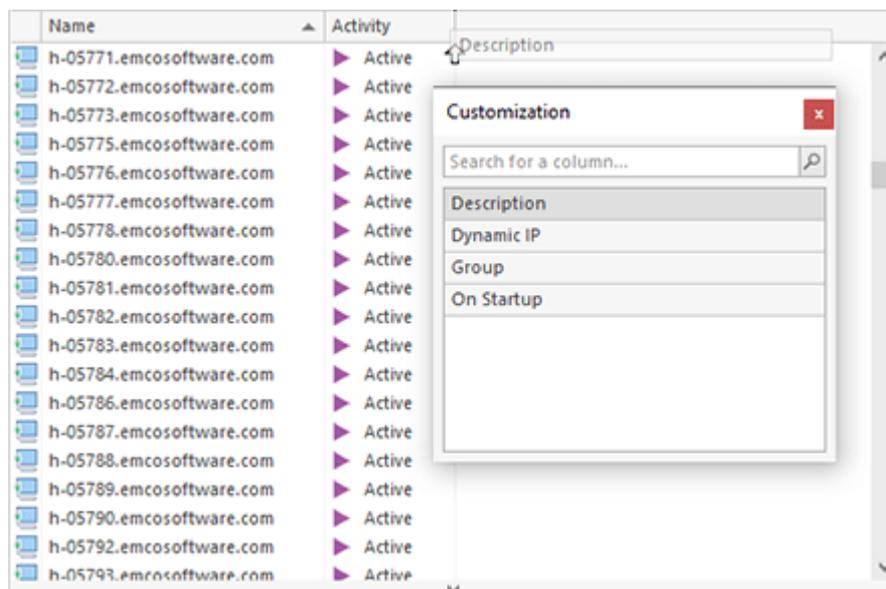
Pic 7. Using the column chooser

To show the column chooser, right click the control's header and select the **Column Chooser** menu item. After that, you can drag and drop columns from the header to the column chooser and backwards.

Automatic Saving and Restoring of Windows Layout

One of the service functions of Ping Monitor user interface is its ability to save and restore the windows layout. All the changeable parameters like the windows sizes and positions; the table columns order, sizes and positions; the grouping and filtering options; the dock windows configuration, etc. are saved between sessions. Thus, you do not need to configure the program's user interface layout every time you start this program.

Chapter 4: Hosts Management

Ping Monitor is a tool for monitoring the hosts connectivity. So the primary object in the program is the one that represents the remote host in the program, it is also called a host. All hosts can be grouped via host groups. A group, for instance, allows you to add a single unit as a report member, adding a group reference, and change a set of hosts included into the report by simply changing a set of group members. Also the group allows you to define custom settings to be applied for all hosts in it during the monitoring, unless the settings are overridden on a host itself. See the **Overriding Common Settings** section of this document for details.

The host is used as a master object for all data gathered by the program. It means that the gathered data is connected to a host, which allows to maintain the host monitoring statistics and to create statistical reports for specific date intervals. The most part of the monitoring data for the host is stored until deleted by the user or until the host is deleted. The historical data can also be deleted automatically when treated as outdated – this option is available for configuration in the program preferences.

All the hosts are displayed in the **Hosts** view. In this chapter we will take a closer look on the process of defining the hosts and groups of hosts, configuring them for monitoring, changing hosts configuration, deleting hosts or groups, integrating with external tools and at the process of hosts import and export.

Defining Hosts and Groups

The hosts are displayed in the **Hosts** view either in the hierarchical or in the flat form, depending on the view configuration. In this chapter, we will describe how to create hosts and groups, configure them for monitoring and delete them when they are no longer needed.

Host	**Host**
	The **Host** button from the **New** Ribbon group on the **Home** page and on the **Hosts** page from the **Hosts Tools** category should be used to add a new host or a range of hosts to be monitored.

To create a new host or a group of hosts from an IP range, you should press the **Host** button from the **New** group on the **Home** Ribbon page or on the **Hosts** page from the **Hosts Tools** category. Alternatively, you can use the **New > Host** routine from the **Hosts Browser** view toolbar and pop-up menu. In any case, the dialog will appear on the screen to help you with the creation process Pic 1.
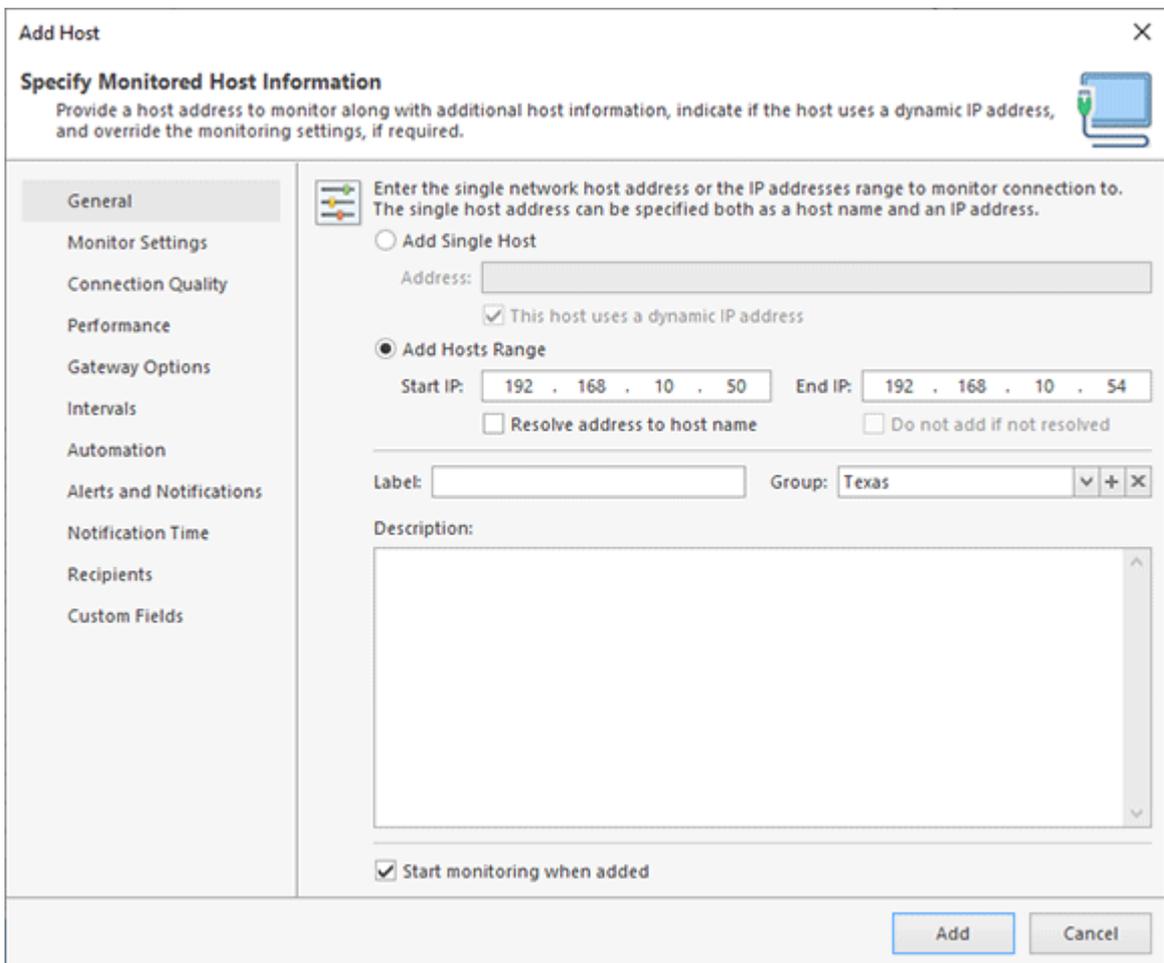
Pic 1. Adding a host or a range of hosts

In the **Add Host** dialog, you should first choose if you would like to add a single host or a range of hosts by specifying their IP addresses. If you would like to add a single host, leave the **Add Single Host** radio button chosen, enter the host address into the **Address** field and indicate if this host uses a dynamic IP address. In case of adding a range of hosts, you should provide the start and end IP addresses for the range. To perform the name resolution from IP addresses to host names when adding a range of hosts, you should check the **Resolve address to host name** option. If the host names resolution is enabled, you can specify if the hosts whose names cannot be resolved should be added to the monitoring data or not by using the **Do not add if not resolved** option.

The **Label** and **Description** fields can be used for easier host identification, and the **Group** field allows you to select the group this host belongs to. Also, you can provide additional configuration settings using appropriate tabs of the **Add Host** dialog.

On the **Custom Fields** page, you can provide values for a set of custom fields defined in the program preferences. Custom fields can be displayed in the **Hosts** view when corresponding columns are added. Custom fields can be used also within notifications and when integrating with external tools.

If you do not want the monitoring process to start automatically for hosts being added, uncheck the **Start monitoring when added** box. When you are done with providing the required information, press **Add** for the host or the hosts to be created. The created hosts will be automatically included into the auto-start list.

Group

The **Group** button from the **New** Ribbon group on the **Home** page and on the **Hosts** page from the **Hosts Tools** category allows you to create a new hosts group.

To create a new group of hosts, you should use the **Group** button from the **New** Ribbon group on the **Home** page or on the **Hosts** page from the **Hosts Tools** category. Alternatively you can use the **Group** item from the **New** button pop-up on the **Hosts** view toolbar and the appropriate item in the view pop-up menu. The **Add Group** dialog will appear on the screen to configure the group being created `Pic 2`.

Pic 2. Creating a group of hosts

When creating a group you are proposed to define the group name and description as well as the set of hosts and groups to be included into a group being created. The name and description are used to make it easier for you to identify the group being created in the future. To add a host or a group to the group being created use the **Add** button from the members tree toolbar or choose an appropriate item from the pop-up menu. The dialog will be displayed to let you choose the hosts and groups to be added. Those items that are already in the group being created are filtered from those available. The **Delete** button and menu item are used to remove the selected hosts and groups from the group being created. When configuring a group, it is also possible to provide the settings to be applied to hosts within the group, unless overridden, on the corresponding tabs. As soon as the group is configured, press **Add** to create it.

To edit any host or group, select it and either choose the Edit button from the **Organize** Ribbon group on the **Program** page or use the **Edit** items from the view toolbar and pop-up menu. The editing process is similar to the creation. When some hosts or groups are no longer needed you can delete them using either the **Delete** button from the **Organize** Ribbon group on the **Program** page or use the **Delete** items from the view toolbar and pop-up menu. When you are deleting hosts and groups they are also deleted from all groups and reports they are currently included into.

Within the **Hosts** view it is also possible to copy and move hosts and groups between other groups as well as create their duplicates. This can be done either via the drag and drop technique, or via the copy/paste one. The **Cut**, **Copy**, and **Paste** items from the **Clipboard** Ribbon group on the **Program** page can be used, as well as the appropriate items from the pop-up menu. It is also possible to copy hosts and groups between different editions of the program and use the export feature. For the details on import and export, refer to the Importing and Exporting Hosts section of this document.

Overriding Common Settings

Ping Monitor comes with a wide range of monitoring and notification options those are defined in the program preferences. The options defined in preferences are initially used for all monitored hosts, but you can override specific groups of options for particular hosts or groups of hosts.

> It is possible to override common settings when using the Enterprise or Professional editions of the program. The Free edition doesn't allow overriding common settings and specifying custom settings for hosts and groups.

When an options value for a host is calculated, first it checks if it is overridden on a host itself and on any of the parent groups. In case it is overridden on any level, than the overridden value is used, otherwise the value from program preferences is taken into account.

The overriding features are available during the hosts and groups addition and modification. The options are gathered on the corresponding navigator pages of the configuration dialog, those are:

Monitor Settings, **Connection Quality**, **Performance**, **Gateway Options**, **Intervals**, **Automation**, **Alerts and Notifications, Notification Time, Recipients** and **Custom Fields**.

For example, to override the monitoring settings, you should check the **Override ping options configuration** box on the **Monitoring** page, and then perform the required changes. Changing the common configuration, either from preferences or from the parent group, can be reached via the **Change common/parent configuration** link. To reset the settings to common, you can use the **Reset to common/parent** link. As you can see, the approach is easy and can be used to reach maximum flexibility of the monitoring process configuration.

Using Custom Fields

Using custom fields you can specify additional characteristics of hosts that can be used in various of cases. For example, you can specify a geographical location of the host, a name of the responsible person or a room number where a host is located. Custom fields can be displayed for a host together with other characteristics, so you can search, group and filter hosts by custom fields and use custom fields in notifications and custom actions.

To start using custom fields you need to specify a set of custom fields in the **Custom Fields** section of the program preferences Pic 1 . You can add one or multiple fields according to your needs. You can add fields by specifying a custom field name only, or specify a custom field name and its value. Custom fields specified in preferences are automatically set to all hosts.
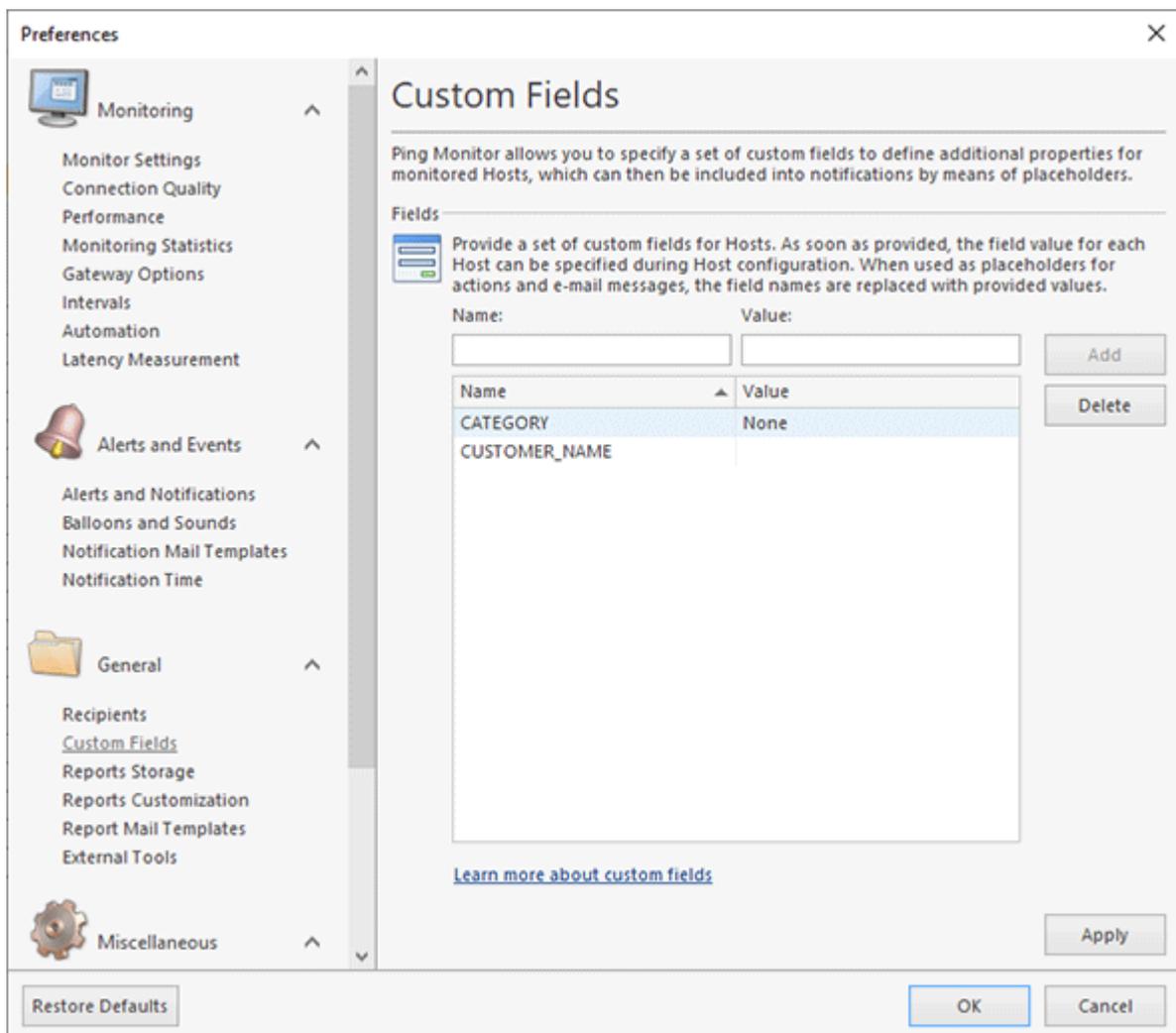
Pic 1. Custom fields specification in Preferences

If you plan to set different custom fields values for hosts, you can specify custom fields names only in the program preferences and set custom fields values for hosts. To do that you need to create a new host or edit an existing host. Open **Custom Fields** in the host settings and turn on the **Override configuration** option. Now you can set custom values for the fields for this particular host `Pic 2`.
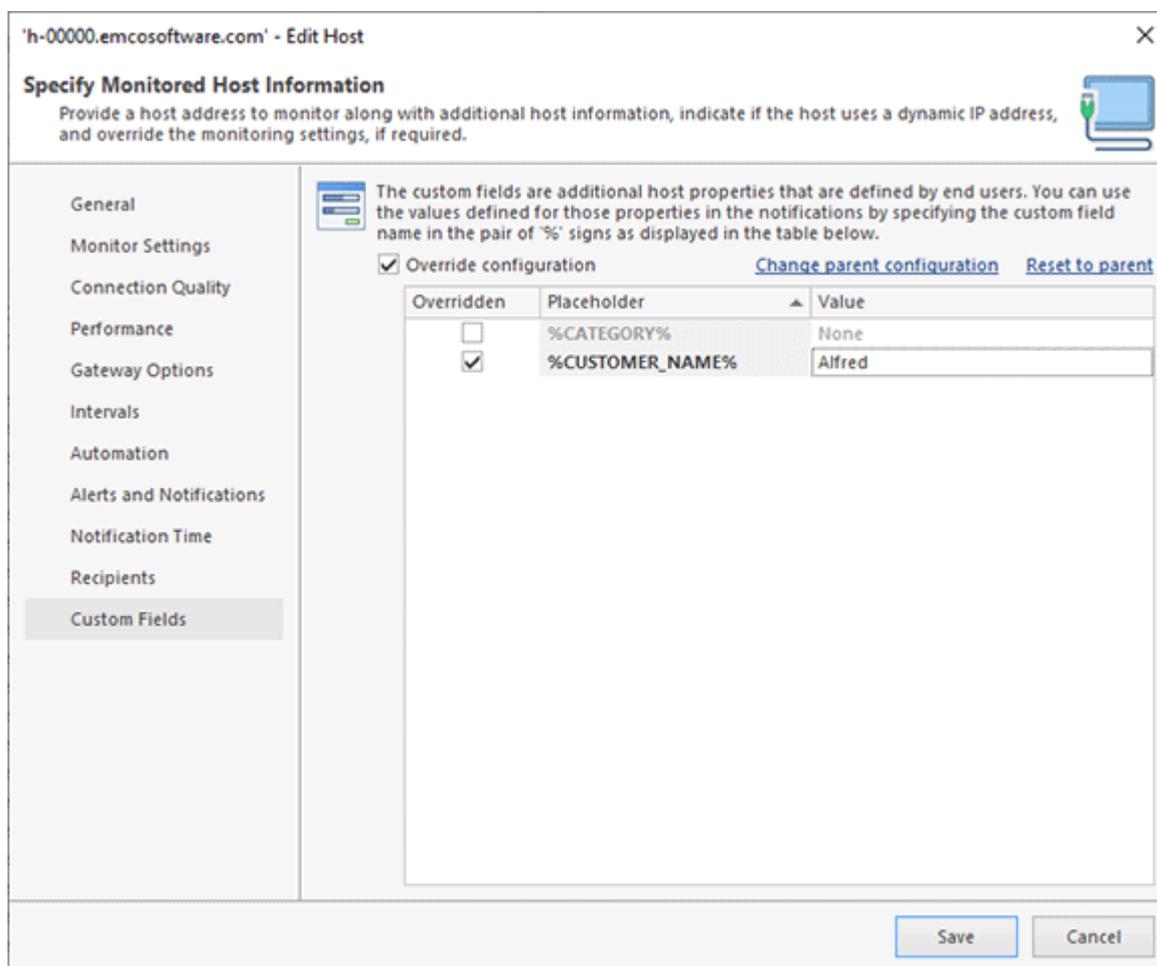
Pic 2. Specifying a value for the custom fields of a specific host

Once custom values are set for the hosts, you can start using them in the program. For example, you can display custom fields in the **Hosts** view. To do that you can right-click the **Hosts** table header and select the **Choose Columns** in the content menu. In the displayed dialog you can see the added custom fields, so you can click them to add to the hosts table. Now you can use the standard grouping, filtering and sorting features available in the table to organize hosts by custom fields.

You can use custom fields in notifications and custom actions where custom fields are available as placeholders. Edit **Notification Mail Templates** or configure a **Custom Actions** where you can use configured custom fields.

Integrating External Tools

Ping Monitor allows you to launch external tools directly from the **Hosts** view, providing host properties as the command line parameters. The options are available in the **External Tools** submenu of the **Hosts** view pop-up menu when a single host is selected. The program comes with a built-in set of predefined tools that allow you to open remote desktop connection to the host, view the hosted web-site in a browser, launch console utilities, such a ping and tracert. You can disable predefined tools and add you custom ones on the **External Tools** preference page, which can be also reached directly from the menu when choosing the **Configure External Tools** option. Please note, that the external tools are launched on the client side, i.e. on the PC where the Ping Monitor client is running.

Importing and Exporting Hosts

With Ping Monitor, you can easily import and export hosts information any time you want. You can export one or all of the available hosts and groups to use the exported data as a back-up, to share the hosts with your colleagues or simply to import them to another instance of the program. The import feature can be used to import hosts information both from the files created during export and those created manually. For example, you can create a CSV file manually to add multiple hosts by adding their data in Microsoft Office Excel. To get detailed information on the file formats used for import and export, review the Export/Import Formats section. This chapter covers the process of importing and exporting host information.

Import

The **Import** button from the **Organize** Ribbon group on the **Program** page should be used to import hosts information from an XML or CSV file with the help of the wizard.

The hosts information can be imported into Ping Monitor from XML and CSV files. The XML file structure is quite complex, so it is not recommended to create it manually, but it is recommended to use it for export. The CSV file should consist of five columns: the host address, the label, the indication if the host uses a dynamic IP, the group and the description - each column should be separated with the field delimiter. The CSV file can be created manually to be able to add multiple hosts to Ping Monitor easily.

If you want to import the hosts information into Ping Monitor, press the **Import** button from **Organize** Ribbon group on the **Program** page. The **Import Hosts Wizard** will appear on the screen Pic 1.
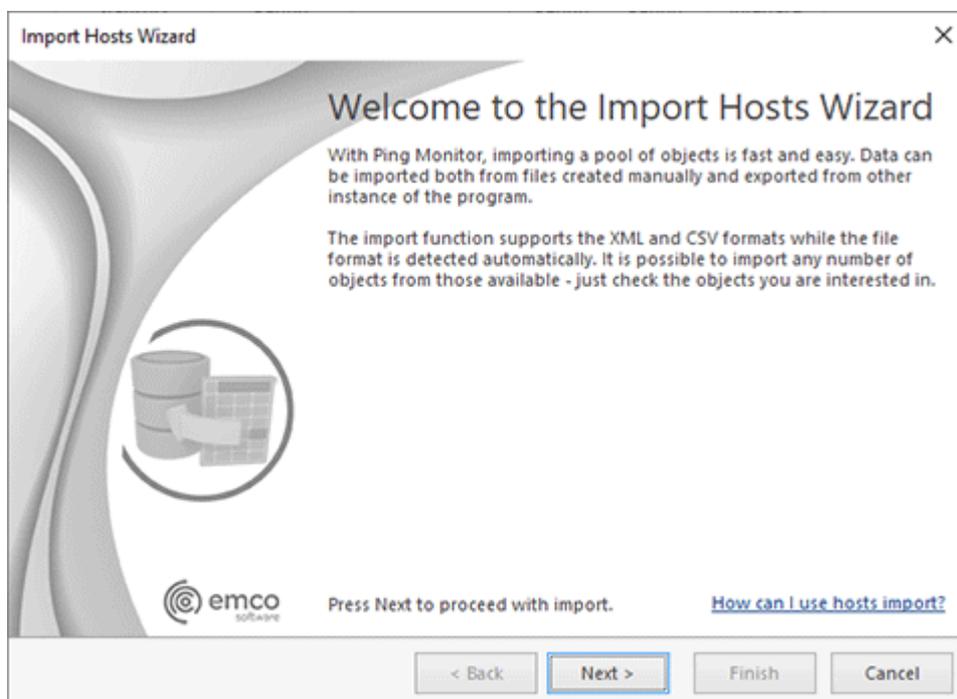
Pic 1. The Import Hosts Wizard welcome page

The first page of the **Import Hosts Wizard** is the welcome page, which is used to introduce you to the feature the wizard is supposed to help you with. After reading the welcome information, press **Next** to continue with import.

On the next page of the **Import Hosts Wizard**, you are offered to choose the file you are going to import hosts information from. The file path should be provided in the **Import** From field `Pic 2`. The format of the provided file is detected automatically. The encoding of the XML file with hosts information is also detected automatically. For the CSV format, the preview page is displayed, where you can tune the parse options, being able to preview the parsing results.
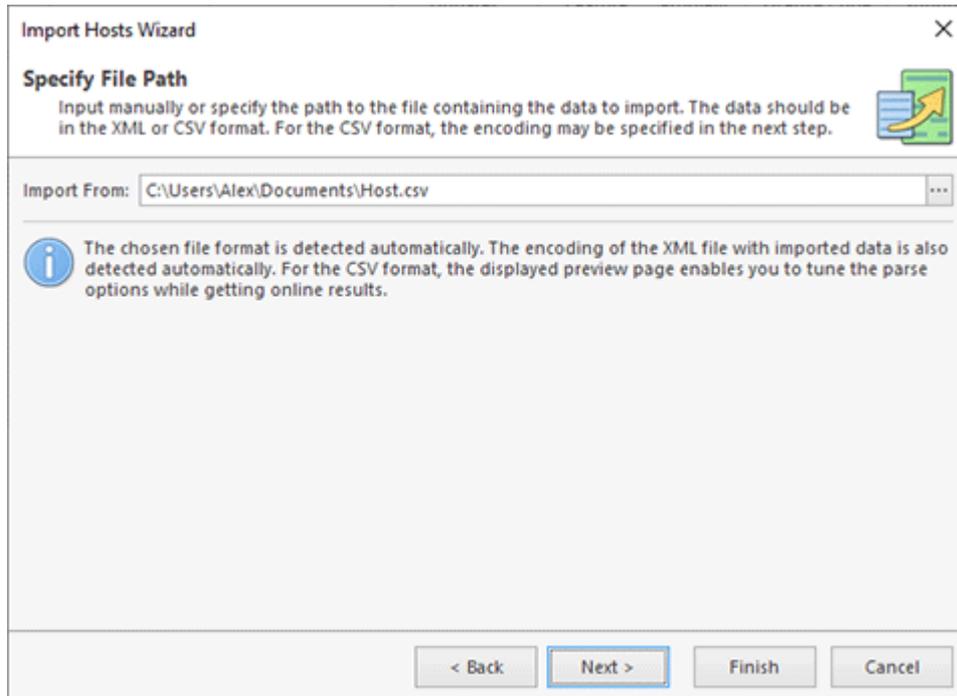
Pic 2. Choosing the import source file

The next page offers you to choose the hosts to import. By default, all the valid hosts that does not duplicate already existing addresses are selected **Pic 3**. Optionally, you can specify if the monitoring for new hosts should be started as soon as the hosts are added.
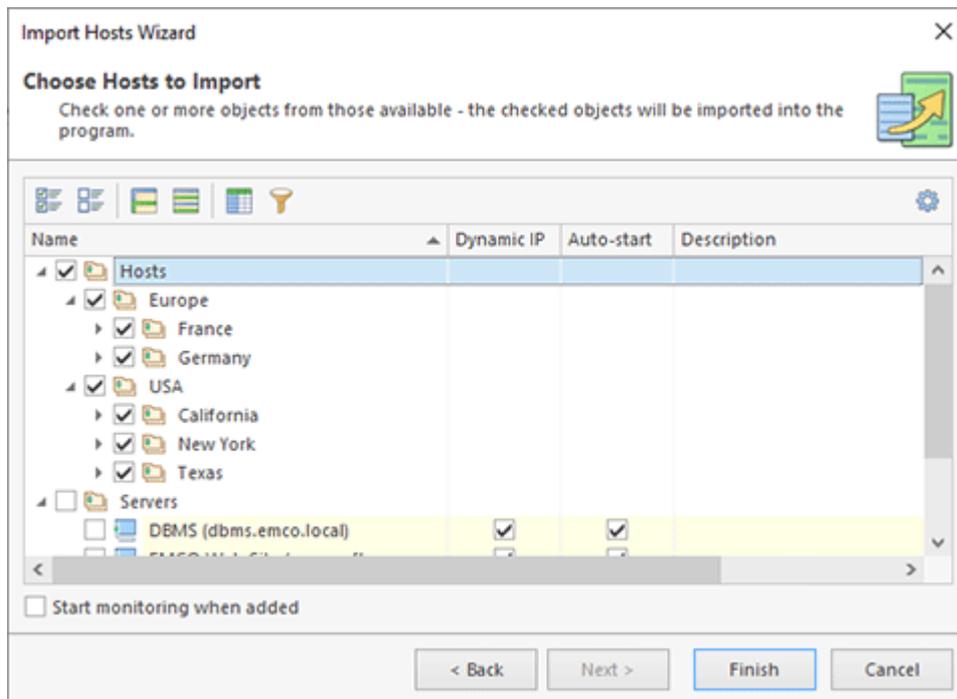
Pic 3. Choosing the hosts to import

When the hosts to import have been chosen, press **Finish**. When the import is done, the hosts are added the program thus can be monitored.

Export

The **Export** button from the **Organize** Ribbon group on the **Program** page should be used to export hosts and/or groups of hosts from the program to an XML or CSV file that can be used in the future for import.

The hosts' information can be exported to the XML or CSV file format. The overridden settings are saved only into an XML format file. The hosts export can be performed either from the **Hosts Browser** or from the **Hosts** view. You can choose between exporting all objects and those that are currently selected. To perform export, use an appropriate option from the drop-down of the **Export** button from the **Organize** Ribbon group on the **Program** page. The **Export Hosts Wizard** will appear on the screen `Pic 4`.

Pic 4. The Export Hosts Wizard welcome page

The first page of the **Export Hosts Wizard** is the welcome page, which is used to introduce you to the feature the wizard is supposed to help you with. After reading the welcome information, press **Next** to continue with export.

On the next page you are offered to choose the file you are going to save the hosts information to, the file format and the format options. The file path should be provided in the **Export To** field Pic 5 . For the XML format, you can choose the encoding to be used for saving the host information, and for the CSV file, the field delimiter and the text qualifier should be specified together with the encoding. When exporting to the CSV file format, you can also define if you would like the column headers to be preserved in the resulting file, which can make it easier for you to identify each column – this feature can be enabled using the **Include column header** option.
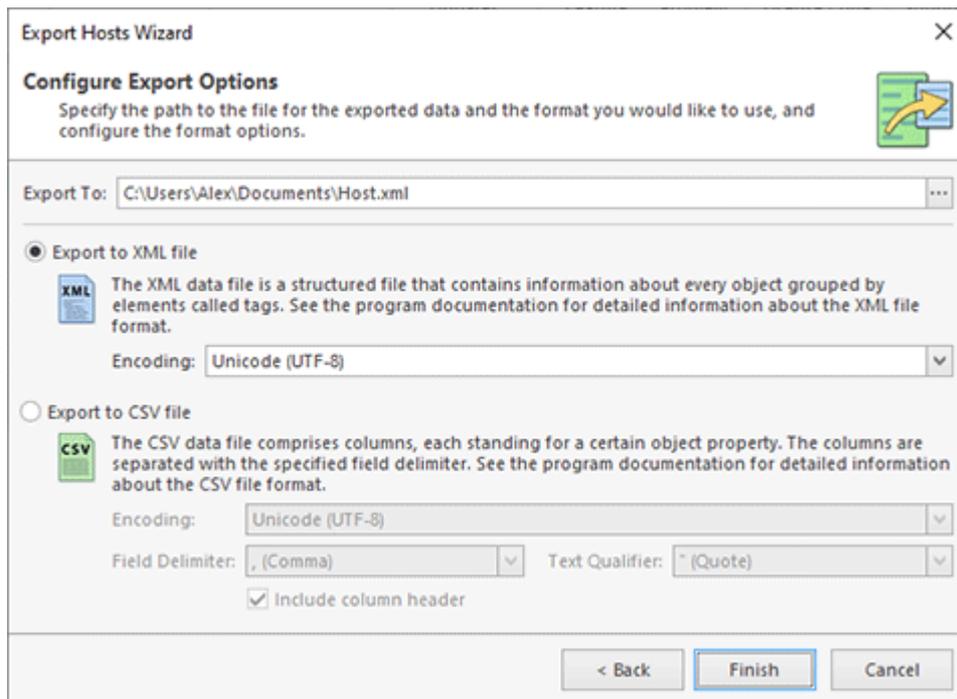
Pic 5. Configuring export options

When the file path and the export form are chosen, press **Finish** to proceed with export. The file containing the hosts' information will be created in the location according to the path specified. The file created during export can be used in the future to import the hosts' information back to the program.

Now you are fully introduced to the export and import capabilities of Ping Monitor and can use them in future to solve your tasks.

Export/Import Formats

This section describes the file formats used by Ping Monitor during hosts import and export. The available formats are CSV and XML. The CSV format file consists of five columns, namely:

Index	Header	Description	Mandatory
1	Address	The host name or IP address.	Yes
2	Label	The label used for the host.	No

Index	Header	Description	Mandatory
3	DynamicIP	The indication that the host uses a dynamic IP address. 'yes' should be used if the IP address is dynamic, otherwise use 'no'.	No
4	Group	The group the host belongs to.	No
5	Description	The description used for the host.	No

Sampe CSV file

"Address","Label","DynamicIP","Group","Description","QuickLaunch"

"h-00001.emcosoftware.com",,"yes","Hosts\USA\California",,"yes"

"h-00002.emcosoftware.com",,"yes","Hosts\USA\California",,"yes"

"h-00003.emcosoftware.com",,"yes","Hosts\USA\California",,"yes"

"h-00004.emcosoftware.com",,"yes","Hosts\USA\California",,"yes"

"h-00005.emcosoftware.com",,"yes","Hosts\USA\California",,"yes"

"h-00006.emcosoftware.com",,"yes","Hosts\USA\California",,"yes"

The host and groups in the XML file are hierarchically structured. Each item is represented with the **Entry** node, which has its **Type** attribute set either to **Group** or to **Host**. The other attributes are the following.

Attribute	Description	Mandatory
The following attributes are used for the Host entry type.		
Address	The host name or IP address.	Yes
Label	The label used for the host.	No
DynamicIP	The indication that the host uses a dynamic IP address. 'True' should be used if the IP address is dynamic, otherwise use 'False'.	No
The following attributes are used for the Group entry type.		
Name	The name of the hosts group.	Yes
The following attributes are used for both the Host and the Group entry types.		
GUID	The unique item identifier in the database.	Yes
Description	The description used for the item.	No
Settings	Overridden monitoring process settings applied to this item in the XML format.	No

Sampe XML file

<?xml version="1.0" encoding="utf-8"?>

<Data Version="3" Format="Hosts">

  <Entry Type="Group" GUID="95ed6793-f3f8-4820-ad73-c504bd00b1c6" Name="Hosts">

    <Entry Type="Group" GUID="323bde41-118f-4e97-ae4b-641d5c94db56" Name="USA">

```
<Entry Type="Group" GUID="e08465bf-6df2-4d3e-aa46-70db5f71610b" Name="California">

        <Entry Type="Host" GUID="2f56be60-272a-4549-b152-542c5a90d15a" Address="h-
00001.emcosoftware.com" DynamicIP="yes" QuickLaunch="yes" Settings="" />

        <Entry Type="Host" GUID="47d47b21-f3cf-44be-8056-673d134fc40c" Address="h-
00002.emcosoftware.com" DynamicIP="yes" QuickLaunch="yes" Settings="" />

        <Entry Type="Host" GUID="5ea43d1e-c276-4705-a577-90217f734aaf" Address="h-
00005.emcosoftware.com" DynamicIP="yes" QuickLaunch="yes" Settings="" />

    </Entry>

  </Entry>

 </Entry>

 <Entry Type="Group" GUID="46678cbc-43e2-4a8f-9266-d02061919af6" Name="Texas">

        <Entry Type="Host" GUID="bdb50796-d206-4092-99ad-23c1890d861a" Address="h-
00111.emcosoftware.com" DynamicIP="yes" QuickLaunch="yes" Settings="" />

        <Entry Type="Host" GUID="b8d3110c-32c2-4646-84c6-9eff75fa3045" Address="h-
00114.emcosoftware.com" DynamicIP="yes" QuickLaunch="yes" Settings="" />

        <Entry Type="Host" GUID="53c88234-2b91-4b38-a5a9-424a5ad7bf1b" Address="h-
00115.emcosoftware.com" DynamicIP="yes" QuickLaunch="yes" Settings="" />

  </Entry>

</Data>
```

Now you are introduced to the formats used for storing the hosts information and can prepare the files to be used for export manually or edit the data exported earlier to be used for future imports.

Chapter 5: Monitoring Connectivity

The main goal of Ping Monitor is to provide you with easy-to-use connection monitoring features. After you have added and configured the hosts to monitor, you are ready to start the monitoring process. As soon as the process is started, the program checks for the host state and connection quality changes using the options defined on the **Monitoring Settings** and **Connection Quality** preference pages. During this process the monitoring statistics is gathered by the program, to allow you review the overall monitoring statistics for each host and build performance and availability reports for required periods of time. The mentioned reports are covered in details in the **Reporting** section of this document.

The monitoring process for each host can either be inactive, active or paused. The activity can be either controlled manually or by the program taking into account the automation and monitoring intervals options defined in the program preferences and per host. While the monitoring process is paused, the ping packets are not sent to the remote hosts and the ping statistics stays the same until the monitoring process is resumed.

The monitored host can be in one of three states, those are: **Up**, **Down** and **Pending**. For the details on state monitoring, please refer the Host State Monitoring section of this document. Along with the host state, Ping Monitor monitors the connection quality. The available qualities are **Good**, **Warning**, **Bad**, **Critical** and **Pending**. The Connection Quality Monitoring section covers the process of monitoring a connection quality.

Ping Monitor can alert you on the hosts state or connection quality changes via e-mail, balloon or sounds. Also it is possible to trigger custom actions on hosts state or connection quality changes. The program alerts and notifications can be configured on the **Alerts and Notifications** preference page. You can choose which notification is enabled for each trigger and specify the delay for each action, if required.

In this chapter we will go through all the aspects of monitoring activity management and describe the statistics gathered during hosts monitoring in details.

Controlling Activity

Ping Monitor is used to check the remote host state and connection quality and notify the user on changes. The state and connection quality checks are performed only when the monitoring process is active. The monitoring process can be activated either automatically on the server startup, if this is enabled on the **Automation** preference page, or manually. Then the process can be either paused or stopped both automatically and manually. This chapter will show you how to control the monitoring process activity.

	Start The **Start** button from the **Activity** Ribbon group on the **Home** page should be used to start monitoring for the currently selected hosts.

The monitoring process can be activated automatically on startup in two cases: either the host monitoring was active at the end of the previous session and it is configured to restore activity for hosts or the host is included in auto-start and it is configured to start monitoring for such hosts.

To start a monitoring manually for specific hosts, you can select those hosts in the **Hosts** view and press the **Start** button on the **Activity** Ribbon group located on the **Home** page. You can also start monitoring by clicking the **Start Monitoring** item in the pop-up menu or the **Start** item on the **Manage Activity** button drop-down available on the toolbar. The **Statistics** view can be used to start monitoring too.

	Stop The **Stop** button from the **Activity** Ribbon group on the **Home** page allows you to stop monitoring for the currently selected hosts.

With Ping Monitor, it is possible to stop the monitoring process for any host being monitored any time you want. If you want to stop monitoring for hosts, select them in the **Hosts** or **Statistics** view and press the **Stop** button from the **Activity** Ribbon group on the **Home** page. Alternatively you can use the **Stop Monitoring** item from the pop-up menu or the **Stop** item from the **Manage Activity** button drop-down on the toolbar.

	Pause The **Pause** button from the **Activity** Ribbon group on the **Home** page allows you to pause monitoring for the currently selected hosts.
	Resume The **Resume** button from the **Activity** Ribbon group on the **Home** page should be used to resume monitoring for the currently selected hosts.

With Ping Monitor, it is possible to pause the monitoring process any time you want. While the monitoring process is paused, the ping packets are not sent to the remote hosts and the ping statistics stays the same until the monitoring process is resumed. To pause monitoring manually, select the required host and press the **Pause** button from the **Activity** Ribbon group on the **Home** page. Alternatively you can use the **Pause Monitoring** item from the pop-up menu or the **Pause** item from the **Manage Activity** button drop-down on the toolbar. It can also be paused automatically upon a certain predefined condition for a specified interval using the automation features of Ping Monitor. If the monitoring is paused, you can restart its operation using the **Resume Monitoring** menu item, or stop it completely using the **Stop Monitoring** menu item.

Analyzing Statistics

Ping Monitor gathers and stores per host performance and availability data while monitoring remote hosts connectivity. This data consists of the live statistics, integral historical statistics and raw historical data. You can review the monitoring statistics within on the **Statistics** page of the document, located at the center of the main screen. Let's take a detailed look on each layer of the monitoring data.

The live statistics is gathered while the server is running and restored on startup from raw historical data, in case if the raw data is configured to be persisted. The available live statistics intervals are provided within the **Live Data** section of the **Monitoring Statistics** preference page.

The historical data is stored hourly since the first time the monitoring was started. For each hour, all required characteristics are available: the monitoring time, the pause time, the uptime interval, the downtime interval, all latency characteristics, etc. This approach allows Ping Monitor to provide you with monitoring data for specific periods of time in the past with the maximum precision of one hour. Along with the hourly integrated data it is possible to store the raw responses data, that can be used to review **Timeline** and restore live statistics on restart. By default, the program stores all historical data for all hosts ever monitored until their statistics is deleted. If required, you can prevent the history database from continuous growing by configuring the historical data automatic removal or by disabling raw data storing in the **Historical Data** section of the **Monitoring Statistics** preference page.

Delete Statistics

The **Delete Statistics** button from the **Statistics** Ribbon group on the **Home** page should be used to delete all monitoring data for the selected hosts.

In case you want to begin the host monitoring from scratch, you do not need to delete the host and then create a new one. Ping Monitor provides you with an option of deleting the monitoring data for any host even without stopping the monitoring process. To delete all monitoring data for a host, select it and press the **Delete Statistics** button from the **Statistics** Ribbon group on the **Home** page. Alternatively, you can use the **Delete Statistics** button on the toolbar and the corresponding item from the pop-up menu.

Please note, that both live data, historical data and summary data will be permanently deleted when deleting monitoring statistics, so it won't be possible to generate historical data reports and review statistics for previous monitoring sessions.

If you have enable the raw data storing, you can review the monitoring timeline and export the information on each ping reply any time you want from the **Statistics** view while reviewing single host details. Just use the **Timeline** and the **Export Raw Data** buttons in the view header.

Pic 1. Choosing the raw data export period

The **Export Raw Data Wizard** will be displayed on the screen to guide you through the export process. You can either choose to export raw ping replies data for a specific period of time or entire data set `Pic 1`. The data is exported to the specified CSV file when you press the **Finish** button on the data export wizard after providing the required information.

Using Alerts

The program allows you to detect connection problems of monitored hosts using alerts. You can configure custom alerts according to your needs to detect different types of problems. In alert configuration you can specify a condition that is evaluated for each monitored host separately. Once this condition is satisfied, the program reports an alert for the host, so you can see the alert in the program and this alert shows the host for which it is reported. The alert ended once the condition isn't satisfied.

You can see current alerts in the system reported in **Alerts Summary**. Each alert there displays the name or the alert, a host name for which the alert is reported, alert state, severity and duration **Pic 1**. The alerts list displays all current alerts for all hosts. If you click a host name, you can navigate to the host level where current alerts for the selected host are reported only.

Pic 1. Alerts summary

The total number of current alerts is displayed in the **Alerts** section of **Overview**. Alerts means the current problems, is there are no alerts, it means that you don't need any monitoring problems at the current moment. If there are alerts reported, you can review them in **Alerts Summary** and start to resolve the problems with hosts. Once the problem has been discovered, you can acknowledge it while working on the solution. To acknowledge the problem select the corresponding action in the context menu or on the toolbar. The alert can be acknowledged for a selected period of time or indefinitely. Acknowledged alerts are reported with the corresponding state, so you can see which alerts are active and acknowledged. If the problem isn't resolved during the acknowledge time period, the alert becomes active again.

The program can send notifications and execute custom actions when an alert is started and ended. It is described in the **Notifications of Alerts and Events** chapter. You can configure alerts and their conditions on the **Alerts and Notifications** page of the program preferences. By default the program provides two preconfigured alerts, but you can change them or create custom alerts in preferences. It is possible to use any real-time monitoring characteristics in the alert condition, including host state, quality characteristics, packet loss, latency, jitter and other metrics **Pic 2**.
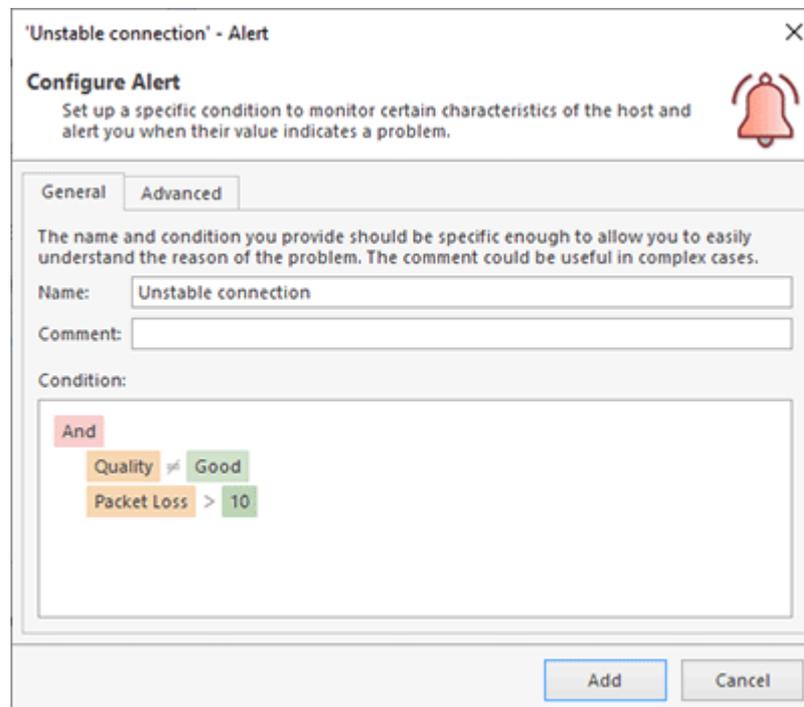
Pic 2. Alert configuration

When you configure an alert condition you can use logical operators to create condition of any complexity. Alternatively you can create a few separate alerts where each alert includes a simple condition. Use the approach that works the best in every particular case.

Host State Monitoring

EMCO Ping Monitor was primarily designed to monitor host state thus detect outages. The main characteristic of the monitored host is its uptime – the percentage of the monitoring time the host was online. The time period when the host is offline is called an outage. Each outage is detected regarding the condition defined in the monitoring settings. The conditions to treat the host as online is also configured through the monitoring settings.

For the host that is online, the state is **Up** and it is **Down** for the hosts that are offline. The **Pending** state is used to describe the moment when neither **Up** nor **Down** condition is reached. If you are using the gateway to check if the host is reachable and the host is currently not reachable, the **Unreachable** sign is added to the state. In case the host is in a non-pending state and the state is going to change (for example, the host state is **Up**, the packet is lost, but the **Down** condition is not reached yet) the state is considered as **Unstable**.

The summary information on hosts in different state is available on the **Overview** page of the document, located at the center of the main screen. There you can find the number of hosts that are in **Up**, **Down** and **Pending** states. The detailed per-host information on the current state can be found on the **State Summary** page. It is specially designed to focus on states monitoring. You can either monitor the per-host state, or monitor a number of hosts in different states per-group.
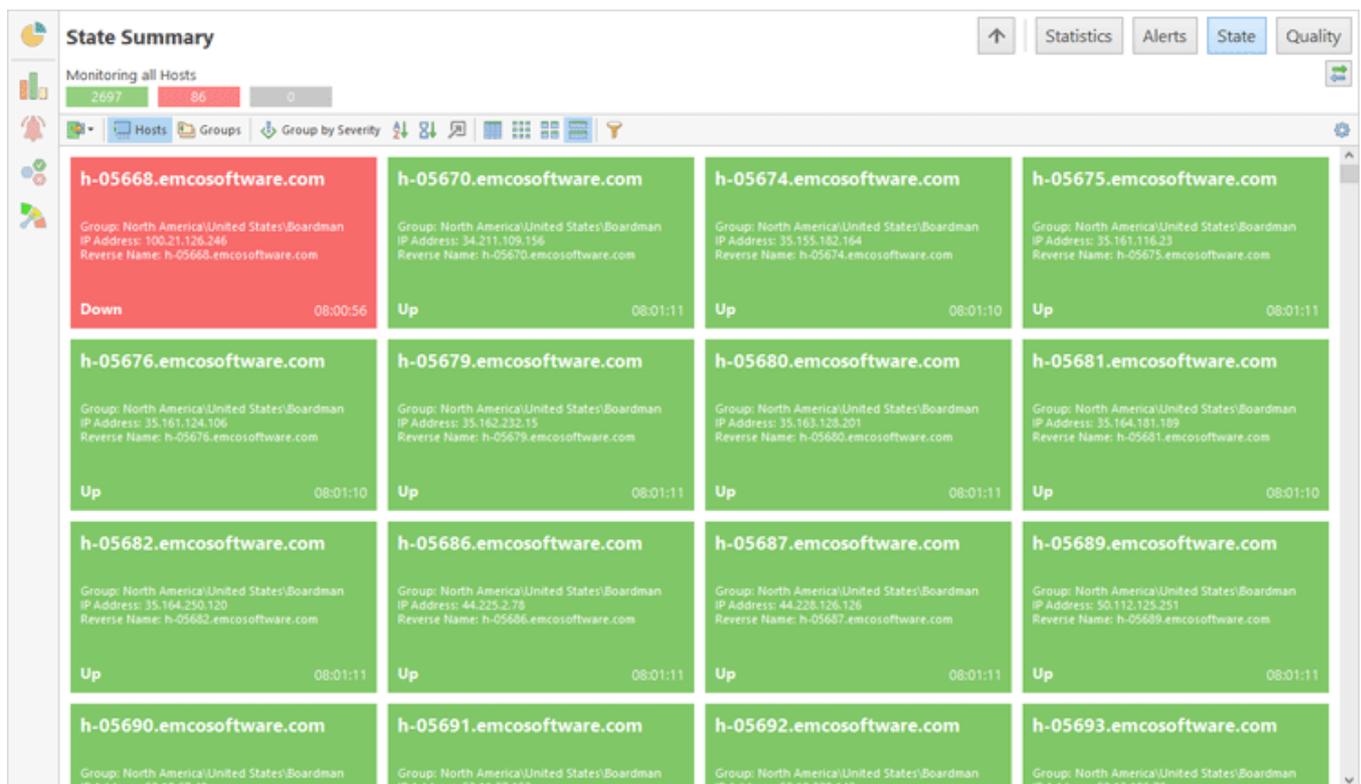
Pic 1. State Summary for all hosts

All information on ping replies, state changes, etc is stored to the monitoring statistics, unless explicitly disabled in program preferences on the **Monitoring Statistics** page.

Connection Quality Monitoring

Along with remote hosts state monitoring, EMCO Ping Monitor comes with an ability to monitor connection quality based on the provided settings. The connection quality check is performed on a basis of a sample containing the specified number of latest responses. The following characteristics can be used for calculation:

- **Packet Loss Percentage** - a ratio of the number of lost packets in a connection quality check sample to the number of packets being sent within the same sample;

- **Latency Percentile** - a specified percentile for latency in a sample of responses;

- **Jitter** - a packet delay variation for a sample of delivered packets of a specified length with reference to the specifications defined in RFC-1889.

The packet loss percentage cannot be removed from quality calculation and the connection quality is treated as **Critical** when 100% of packets are lost. The connection quality is **Bad** in case if any condition from enabled for bad quality is reached, the same is true for the **Warning** quality. The quality is **Good** when no problematic condition is reached. When the sample size is insufficient to calculate the connection quality, it is **Pending**. If you are using the gateway to check if the host is reachable and the host is currently not reachable, the **Unreachable** sign is added to the connection quality.

The summary information on hosts with different connection quality is available on the **Overview** page of the document, located at the center of the main screen. There you can find the number of hosts with **Good**, **Warning**, **Bad**, **Critical** and **Pending** quality. The detailed per-host information on the current connection quality can be found in the **Quality Summary** page. It is specially designed to focus on connection quality monitoring. You can either monitor the per-host connection quality, or monitor a number of hosts with different connection quality per-group.
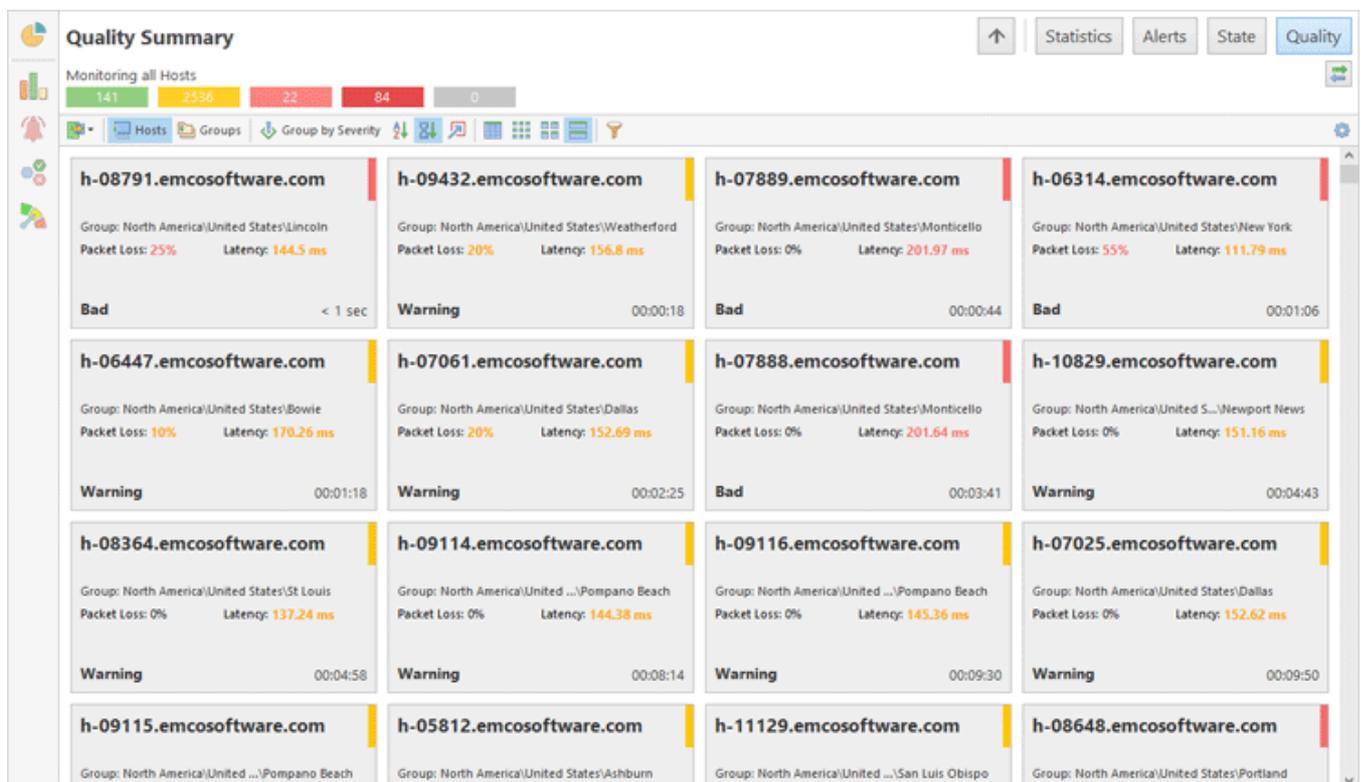
Pic 1. Quality Summary for all hosts

All information on connection quality changes is stored to the monitoring statistics, unless explicitly disabled in program preferences on the **Monitoring Statistics** page.

Notifications on Alerts and Events

One of the most outstanding features of Ping Monitor is an ability to trigger notifications on alerts and on specific host state and connection quality changing events. You can flexibly configure each and every notification: choose a delay for notification, specify the periods of time when the notification can be triggered, provide the number of iterations for the notification to reoccur, etc. The program allows you to use the following notification types:

- E-mail Message;

- Custom Action;

- Sound;

- Balloon Tip.

The balloon tips and sound notifications are triggered on a client side, whereas the e-mail messages and custom actions are handled by the server.

E-mail messages are sent using the specified **E-mail Options**. The e-mail message subject and body used for building notification messages are configured on the **Notification Mail Templates** preferences page, and the placeholders that can be used in the templates are described in the Using Placeholders part of this guide. For the custom actions, you can provide any command that does not require interaction with an end-user. The sound notification can play any system sound or the custom one, provided by the user during notification configuration.

> 💡 With Ping Monitor, you can use the placeholders for the **Custom Actions** definitions similarly to the connection status notifications, e.g. *ConnectionLoss.cmd "%REMOTE_HOST_ADDRESS %"* for connection loss. Do not forget to quote the placeholders that contain white spaces.

Ping Monitor sends notifications in the following cases:

- **On Alert** - occurs when an alert is started and ended;

- **On Down State Event** - occurs when the outage condition is met for the host thus it goes down;

- **On Up State Event** - is considered to occur when the host connection to which was lost goes up;

- **On Good Quality Event** - occurs when a connection quality to the monitored host becomes **Good**;

- **On Warning Quality Event** - occurs when a connection quality to the monitored host is changed to **Warning**;

- **On Bad Quality Event** - occurs as soon as the **Bad** connection quality to the host is detected;

- **On Critical Quality Event** - occurs when a connection quality to the host goes **Critical**.

E-mail notifications and custom actions can be configured on the **Alerts and Notifications** page of preferences. Sounds and balloons can be configured on the **Balloons and Sounds** page of preferences. You need to configure alerts and events first and then assign required notifications that should be sent on these alerts and events.

When you configure notifications you can specify their settings that are different for the different type of notifications. For example, for e-mails you can configure e-mail recipients, for custom actions you can configure commands to be executed. On the **Advanced** tab of the configuration you can specify additional options such as timeout, execution time, etc.
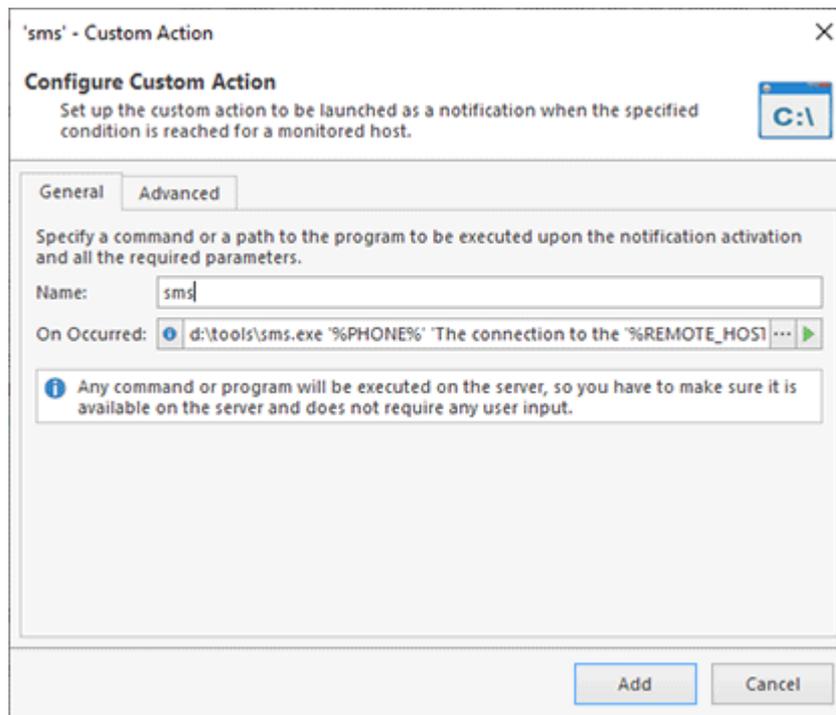
Pic 1. Notification configuration

For each notification, it is possible to define a timeout, in minutes, i.e. the waiting period before the notification is triggered. If the host state or connection quality is changed during such waiting period, the corresponding notification is not triggered. You can configure the notifications to reoccur multiple times with the specified interval between occurrences as long as the triggered condition is met. Default configuration is specified on the **Notification Time** page in preferences, but you can override these settings and specify custom configuration for each notification.

If you want the notification to trigger only during a specific period of time, enable the **Trigger this notification only during the following hours** option and specify the time period. The program skips the notifications for the events that occur outside the configured interval.

Auto-start List

Ping Monitor is a program used to monitor connectivity to remote hosts, so the monitoring activity management is one of the main functionality parts. To make it more comfortable to start bulk monitoring we have introduced automation settings available on the **Automation** preference page. You can configure either to restore the previous monitoring activity for hosts on the next server startup, or start monitoring only for those hosts that are included in the auto-start list, or leave the monitoring process inactive for all hosts. In case you have chosen the second option, you should configure the auto-start list, by including and excluding specific hosts.

	Include The **Include** button from the **Auto-Start** Ribbon group on the **Hosts** contextual page from the **Hosts Tools** category should be used to add the selected hosts to the auto-start list.
	Exclude The **Exclude** button from the **Auto-Start** Ribbon group on the Hosts contextual page from the **Hosts Tools** category should be used to remove the selected hosts to the auto-start list.

When a host is created it is automatically added to the auto-start list. You can then use the **Include** and **Exclude** button from the **Auto-Start** Ribbon group on the **Hosts** contextual page from the **Hosts Tools** category to include hosts to and exclude hosts from this list. These items are also available in the **Hosts** view toolbars and pop-up menus. To check if the host is currently included to the quick launch, just review if the **On Startup** column of the **Hosts** view has the **Activate** value.

Chapter 6: Reporting

Ping Monitor comes with a built in feature of generating statistical reports based on the historical data gathered while monitoring remote hosts connectivity. The generated reports can be sent to you via e-mail and stored either locally or on an FTP server. You can generate a generic report for any period of time any time you want. It is also possible to save preconfigured reports to be generated either on demand or automatically on a regular basis.

There are two different types of reports; those are the **Summary** and the **Detailed** ones. The summary reports provide you with a brief information on monitors availability and performance in a form of a table, where each row represents a single host from the report members. The detailed report contains a wider range of data and consists of multiple sections, where each section stands for a single host. Within a section, you can find the monitoring activity, response time and availability characteristics. The cumulative characteristics are amplified with the graphical representation of the characteristics dynamic in time for the report period. The presentation and the actual set of displayed characteristics depends on the report output settings.

In the following chapters, we will provide you with the detailed description of the reports configuration process.

Generic Reports

Ping Monitor allows you to generate reports based on historical data for any set of hosts and for any period from the past. The generated report can be either sent via e-mail or saved to the reports storage. Let us take a look at generating reports from a scratch.

Generate Report

The **Generate Report** button from the **Reporting** Ribbon group on the **Home** page should be used to generate a performance and availability report for any period of time.

To generate a new report at the current moment, you should use the **Generate Report** button from the **Reporting** Ribbon group on the **Home** page. The wizard will be displayed on the screen to guide you through the steps of the report generation process `Pic 1`.
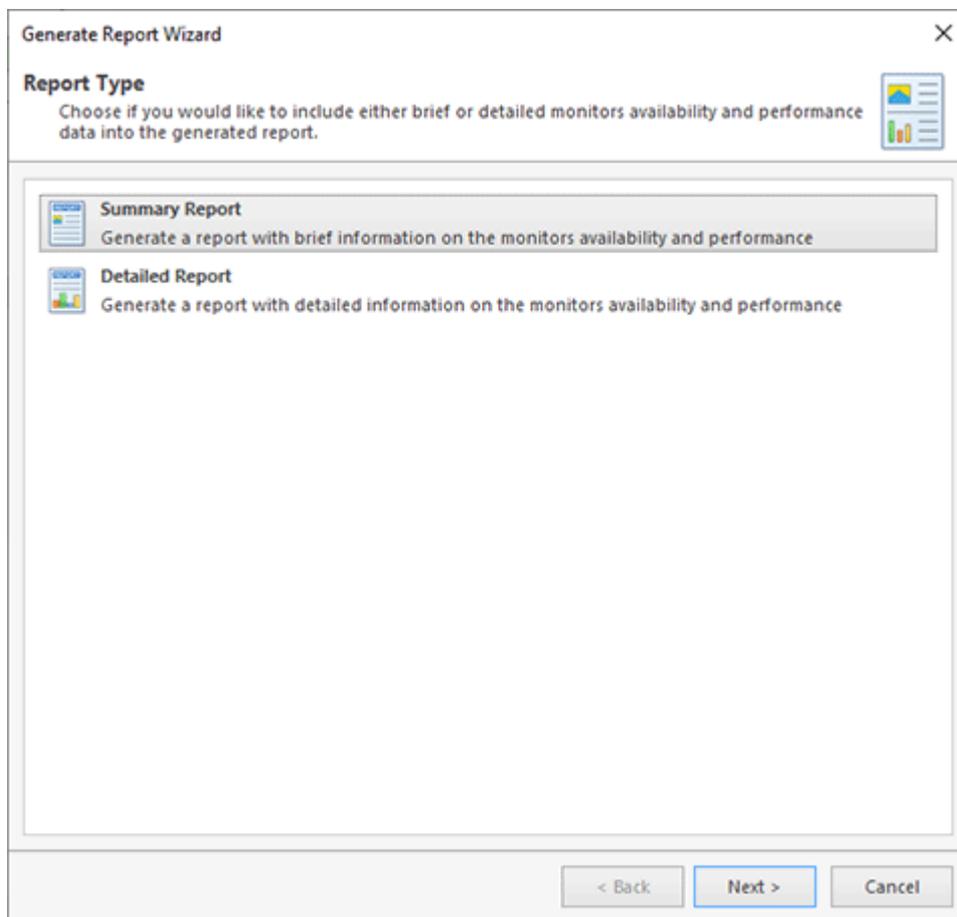
Pic 1. Choosing a report type

On the first page of the wizard, you are proposed to choose the type of the report to be generated. The **Summary** reports provide you with a brief information in a form of a table, where each row represents a single host, and the **Detailed** report contains a wider range of data and consists of multiple sections, where each section stands for a single host. When the report type is chosen, press **Next**.
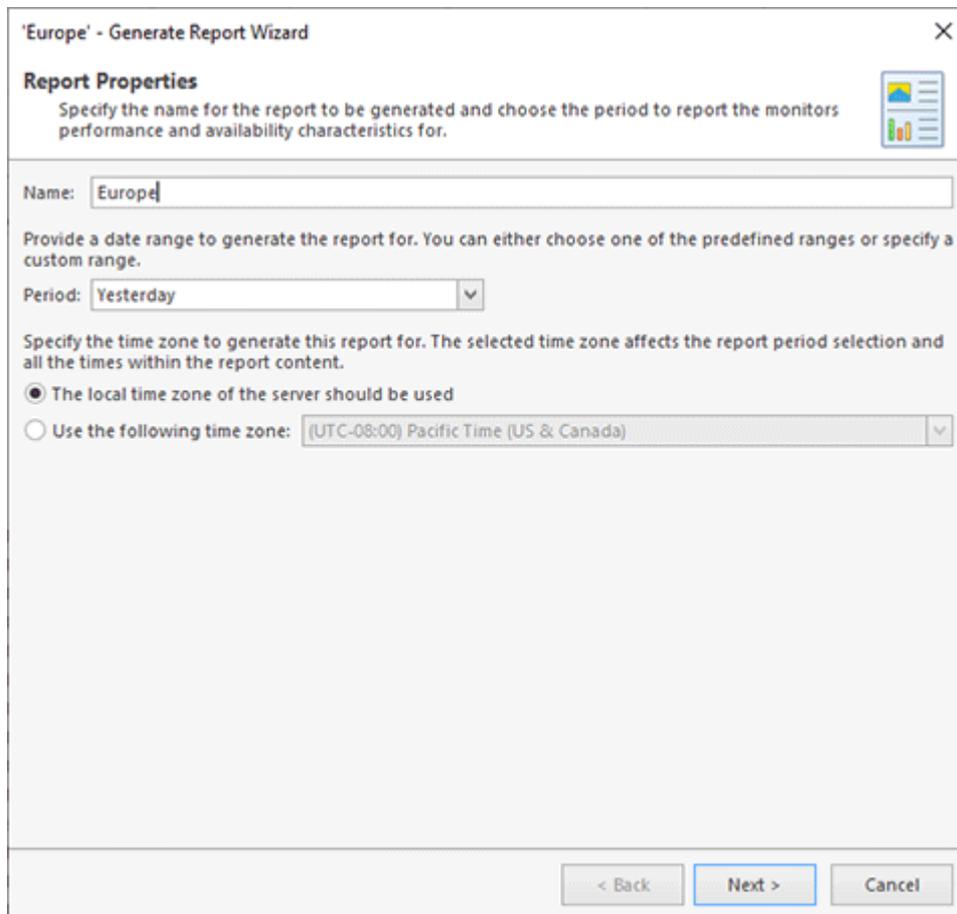
Pic 2. Specifying the report properties

On the next page of the wizard Pic 2, you are proposed to specify the report properties. Those are the report name and the period to generate the report for. You can choose between the predefined periods available in the **Range** drop-down, or choose the **Custom Range** value and specify the required period. When the detailed report is generated, the level of details will be adjusted to the report period automatically. Next to the report range, you can specify the time zone used for generating the report. The selected time zone affects the selection of the report period and all the times within the report content. You can either use the local time zone of the monitoring server, which is the default behavior, or choose a specific time zone.

On the next pages, you are proposed to choose a list of report members and define report output options. In case the **Hosts** view or the **Statistics** view was active while initiating a generic report generation, the selected hosts and groups are automatically added to the report members. For the detailed information on report members configuration, refer to the Report Members section of this document. You can filter the members based on their performance and availability characteristics by specifying the Report Filter. As for the reports output, you can save it to the file or send via e-mail, and indicate which information should be included into the detailed report. The outputs configuration is described in the Report Outputs section.

After you have configured the report options, press **Finish** for the report to be generated. As you can see, creating a generic monitoring data report is a fast and easy process, and you should be able to use it in the everyday work without any difficulties.

Preconfigured Reports

Along generating the monitoring performance and availability reports from scratch, Ping Monitor allows you to save preconfigured reports to be generated either on a regular basis or on demand. The preconfigured reports are saved in the program database and displayed in the **Reports** view. Let us take a closer look on those reports.

Summary Report

The **Summary Report** button from the **New** Ribbon group on the regular **Home** and contextual **Reporting** page from the **Reporting Tools** category should be used to create a new preconfigured report with the brief information on monitors performance and availability.

Detailed Report

The **Detailed Report** button from the **New** Ribbon group on the regular **Home** and contextual **Reporting** page from the **Reporting Tools** category should be used to create a new preconfigured report with the detailed information on monitors performance and availability.

The same way as for creating generic reports, you can choose between summary and detailed report. To create a preconfigured summary report, use the **Summary Report** button from the **New** Ribbon group on the regular Home and contextual **Reporting** page from the **Reporting Tools** category. For the detailed reports creation, the **Detailed Report** button should be used. The corresponding items are also available under the **New** drop-down button of the **Reports** view toolbar and the corresponding item in the pop-up menu. In any case a dialog will be opened to help you configure the report object `Pic 1`.

Pic 1. Creating a detailed report

The report configuration pane consists of four navigation pages, those are: **General**, **Members**, **Filter** and **Outputs**. On the general page, you are supposed to provide a common information about the report object to be created. The name for the report to be created should be provided to the **Name** field. Optionally, you can provide a description for the easier report object identification to the **Description** field.

For the preconfigured reports, one of the main properties is the recurrence type. It defines if the report is generated on demand or on a regular basis. In case the report should be generated on a regular basis, you can choose between daily, weekly and monthly reports.

The daily report, when being generated, includes the monitoring data for the day prior to the generation date. The daily reports are generated every day at the specified time.

For the weekly report, you can specify if it should contain the information for the previous calendar week or the previous seven days when generated. In case you have chosen the previous seven days and the report is generated on the *Autust the 28th 2019*, the report period will be from the *August the 21st* to the *August the 27th*, inclusive. When the previous calendar week is chosen, the

report period will be from the *August the 19st* to the *August the 25th*, inclusive. The weekly reports are generated on a specified week days at the specified time.

The monthly report can be generated on a basis of the monitoring data for the previous calendar month or the previous month to date. For example, if the report is generated on the *May the 5th*, the report period will be from the *April the 5th* to the *May the 4th*, inclusive in case of the previous month to date, and from the *April the 1th* to the *April the 30th*, inclusive in case of the previous calendar month. The monthly reports are generated in case of the previous month to date, and from the April the 1th to the April the 30th, inclusive in case of the previous calendar month on a certain week day of the month at the specified time.

You can also specify the time zone used for the predefined report being configured. The selected time zone affects the report generation time, when recurrent, the report period and all the times within the report content. You can either use the local time zone of the monitoring server, which is the default behavior, or choose a specific time zone. When configuring recurrent reports, in case the time zone differs from the client's one, the next report time preview will show both the time in the selected time zone and the local time.

The other pages are used to define the report members, filter and outputs. For the information on defining members, you can refer the Report Members section of the document, the filtering is described in the Report Fitler section, and the guidance on report outputs configuration is available in the Report Outputs section.

	Generate
Generate	The **Generate** button from the **Reports** Ribbon group on the **Reporting** contextual page from the **Reporting Tools** category should be used to manually generate the selected preconfigured report.

For the report to be generated on a regular basis, the server should be up and running at the date and time the report is going to be generated. You can also generate such report manually at any time, the behavior will be the same as it is generated automatically at the same time.

If you have chosen to generate the report on demand, the program will ask you to provide the report period when you are requesting the report generation. The level of details in the detailed report will then be adjusted automatically to the report period.

To generate the report on a basis of predefined configuration, you should select it in the **Reports** view and press the **Generate** button from the **Reports** group on the **Reporting** contextual **Ribbon** page from the **Reporting Tools** category. Alternatively, you can use the corresponding items on the **Reports** view toolbar and in the pop-up menu.

	Enable
Enable	The **Enable** button from the **Reports** Ribbon group on the **Reporting** contextual page from the **Reporting Tools** category allows you to turn on an ability of generating the selected reports.

	Disable
Disable	The **Disable** button from the **Reports** Ribbon group on the **Reporting** contextual page from the **Reporting Tools** category allows you to turn off an ability of generating the selected reports.

In case for some reason you do not want the preconfigured report to be generated automatically or would like to prevent on demand reports from being mistakenly generated, you can disable those reports generation. To disable an ability of reports generation, select those reports in the **Reports** view and choose either the **Disable** button from the **Reports** Ribbon group on the **Reporting** contextual page from the **Reporting Tools** category, or the **Disable** button on the view toolbar, or the **Disable** item from the pop-up menu. As soon as the report is disabled, it won't be possible to generate it until it is enabled again. To enable the report, use the **Enable** buttons and menu item.

To edit any report, select it and either choose the **Edit** button from the **Organize** Ribbon group on the **Program** page or use the **Edit** items from the **Reports** view toolbar and pop-up menu. The editing process is similar to the creation. When some reports are no longer needed you can delete them using either the **Delete** button from the **Organize** Ribbon group on the **Program** page or the **Delete** items from the view toolbar and pop-up menu.

Within the Reports view it is also possible to copy reports and add members to reports without opening the report editing dialog. This can be done either via the drag and drop technique, or via the copy/paste one. The **Cut**, **Copy**, and **Paste** items from the **Clipboard** Ribbon group on the **Program** page can be used, as well as the appropriate items from the pop-up menu. It is also possible to copy reports between different editions of the program and use the export feature. For the details on import and export, refer to the Importing and Exporting Preconfigured Reports section of this document.

Report Members

When configuring both generic and preconfigured reports, you are proposed to provide a list of report members `Pic 1` . This list is used to define a set of host to report their availability and performance characteristics.
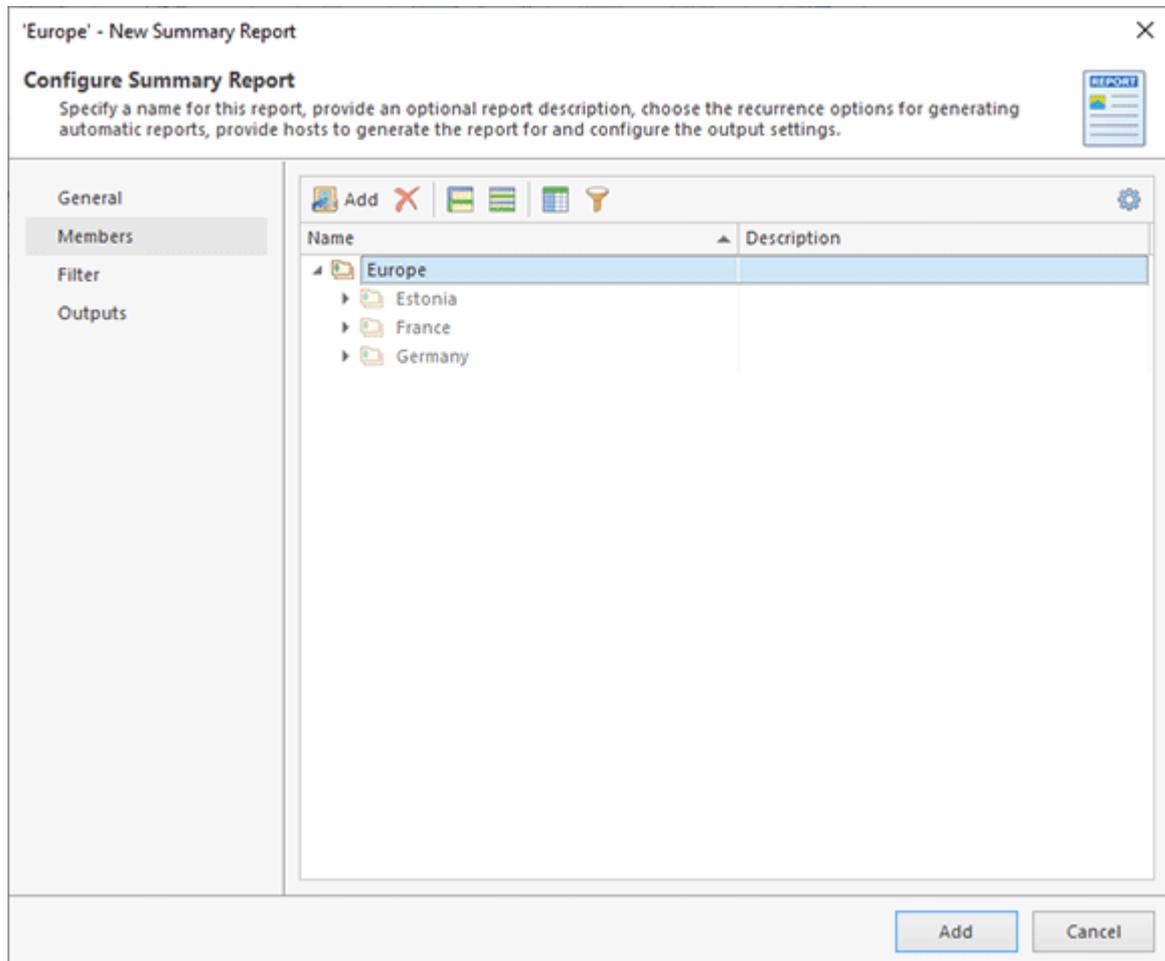
Pic 1. Defining report members

When defining report members, you can add to the members lists any host or group of hosts. In case a group of hosts is added, all hosts from this group and subgroups will be processed while generating a report. When you perform the changes to the group content it is automatically reflected in the report, because the group is actually linked. You can review a group content in the members list editor by expanding the group node. If you want to ensure, that specific host will surely be included in the report, you can add that particular host even if it contains in a group already added. The program guarantees that a single host will appear in a report content only once.

To add members to a report, you can use the **Add** button on the members editor toolbar and the corresponding item from the pop-up menu. The dialog will be opened to let you choose the members from those available in the program to be added. To remote the members from the list, select them in the editor and press the **Delete** button on the toolbar. You can also choose the **Delete** item from the pop-up menu.

145

Report Filter

With Ping Monitor you can filter the report content during the report generation. This feature allows you to flexibly perform dynamic report configuration. For example, you can exclude the hosts that were not monitored during the report period, or those that had no outages. The filter may be specified during the report configuration process `Pic 1`.
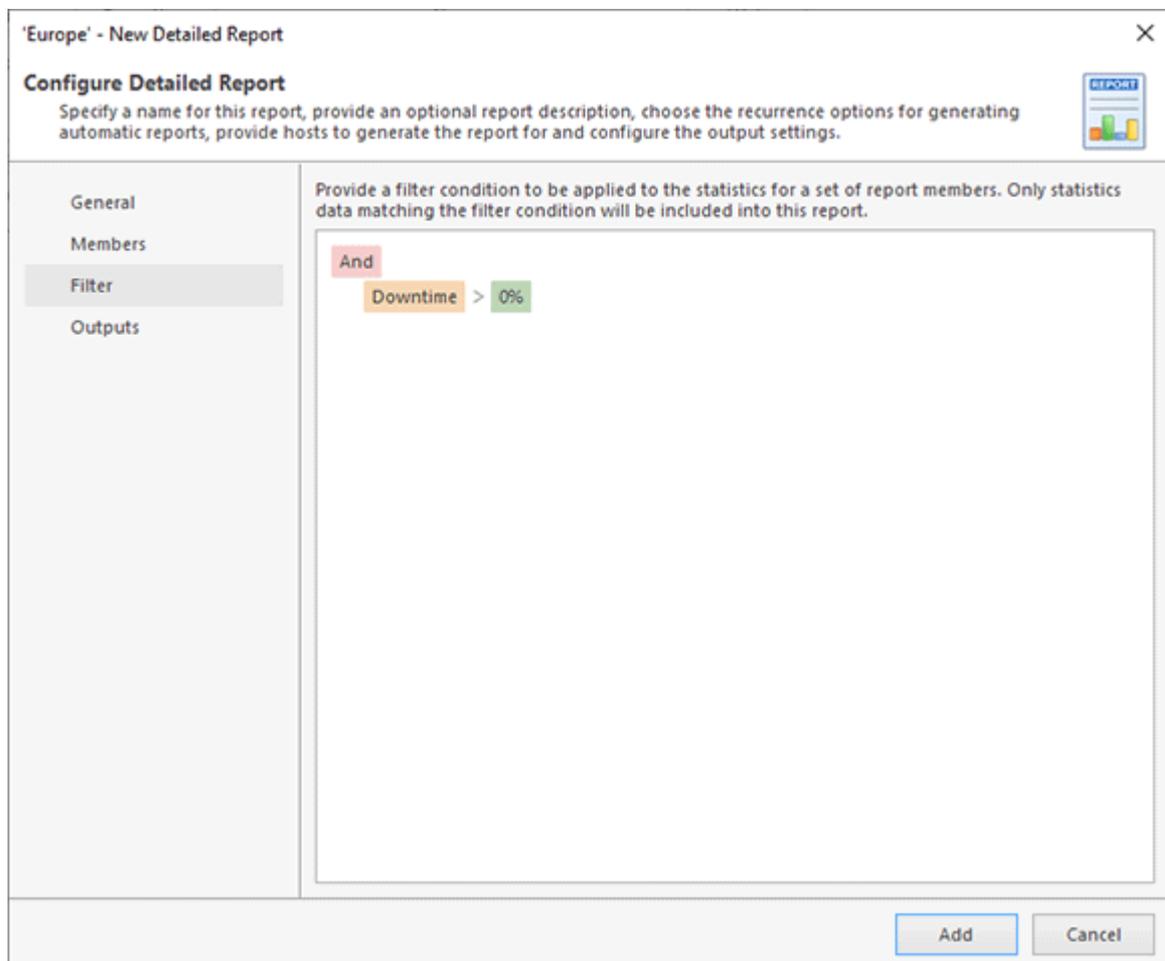
Pic 1. Specifying a report filter

The report filter editor is similar to the filter editor used for filtering data in trees and tables. You can combine any number of conditions, as well as groups of conditions, with **Or** and **And** operators. You can filter by any field from those available in the statistics data.

When the report is generated, the program checks if each host statistics matches the filter condition and, if not, the host is excluded from the report output. In case all hosts are excluded, the report is not generated and the corresponding message is added to the **Log** view.

Report Outputs

Ping Monitor allows you to send monitors performance and availability reports via e-mail or save them to a reports storage. Each of these outputs can be enabled while configuring a generic or reconfigured report `Pic 1`.

Pic 1. Configuring report outputs

When configuring report outputs, you can specify if you would like the report to be sent via e-mail and/or saved to the reports storage. The e-mail generation options are configured within the **E-mail Report** group, and the saving options in the **File Report** group. When configuring a detailed report, within the **Content** group, you can specify if the tables with all state intervals, quality intervals and host events for the report period should be included into the report. You can disable these options to reduce the report size if the corresponding information is not required.

Within the **E-mail Report** group you can enable the e-mail output using the **Send Report via E-mail** check box. When sending reports via e-mail, the message body is by default generated using the Notification Mail Templates specified for the report type and sent to the recipients defined in the mail options. For preconfigured reports, you can override e-mail recipients and mail templates on the corresponding tabs of the outputs configuration page.

To enable saving file reports to the reports storage, you should check the **Save Report to Storage** option within the **File Report** group. The report can be saved to one of the following formats: **Adobe PDF File**, **HTML Web Page** and **MIME HTML** Document. The format is selected within the **Report Format** field. The file name to be used for the file created while generating the report is created on a basis of the template defined within the **Name Template** field. The placeholders that

can be used in the field are described within the **Report Name Template Placeholders** section of the document. The preview of the file name generated using the specified template is available in the **Name Preview** field. The file reports are by default saved to the location configured in the storage settings. For preconfigured reports, you can override these settings on the corresponding tab of the outputs configuration page.

Importing and Exporting Preconfigured Reports

With Ping Monitor, you can easily import and export reports any time you want. You can export one or all of the available reports to use the exported data as a back-up, to share the reports with your colleagues or simply to import them to another instance of the program. This chapter covers the process of importing and exporting reports.

Import	**Import** The **Import** button from the **Organize** Ribbon group on the **Program** page can be used to import reports from an XML file with the help of the wizard.

The reports can be imported into Ping Monitor from XML files. The XML file structure is quite complex, so it is not recommended to create it manually. If you want to import the reports into Ping Monitor, press the **Import** button from the **Organize** Ribbon group on the **Program** page, when the **Reports** view is active. The **Import Reports Wizard** will appear on the screen Pic 1.
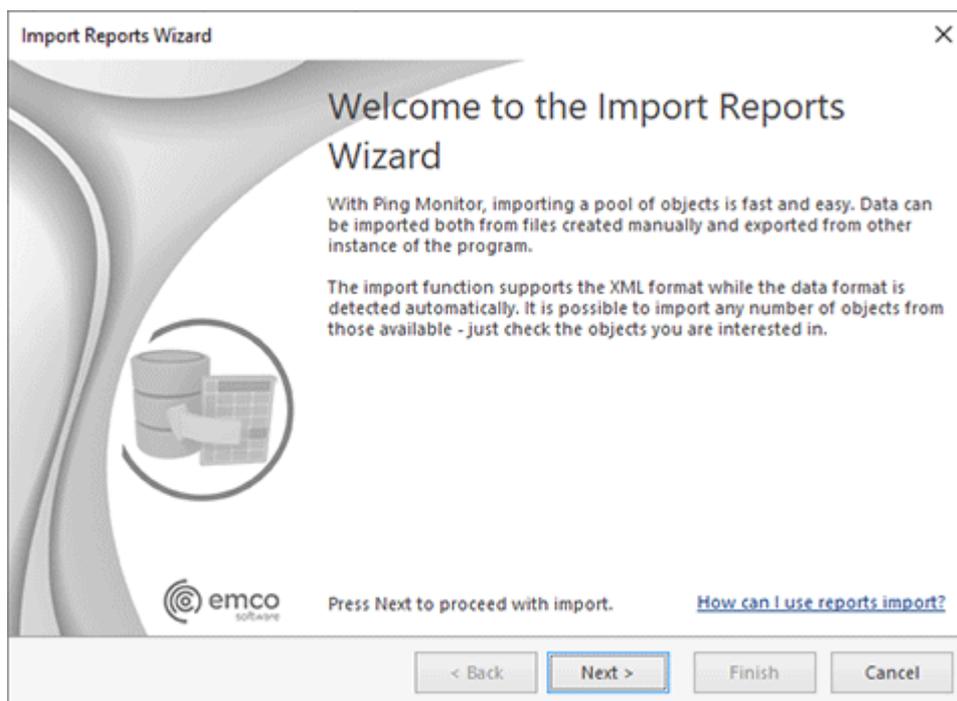
Pic 1. The Import Reports Wizard welcome page

The first page of the **Import Reports Wizard** is the welcome page, which is used to introduce you to the feature the wizard is supposed to help you with. After reading the welcome information, press **Next** to continue with import.

On the next page of the **Import Reports Wizard**, you are offered to choose the file you are going to import reports from. The file path should be provided in the **Import** From field `Pic 2`. The format and encoding of the XML file with reports is detected automatically.
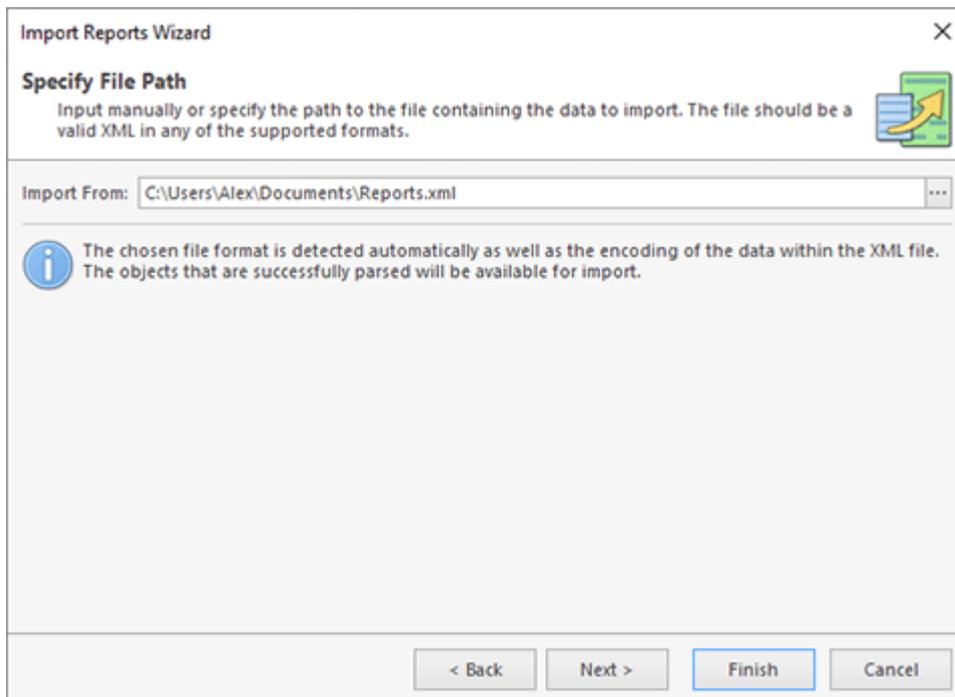
Pic 2. Choosing the import source file

The next page offers you to choose the reports to import. By default, all the valid reports are selected `Pic 3`.
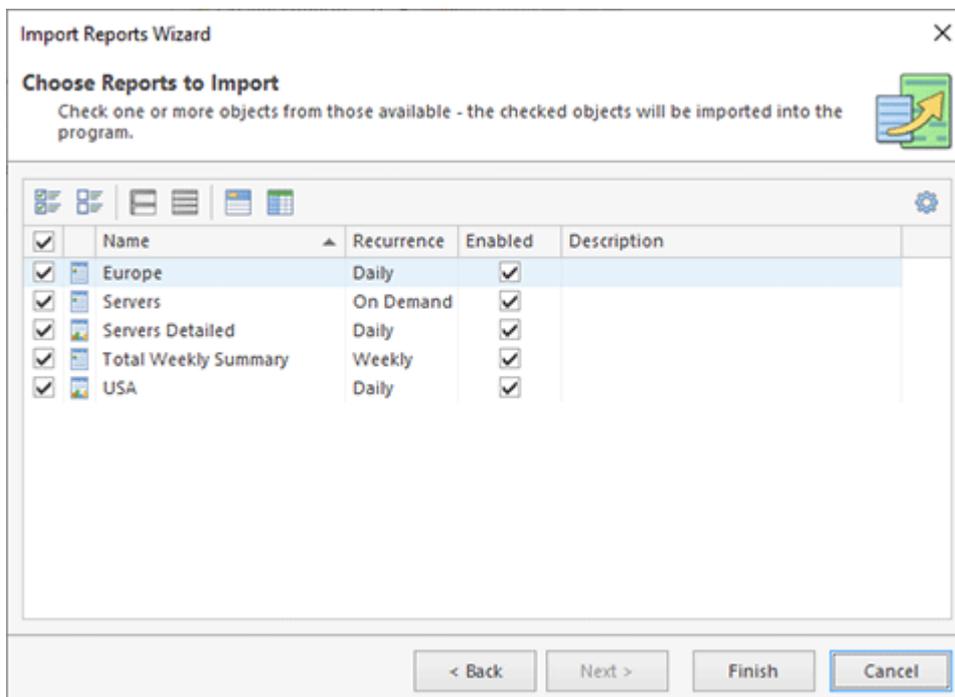
Pic 3. Choosing the reports to import

When the reports to import have been chosen, press **Finish**. When the import is done, the reports are added to the program and displayed in the **Reports** view.

> **Export**
>
> The **Export** button from the **Organize** Ribbon group on the **Program** page should be used to export reports from the program to an XML file that can be used in the future for import.

The reports can be easily exported to the XML file format for future reuse. The reports export can be performed from the **Reports** view. You can choose between exporting all reports and those that are currently selected. To perform export, use an appropriate option from the drop-down of the **Export** button from the **Organize** Ribbon group on the **Program** page. The **Export Reports Wizard** will appear on the screen `Pic 4`.

Pic 4. The Export Reports Wizard welcome page

The first page of the **Export Reports Wizard** is the welcome page, which is used to introduce you to the feature the wizard is supposed to help you with. After reading the welcome information, press **Next** to continue with export.

On the next page you are offered to choose the file you are going to save the reports to and the format options. The file path should be provided in the **Export To** field `Pic 5`.
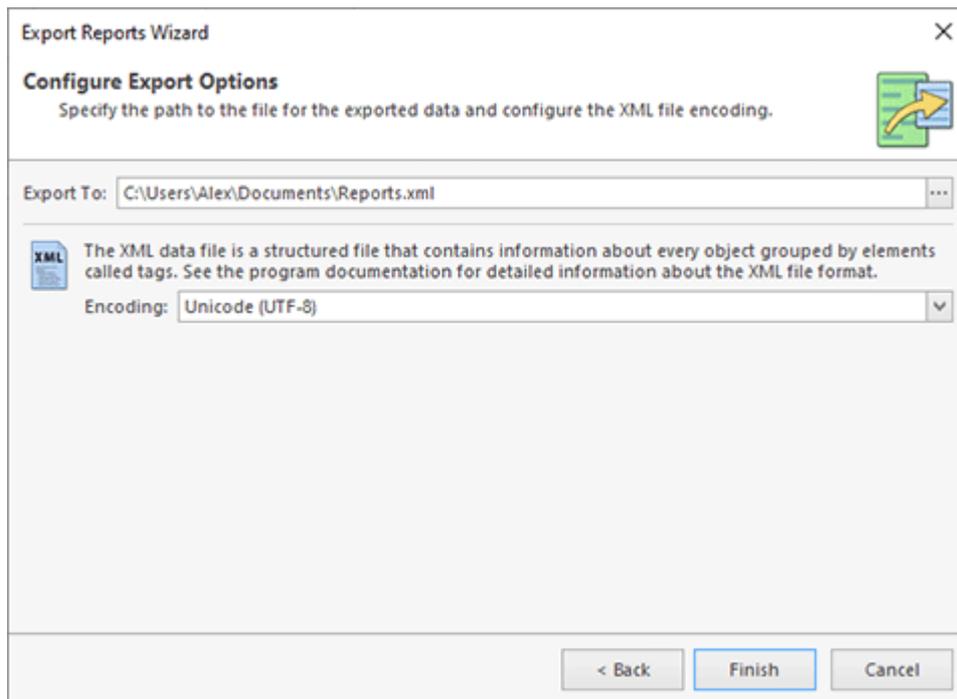
Pic 5. Configuring export options

When the file path and the encoding are chosen, press **Finish** to proceed with export. The file containing the reports' information will be created in the location according to the path specified. The file created during export can be used in the future to import the reports back to the program.

Now you are fully introduced to the reports export and import capabilities of Ping Monitor and can use them in future to solve your tasks.

Chapter 7: Web Interface

Ping Monitor comes with an option of deploying an IIS web site together with the server application to provide web access to hosts monitoring and statistics review. This site is installed by default when performing a complete server installation.

Web Interface

The **Web Interface** button from the **Web** group on the **Home** Ribbon page can be used to open the EMCO Ping Monitor program web site in the default browser.

On the web site home page, you can see the monitoring system overview **Pic 1** and a set of buttons that can be used to navigate through available pages.
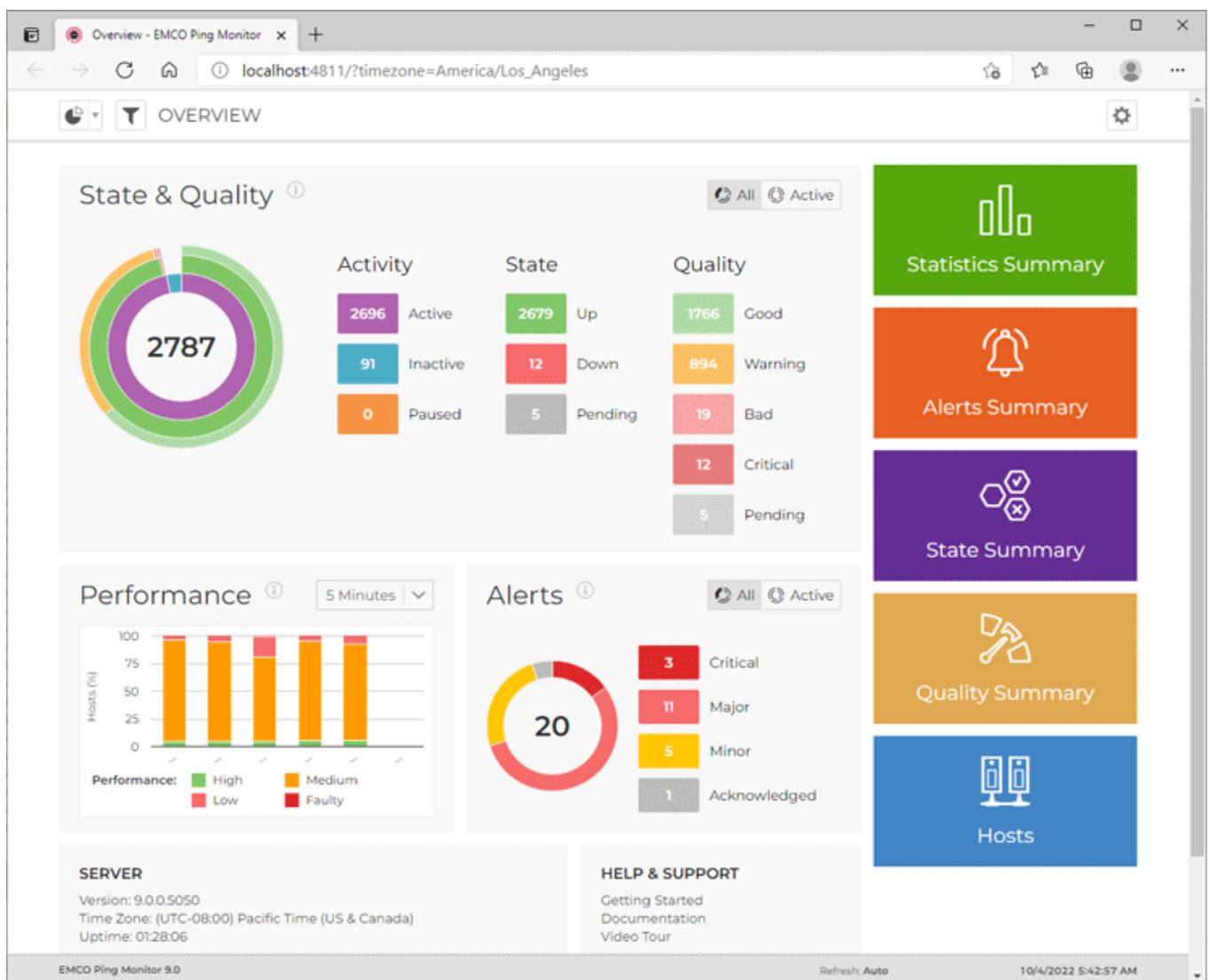
Pic 1. The web interface home page

For each web page in the header part you can find its title, navigation menu, filtering button and tool buttons used to manage the page. The status bar in the bottom of the page always shows the information on the server, page generation date and time till next refresh, in case the auto-refresh is currently enabled.

152

In this chapter, we will take a closer look on each of the available pages.

Overview Page

The **Overview** `Pic 1` page is designed to provide you with the brief information on monitored hosts and their states. It is the home page of the Ping Monitor web interface. You can either overview the entire monitoring system or focus on specific host and/or groups.
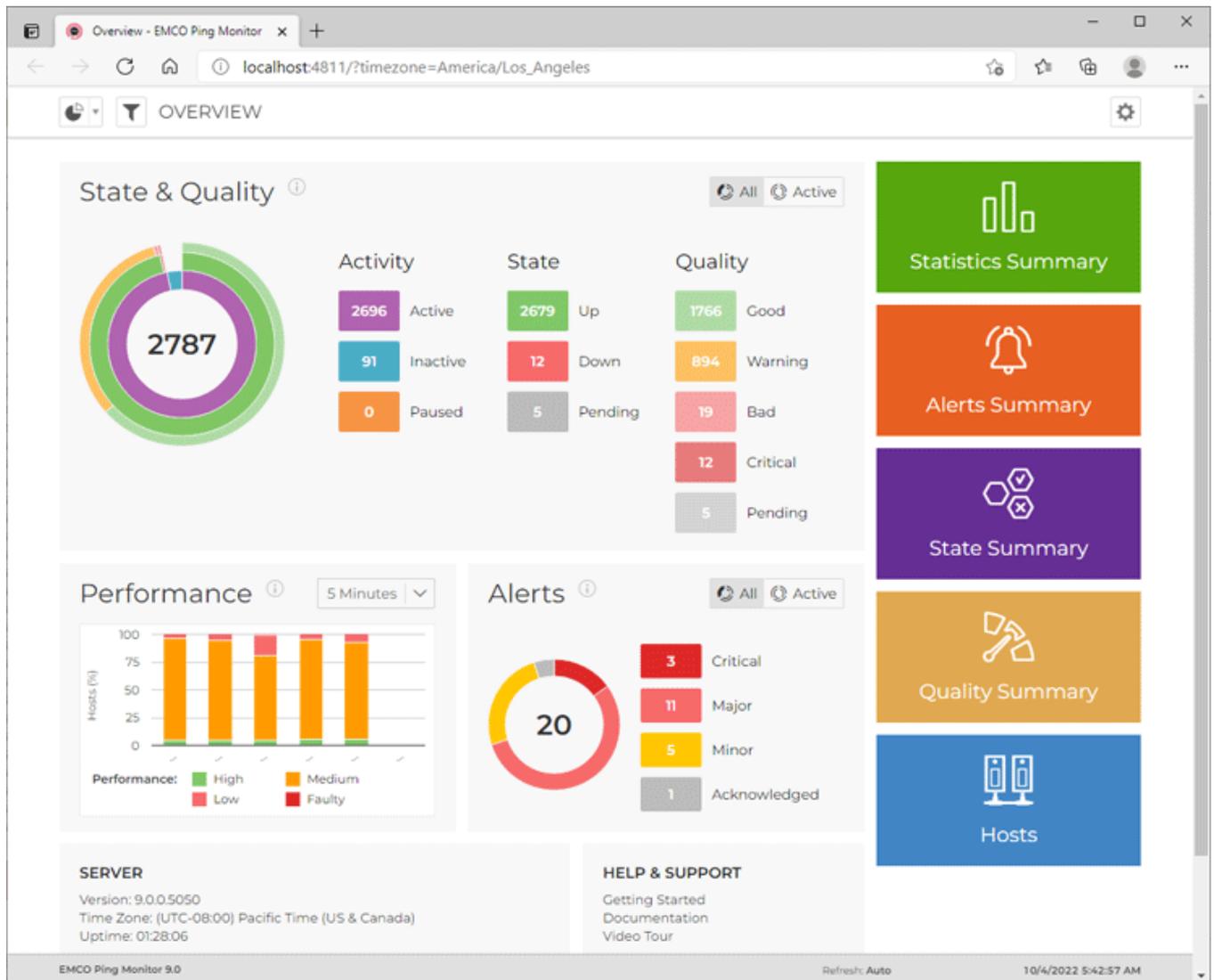
Pic 1. The entire monitoring system overview

In the **State & Quality** area of the **Overview** page the information is summarized in a doughnut chart, so you can easily see the distribution of hosts with different state and quality. Inside a doughnut itself, you can find the total number of hosts you are focusing. The first column of the legend displays the count of active, inactive and paused hosts – this distribution is represented with the inner doughnut.

For the hosts the monitoring is active for, you can find the information on how many of them are Up and Down. This distribution is displayed in the second column of the legend and the middle doughnut respectively. The last column is used to describe the connection quality to monitored hosts. The distribution is reflected in the outer doughnut on the chart. You can focus on host states and connection quality distribution for active hosts by clicking on the **Active** radio button in the right top corner of the area. To switch back to all hosts use the **All** button.

The **State & Quality** and other parts of the **Overview** page are interactive. For example, you can click the values for the activities and/or states and qualities to drill down to the hosts with the corresponding activity, quality and state.

The **Performance** area shows a chart with distribution of the total number of hosts with the different performance characteristics over time. You can select a period of time and see how many hosts had **High**, **Medium**, **Low** and **Faulty** performance in specific periods.

The **Alerts** area displays a chart that shows the number of alerts at the current moment. Alerts are displayed by severity, so you can see the number of alerts with each severity. You can click these numbers to go to the **Alerts** page where the alerts with the selected severity are displayed.

You can configure the **Overview** page to show information only for specific hosts and/or groups using the filter editor that is reached using the **Filter** button next to the navigation menu in the left top corner of the page. The refresh interval is configured within the **Advanced Options** drop-down button from the right top corner.

In the bottom part of the **Overview** page, you can find the information on the server and a set of helpful links. You can use the colored buttons, located either to the left or on the top of the information areas depending on the pages size, to navigate to other pages. The hosts filter is pertained during the navigation.

Statistics Page

The **Statistics** page displays the monitoring statistics for specific periods of time. You can either review the summary statistics for multiple hosts or detailed monitoring statistics for specific host. Let us take a close look at each of the approaches.

Statistics Summary

In the monitoring statistics each row or card stands for a single hosts `Pic 1`. The statistics is displayed for the period chosen in the right part of the page header. You can choose between live intervals, that are configured on the **Monitoring Statistics** preference page, a set of predefined historical intervals and custom historical interval.

The view data is split to pages. The links for switching between pages as well as the combo specifying the number of entries per page are available in the bottom part of the page.

Pic 1. Statistics summary for all hosts

You can configure the **Statistics** page to show information only for specific hosts and/or groups using the filter editor that is reached using the **Filter** button next to the navigation menu in the left top corner of the page. Using the filter editor, you can also filter the page by statistical properties. The refresh interval is configured within the **Advanced Options** drop-down button from the right top corner.

Along with the statistical values, on the **Statistics** page you can find the performance characteristics, calculated on a basis of this values. The conditions for calculating the performance are provided on the **Performance** preference page. The performance values are underlined with color due to their severity, as well as the values that affect the performance.

Toolbar Overview

▤	**List** The **List** button from the **Statistics** page toolbar allows you to display the statistics in a form of a list.
▥	**Cards** The **Cards** button from the **Statistics** page toolbar allows you to display the statistics in a form of cards.
▦	**Table** The **Table** button from the **Statistics** page toolbar allows you to display the statistics in a form of a table.

You can choose between the following representations of statistics summary: list, cards and table. The corresponding buttons are available in the page contents' toolbar. Together with the information displayed, you can find additional summary characteristics, such as periods with different connection quality, in the item tooltip.

Detailed Statistics

With Ping Monitor web interface you can focus on detailed statistics for specific hosts. To reach the detailed statistics, you can click the host name hyper-link in the summary representation. As the result you drill-down to the host level, where you can review all monitoring characteristics of a host.

The detailed statistics page for a single host Pic 2 consists of the common host information, such as the host name, label and group the host is located in, displayed on the top of the page and other sections, such as host performance, tracking, latency, uptime, state and quality. Let us take a closer look on each part of the page.
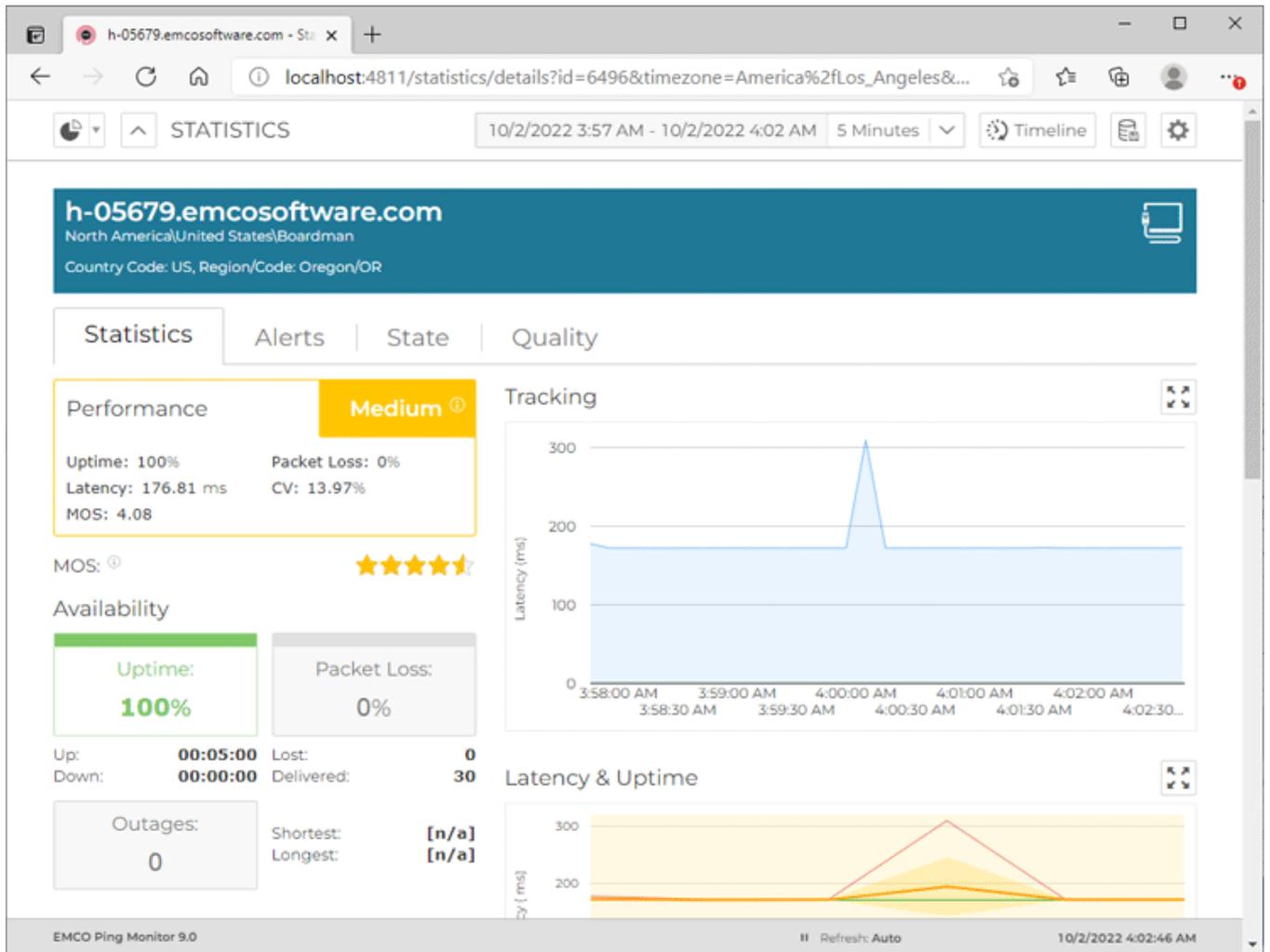
Pic 2. The detailed statistics page for a single host

Detailed host statistics is used to provide you with the integral monitoring statistics gathered during the specified period, graphically visualized and grouped by categories. The information on the page is grouped in several categories. In the left top corner, you can find the performance characteristics. Below the performance characteristics, you can find the information on host availability during the specified interval. It consists of an uptime percentage, uptime and downtime intervals, a packet loss percentage, lost and delivered packets counts and outages information.

The next category to follow is the information on latency: minimum, maximum, average, deviation and coefficient of variation. The next category is showing you the percentage and intervals of different connection quality during the specified period. The last category within the left column displaying information on monitoring activity – you can find the activity time interval and pause time interval.

On the right side of the page you can find a few statistics analysis charts. The top chart displays real-time latency tracking. It shows the actual ping statistics. In case the selected interval is longer than an hour, only the data for the latest hour is displayed due to performance reasons. Under the tracking chart you can find the latency and uptime analytics, and the bottom chart displays the analysis information for state and quality intervals. You can click on the points in both charts to open the detailed timeline for the period the point displays integral data for. Also it is possible to expand each chart to full screen using the corresponding button in the chart header Pic 3.
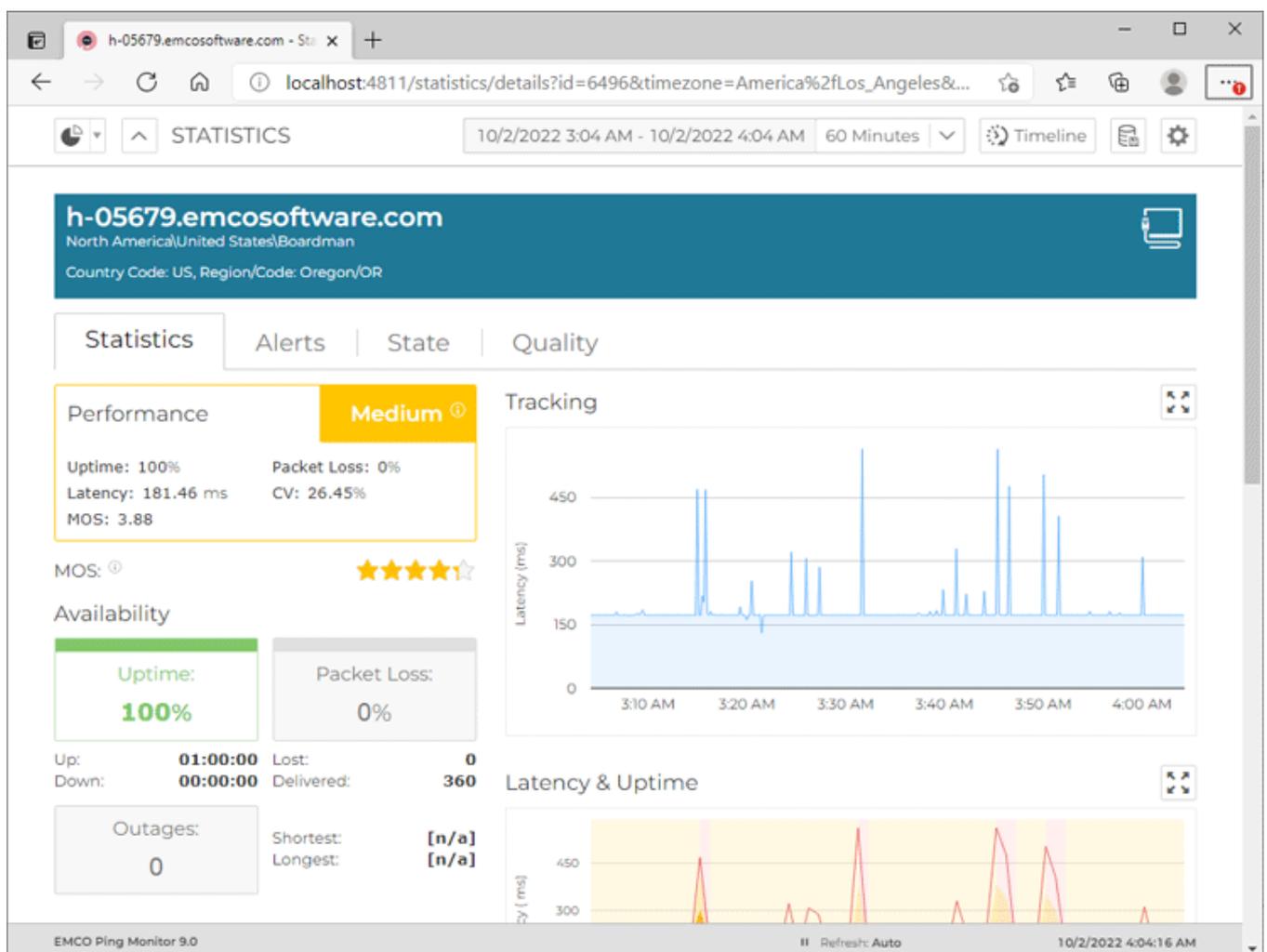
Pic 3. Tracking latency, state and quality

Under the charts you can find a table with the state and quality intervals. By default the table displays the state intervals, but you can switch from state to quality intervals and vice a versa using the buttons located at the top of the table. The table displays the list of all host state intervals for the selected period of time and the list of connection quality intervals. Let us take a closer look at this information Pic 4 .
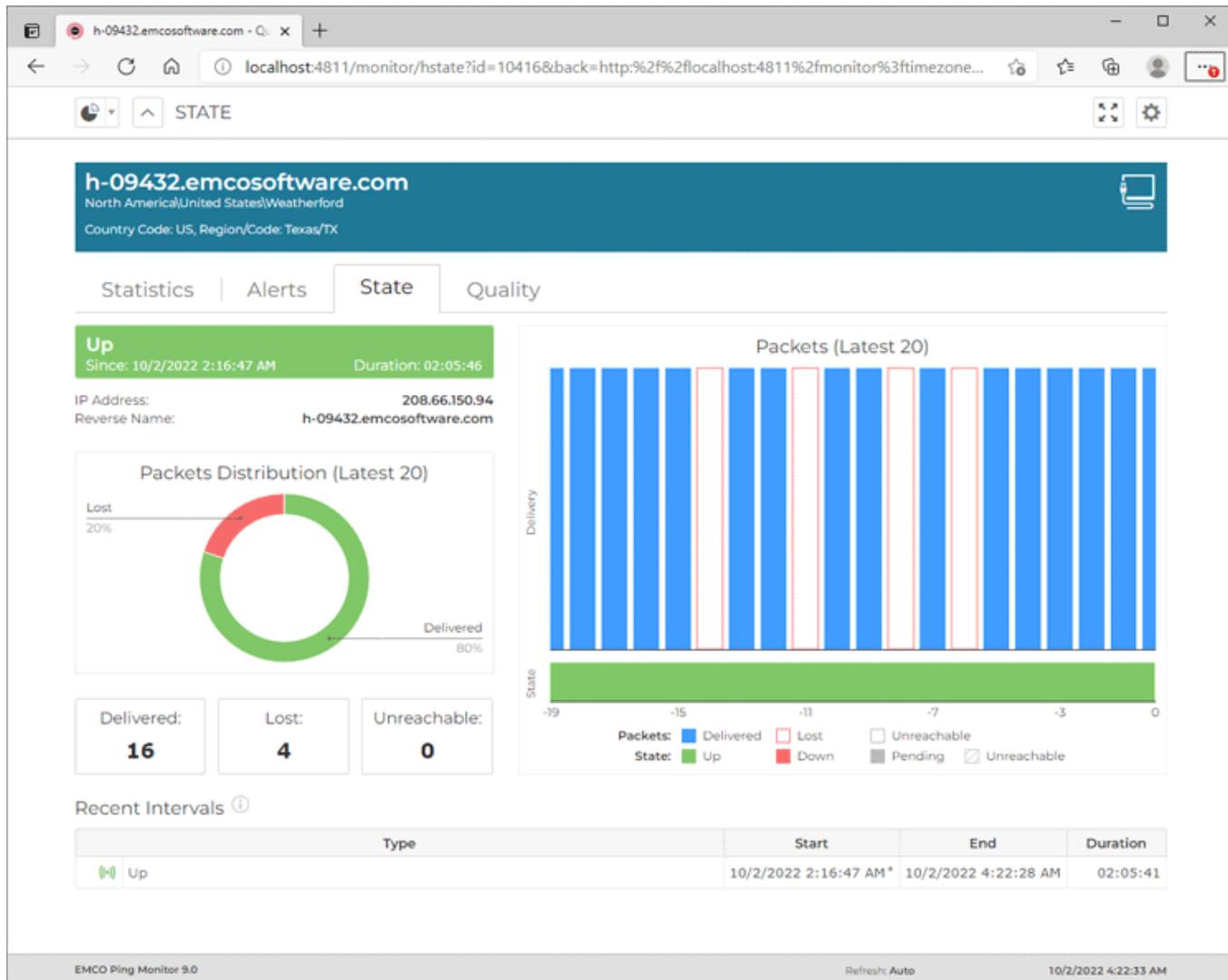
Pic 4. Reviewing state interval

The **State Intervals** and **Quality Intervals** tabs are quite similar. The first one displays the list of all host state intervals for the selected period of time and the second one – the list of connection quality intervals. Let us take a closer look at these tabs using the **State Intervals** one as the reference Pic 5. The list of intervals is displayed in a form of a tree, where the root nodes represent the specific state, and is split into pages. In case the host has been unreachable during any interval, it can be expanded to review when the host was reachable and when not. In case the comment is provided for the interval, it is displayed in root node and spanned through the child nodes, when expanded. For each interval, along with its type, you can find the start time, end time and duration. In case the interval is exceeding the selected period, the exceeding time is marked with a star. You can use the buttons above the table to display only the intervals of the specified types.

At the bottom of the page you can find a list of host events. It contains all monitoring events for the host and can be used as a monitoring log. The events are displayed in a form of a table where each row represents a single event, split into pages.

Pic 5. The host events on a single host details page

If you are facing some problems during monitoring or would like to know when the monitoring process was started and stopped, you should refer to this table.

Timeline

Ping Monitor can show you the timeline of raw ping reply data along with host state and connection quality intervals. You can open the timeline using the **Timeline** button in the header of the detailed statistics page. You can focus on specific interval of the timeline by clicking the point within **Latency & Uptime** or **State & Quality** charts.
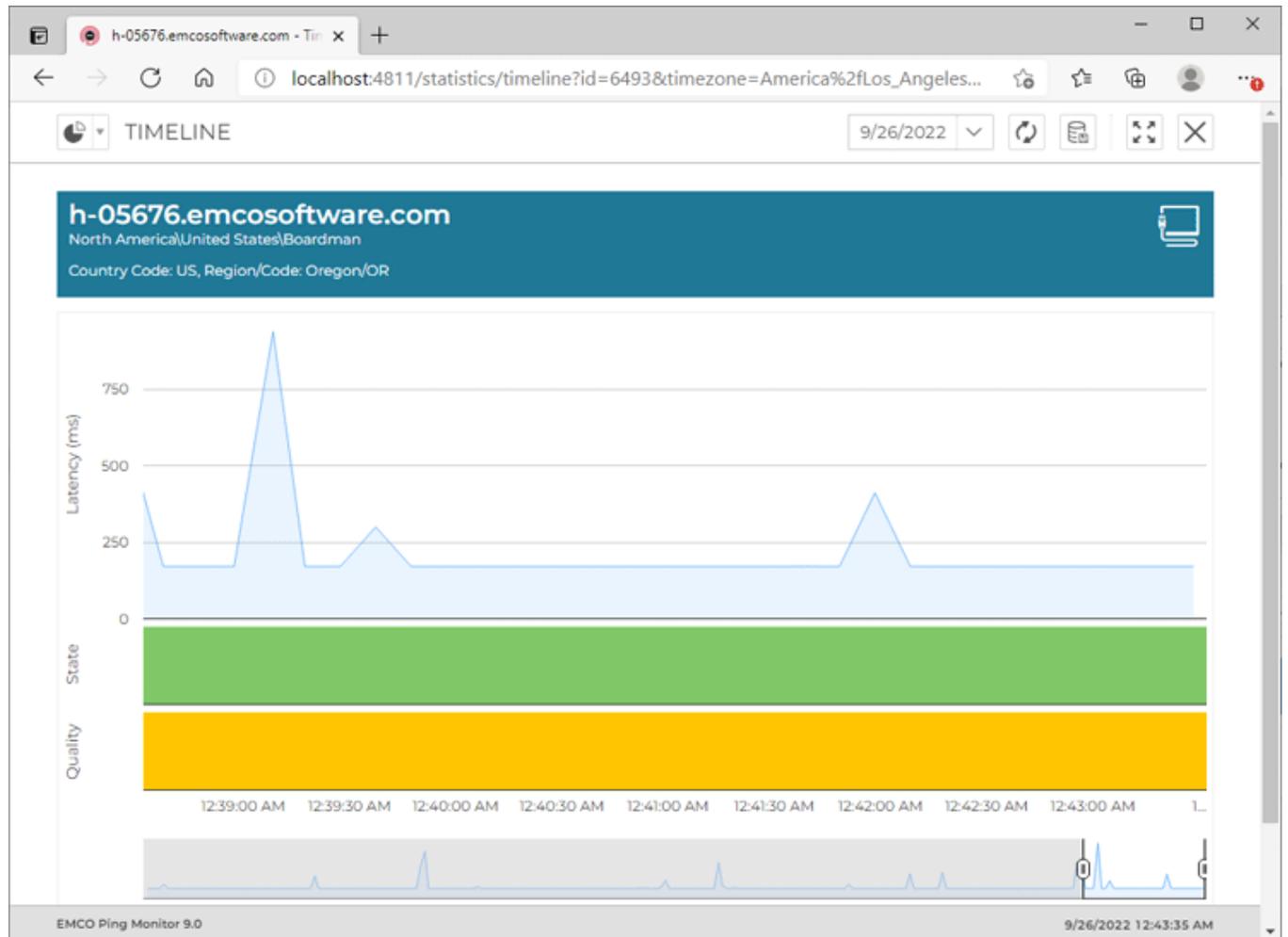
Pic 6. Timeline

On the **Timeline** page Pic 6 , you can find the timeline graph and the sliders to be used for navigation through the timeline. The timeline graph consists of three parts, those are **Latency**, **State** and **Quality**. The **Latency** part is used to display the ping replies data, the **State** part reflects the state intervals on the timeline and the **Quality** part is used for displaying the quality intervals.

The timeline range is limited to 30 days due to performance reasons. You can change the timeline range using the period combo in the page header. To actualize ping replies data along with state and quality intervals, use the **Refresh** button from the header. The **Export Raw Data** button can be used to export raw ping replies data to a CSV format, and the **Full Screen** button allows you to expand the time line to full screen.

Alerts Page

The **Alerts** page is designed to display information about the current alerts. All alerts detected for all hosts are displayed in the table, where each rows represents an alert and columns shows the alert details, such as the alert name, host name, duration of the alert and its severity `Pic 1`.
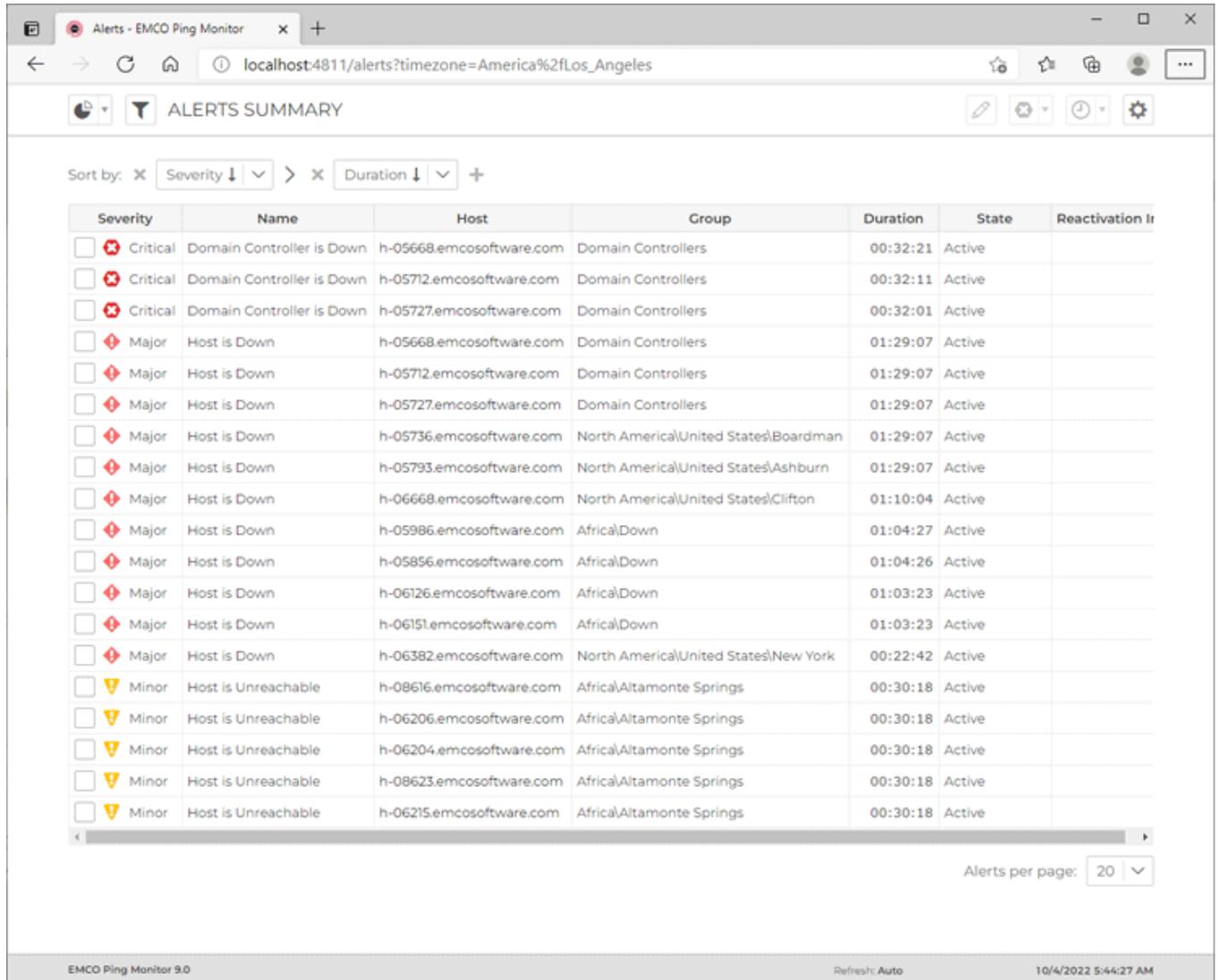
Pic 1. Alerts page

The displayed list can be sorted by one or multiple fields. By default it is sorted by alert severity and duration. You can edit an alert by selecting it and pressing the **Edit** button available on the toolbar. You can change alert severity and acknowledge the alert for a selected time interval or indefinitely. It is possible to filter displayed alerts to show active or acknowledged alerts only.

Pic 2. Host alerts

The **Alerts** page displays alerts for all hosts, but you can click a host name in the table to drill-down to the host level and review alerts for the selected host. The alerts list for a host is similar to the list of alerts for all hosts, but it displays current alerts for the selected host only.

State Page

The **State** page is designed to be used for focusing on hosts states monitoring, where you can easily detect any problematic situations just in time. The page displays only those hosts the monitoring is currently active for. It is possible to monitor per-host states as well as the states distribution for groups of hosts. The default data representation on page is organized with the help of tiles displaying the objects being monitored, that are colored to indicate of the hosts states. Alternatively the hosts state information can be represented as a table. Let us take a closer look at the page. To open the **State** page you need to select the **State Summary** item in the main menu.

State Summary

When you click the **State Summary** item in the main menu, you navigate to the page that displays state information for multiple hosts. By default this page represents hosts as tiles `Pic 1`. Each tile in the page represents a single host that is currently monitored and is colored with the host state color: green – for up, red – for down, and gray – for pending. In case the host is currently unreachable, thus the state is represented with the latest reachable one, the tile is hatched.

Pic 1. Monitoring hosts state

Together with the state, for each host you can find out how long has the host been in this state, the group the host is located in, the host IP address and resolved reverse name. All these information is available in the tool-tip and on the tile itself, when the large tiles are used. For medium tiles, you can see the host name and label on the tile together with the state time stamp. The small tiles are simply filled with the host state color – any information is available in the tool-tip only.
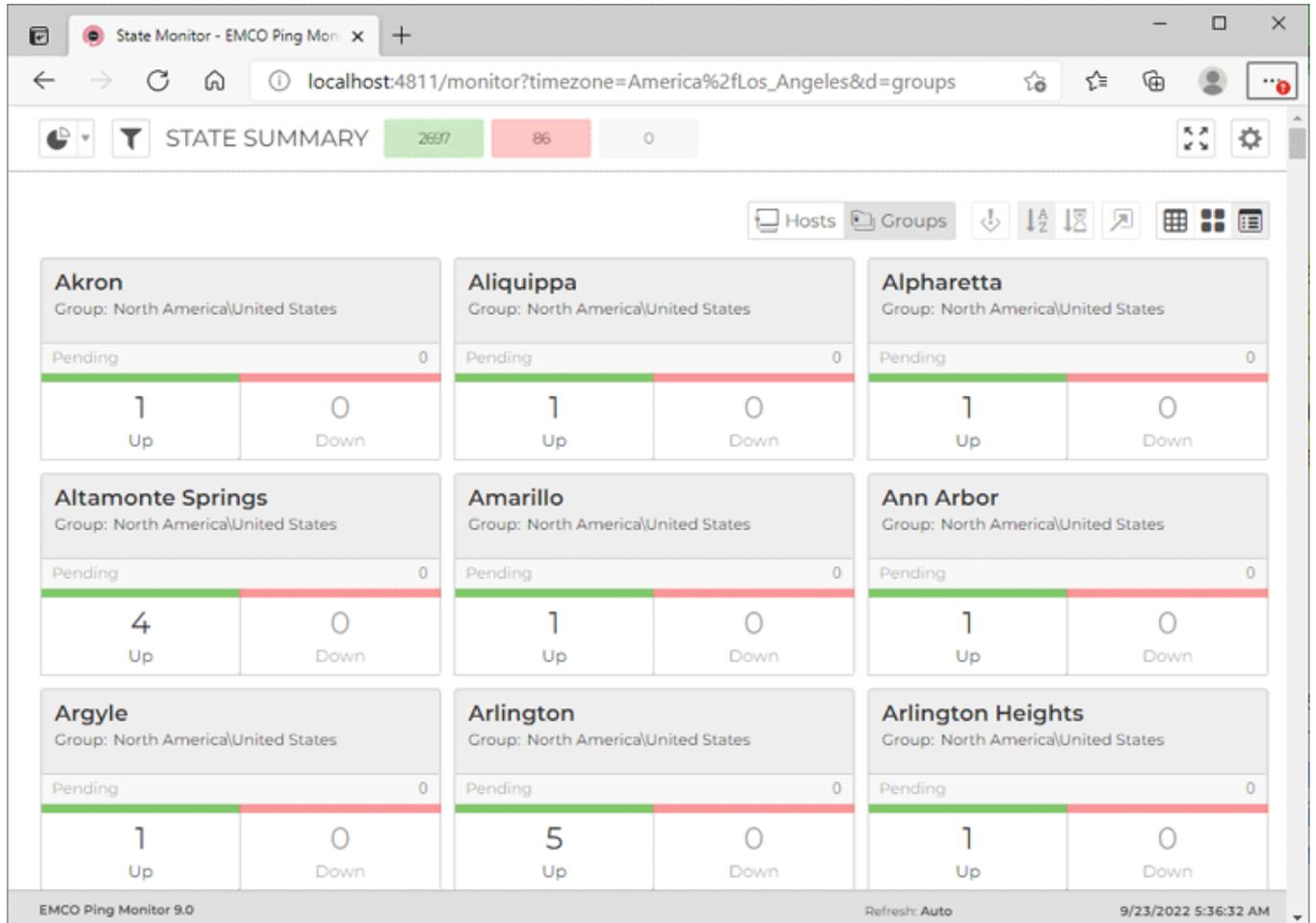
Pic 2. Monitoring state for groups of hosts

Together with per-host state monitoring, it is possible to monitor state for host groups. The group tile can either represent the group or the set of individual hosts (selected individually or not belonging to any group) **Pic 2**. The group tile is displaying the number of hosts within the group that are currently in specific states. When monitoring state in grouped mode, you can click on the group to focus on hosts from that group, or click on the specific state part within a group to focus on hosts with that specific state.

You can switch between different modes using the corresponding buttons on the toolbar.

Toolbar Overview

Hosts

The **Hosts** button is used to configure the page for monitoring each host individually.

Groups	**Groups** The **Groups** button is used to configure the page for monitoring groups of hosts.
⬇	**Group by Severity** The **Group by Severity** button allows you to group the page the way that the problematic nodes are always displayed on top.
↓A/Z	**Sort by Name** When monitoring hosts, the **Sort by Name** button enables the page sorting by entry name.
↓⧗	**Sort by Time** When monitoring hosts, the **Sort by Time** button enables the page sorting by state change time stamp.
↗	**Focus on Problems** The **Focus on Problems** button allows you to configure the page to be automatically scrolled to entries that go down, when grouped by severity and sorted by time.
⊞	**Table** The **Table** button switches the page to the table data representation.
⣿	**Small** The **Small** button switches the page to the mode where each monitored host is represented just with a pictogram describing its state. Any other information on the entry is available in the tool tip only.
▪▪	**Medium** The **Medium** button is used to switch to the mode where each entry is represented with a tile containing only the summary information on the entry. The detailed info is available in the tool tip.
▤	**Large** The **Large** button enables the mode where a tile representing each entry contains maximum information on the entry being monitored.

All entries within the **State Summary** page can be grouped by severity so that the problematic entries are always on top. To enable such grouping, use the **Group by Severity** button on the toolbar. For example, when enabled, the hosts, that are down, will be displayed on top, then hosts that are up will follow the down ones, then there will be the hosts with the pending state. To switch between tiles of different size, use the **Small**, **Medium** and **Large** buttons.

You can configure the **State Summary** page to show information only for specific hosts and/or groups using the filter editor that is reached using the **Filter** button next to the navigation menu in the left top corner of the page. Using the filter editor, you can also filter the page to display hosts with specific states. The refresh interval is configured within the **Advanced Options** drop-down button from the right top corner.

Pic 3. State Summary represented as a table

The **State Summary** page can display host state information as a table. To activate table representation you need to click the **Table** button on the toolbar. In the table mode each host is displayed as a row, you can see host name, state and other information as columns.

Host State

You can also focus on monitoring specific hosts. To monitor single host, just click the tile the host is represented with. As the result you drill-down to the host level. The page containing the monitoring details for this host will be displayed **Pic 4**.
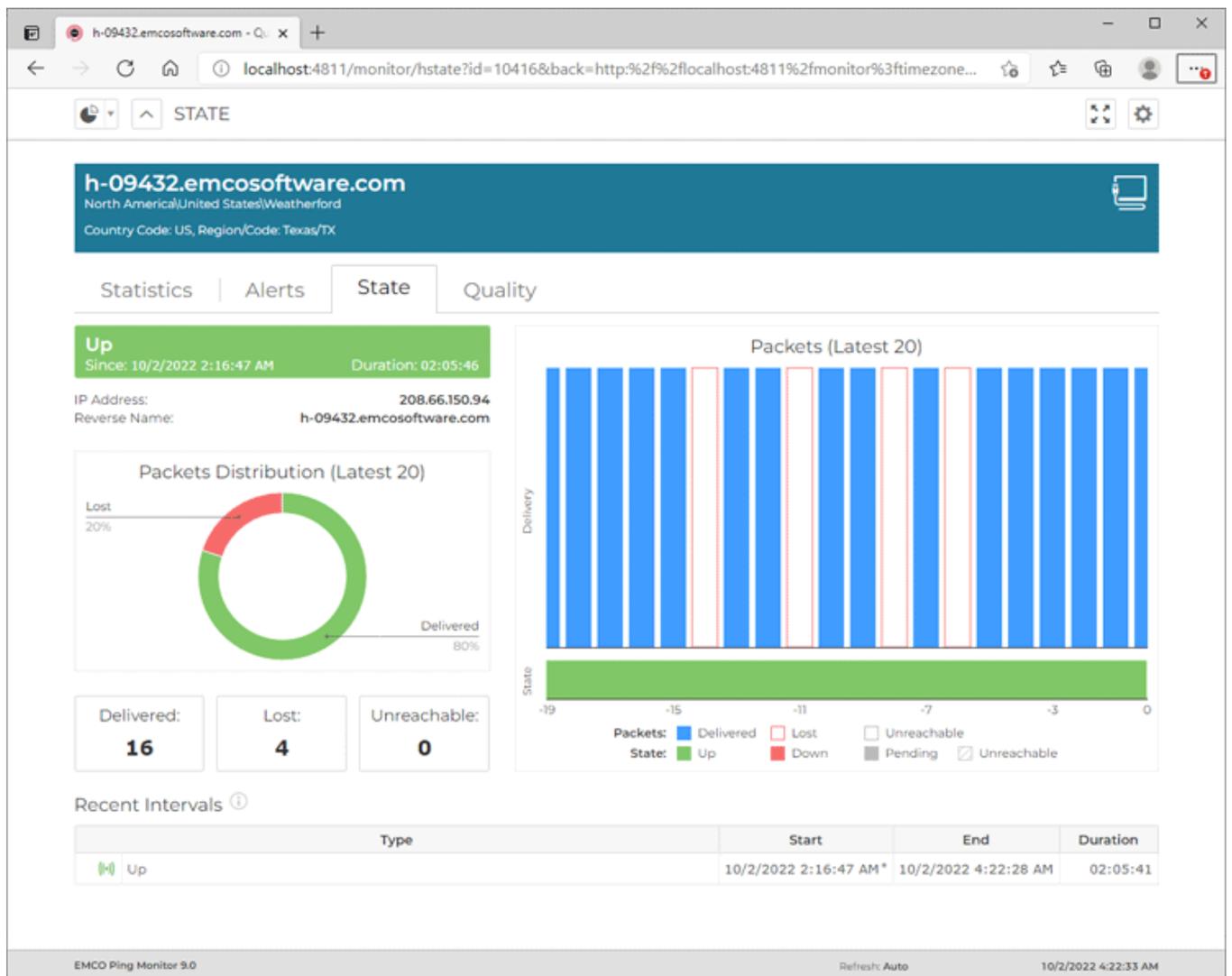
Pic 4. Monitoring state for a single host

On the detailed state monitor page, in the left top corner you can find the block that is quite similar to the large tile representing the host and contains the same information. Below this block, you can view the information on the distribution for the twenty latest packets. To the right those latest packets are displayed in the chronological order as well as the host state that is reached after each response.

On the bottom of the detailed sate monitor page you can find the area with recent state intervals (state changes). It displays all states the host had during the last hour.

Quality Page

The **Quality** page is designed to be used for focusing on connection quality monitoring, where you can easily detect any problematic situations just in time. The page displays only those hosts the monitoring is currently active for. It is possible to monitor per-host connection quality as well as the qualities distribution for groups of hosts. By default the page is organized with the help of tiles representing the objects being monitored, but it is possible to display data as a table. To open the page you need to click the **State Summary** item in the main menu. Let us take a closer look at the page.

Quality Summary

To display the connection quality information for monitored hosts you need to select the **Quality Summary** item in the main menu. The connection quality information on the screen is represented as tiles, where each tile represents a single host **Pic 1**. For the hosts that are monitored, the connection quality is calculated based on the rules defined in the program preferences and/or host settings. The tile is filled with red color in case all packets from the sample used to calculate the connection quality are lost, thus the quality is critical. In other cases, the quality value is displayed with the help of the colored tag on the right of the tile: green – for good quality, yellow – for warning, red – for bad, and gray – for pending. In case the host is currently unreachable, thus the quality is represented with the latest reachable one, the tile is hatched.

Pic 1. Monitoring hosts connection quality

169
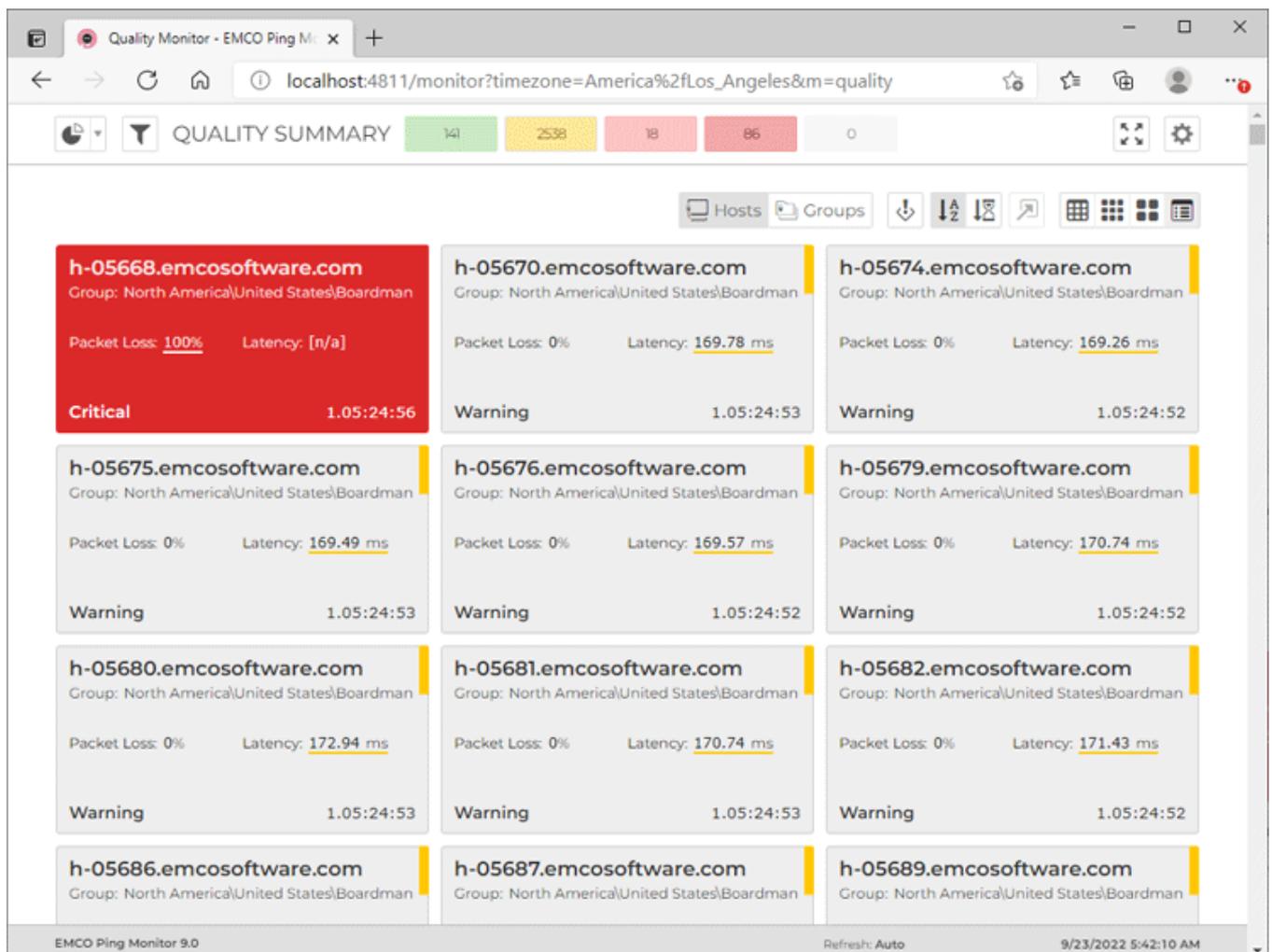
The first mode of the **Quality Monitor** page we are going to introduce is the per-host connection quality monitoring `Pic 1`. This is the default mode, where each tile represents a single host. For the hosts that are monitored, the connection quality is calculated based on the rules defined in the program preferences and/or host settings. The tile is filled with red color in case all packets from the sample used to calculate the connection quality are lost, thus the quality is critical. In other cases, the quality value is displayed with the help of the colored tag on the right of the tile: green – for good quality, yellow – for warning, red – for bad, and gray – for pending. In case the host is currently unreachable, thus the quality is represented with the latest reachable one, the tile is hatched.

On the large tiles, for each host you can find the parameters used to calculate the quality and to see which parameter is leading to the warning or bad quality value. The same way as for the state, you can see how long has the host connection had this or that value. The smaller the tile the less information is available immediately, but there is still a whole set of values in the tool-tip.
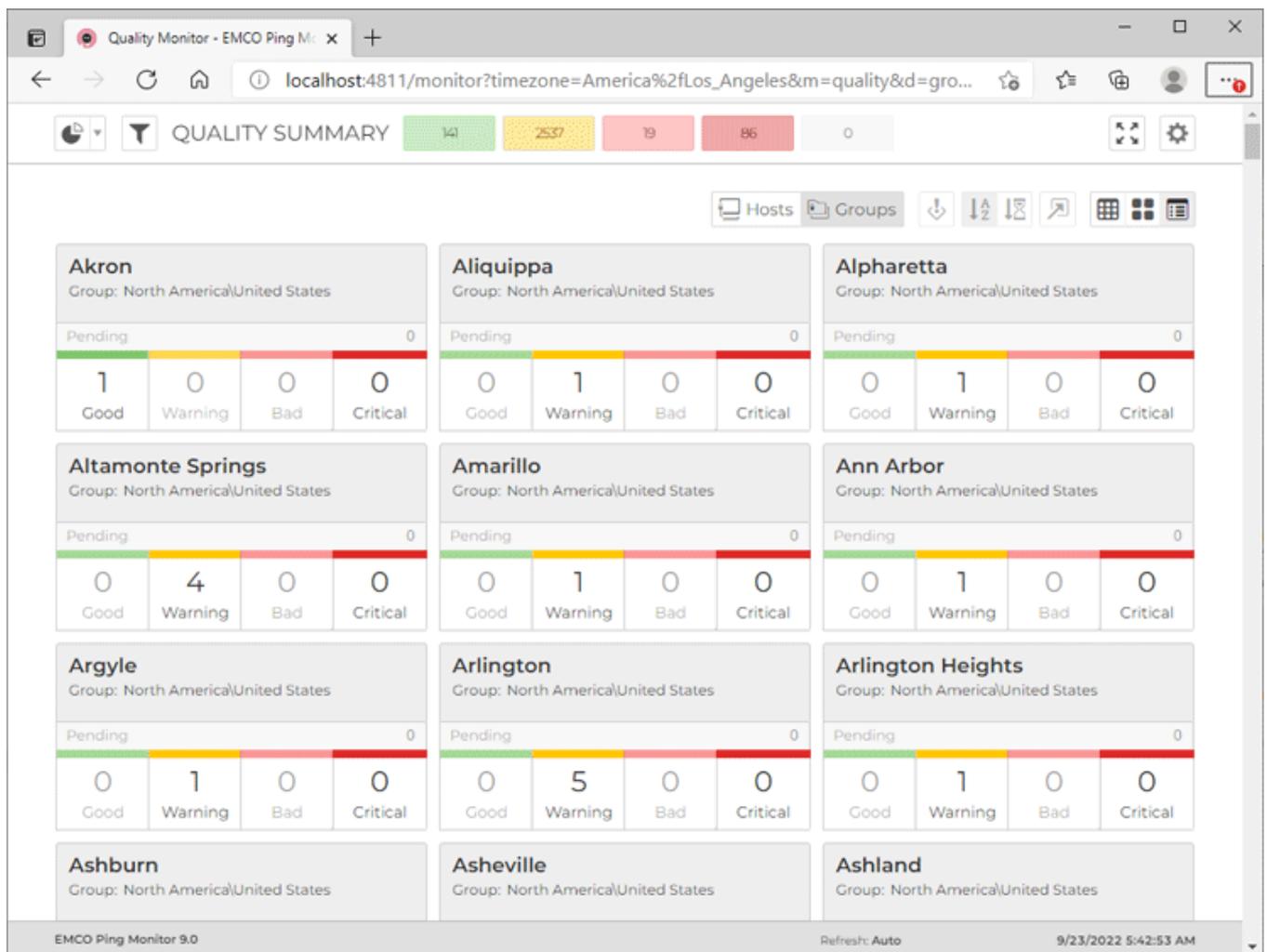
Pic 2. Monitoring connection quality for groups of hosts

Together with per-host connection quality monitoring, it is possible to monitor connection quality for host groups. The group tile can either represent the group or the set of individual hosts (selected individually or not belonging to any group) `Pic 2`. The group tile is displaying the number of hosts within the group having specific connection quality. When monitoring connection quality in grouped mode, you can click on the group to focus on hosts from that group, or click on the specific connection quality part within a group to focus on hosts having that specific connection quality.

You can switch between different modes using the corresponding buttons on the toolbar.

Toolbar Overview

Hosts	**Hosts** The **Hosts** button is used to configure the page for monitoring each host individually.
Groups	**Groups** The **Groups** button is used to configure the page for monitoring groups of hosts.
⬇	**Group by Severity** The **Group by Severity** button allows you to group the page the way that the problematic nodes are always displayed on top.
↓A Z	**Sort by Name** When monitoring hosts, the **Sort by Name** button enables the page sorting by entry name.
↓⌛	**Sort by Time** When monitoring hosts, the **Sort by Time** button enables the page sorting by connection quality change time stamp.
↗	**Focus on Problems** The **Focus on Problems** button allows you to configure the page to be automatically scrolled to entries where connection quality goes critical, when grouped by severity and sorted by time.
⊞	**Table** The **Table** button switches the page to the table data representation.
⣿	**Small** The **Small** button switches the page to the mode where each monitored host is represented just with a pictogram describing its connection quality. Any other information on the entry is available in the tool tip only.
▪▪	**Medium** The **Medium** button is used to switch to the mode where each entry is represented with a tile containing only the summary information on the entry. The detailed info is available in the tool tip.
▤	**Large** The **Large** button enables the mode where a tile representing each entry contains maximum information on the entry being monitored.

All entries on the **Quality Summary** page can be grouped by severity so that the problematic entries are always on top. To enable such grouping, use the **Group by Severity** button on the toolbar. For example, when enabled, the hosts with the critical connection quality will be displayed

on top, then hosts with the bad connection quality will follow, then there will be the hosts with the warning quality, and so on. To switch between tiles of different size, use the **Small**, **Medium** and **Large** buttons.

You can configure the **Quality Summary** page to show information only for specific hosts and/or groups using the filter editor that is reached using the **Filter** button next to the navigation menu in the left top corner of the page. Using the filter editor, you can also filter the page to display hosts with specific connection quality. The refresh interval is configured within the **Advanced Options** drop-down button from the right top corner.

Pic 3. Quality Summary represented as a table

The **Quality Summary** page can display host connection quality information as a table. To activate table representation you need to click the **Table** button on the toolbar. In the table mode each host is displayed as a row, you can see host name, quality and other information as columns.

Host Quality

You can also focus on monitoring specific hosts. To monitor single host, just click the tile the host is represented with. As the result you drill-down to the host level. The page containing the monitoring details for this host will be displayed **Pic 4**.
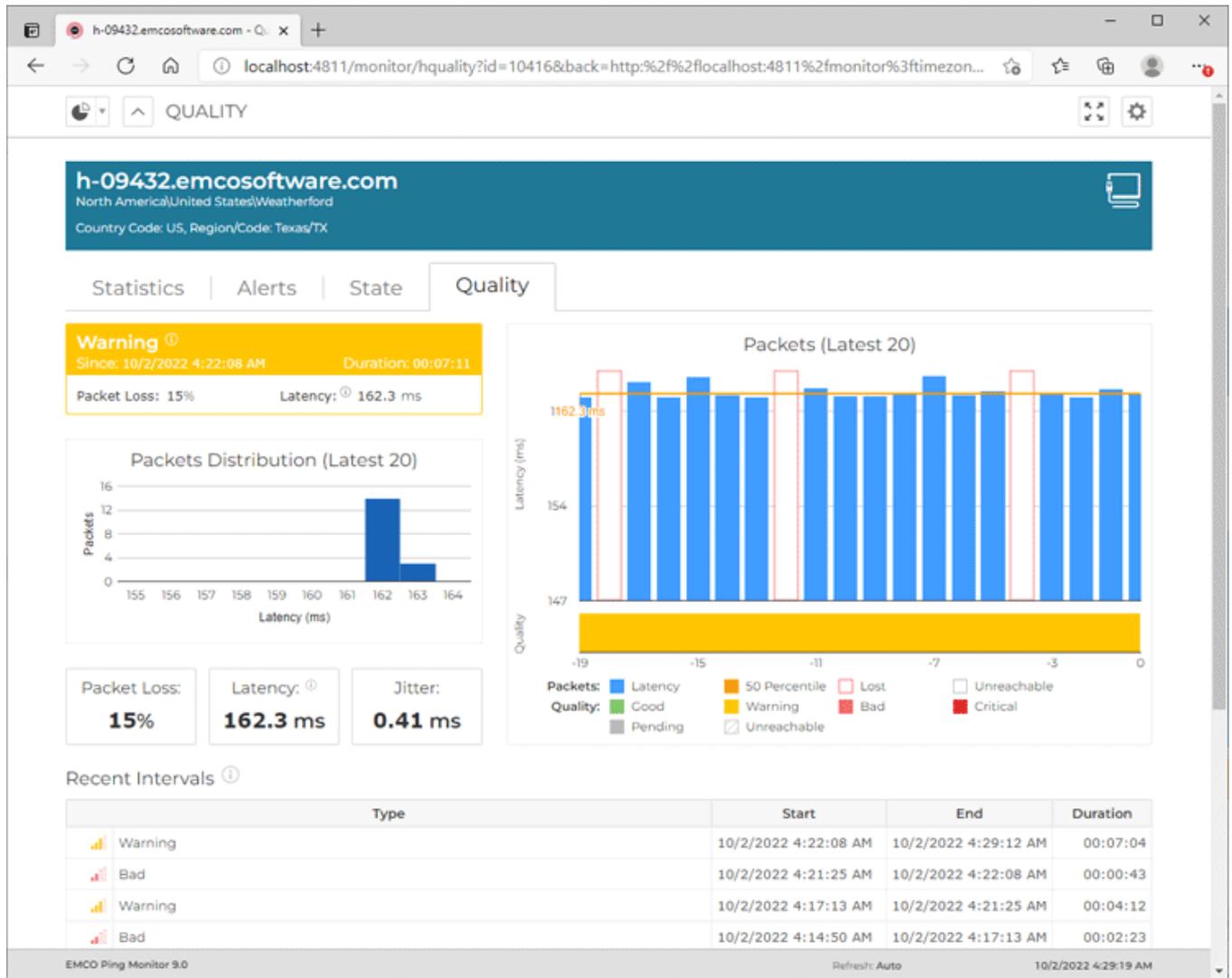
Pic 4. Monitoring connection quality for a single host

On the detailed connection quality monitor page, in the left top corner you can find the block that is quite similar to the large tile representing the host and contains the same information. Below this block, you can view the information on the distribution for the packets from a sample used to calculate the connection quality. Below the packets distribution, you can find the connection quality characteristics. To the right those latest packets are displayed in the chronological order as well as the connection quality that is reached after each response.

On the bottom of the detailed connection quality monitor page you can find the area with recent quality intervals. It is used to display the most recent quality intervals (quality changes) that occurred during the last hour.

Hosts Page

The **Hosts** page `Pic 1` was primarily designed for performing monitoring activity management as well as host state and connection quality monitoring. It can displays hosts available in the program split into pages.
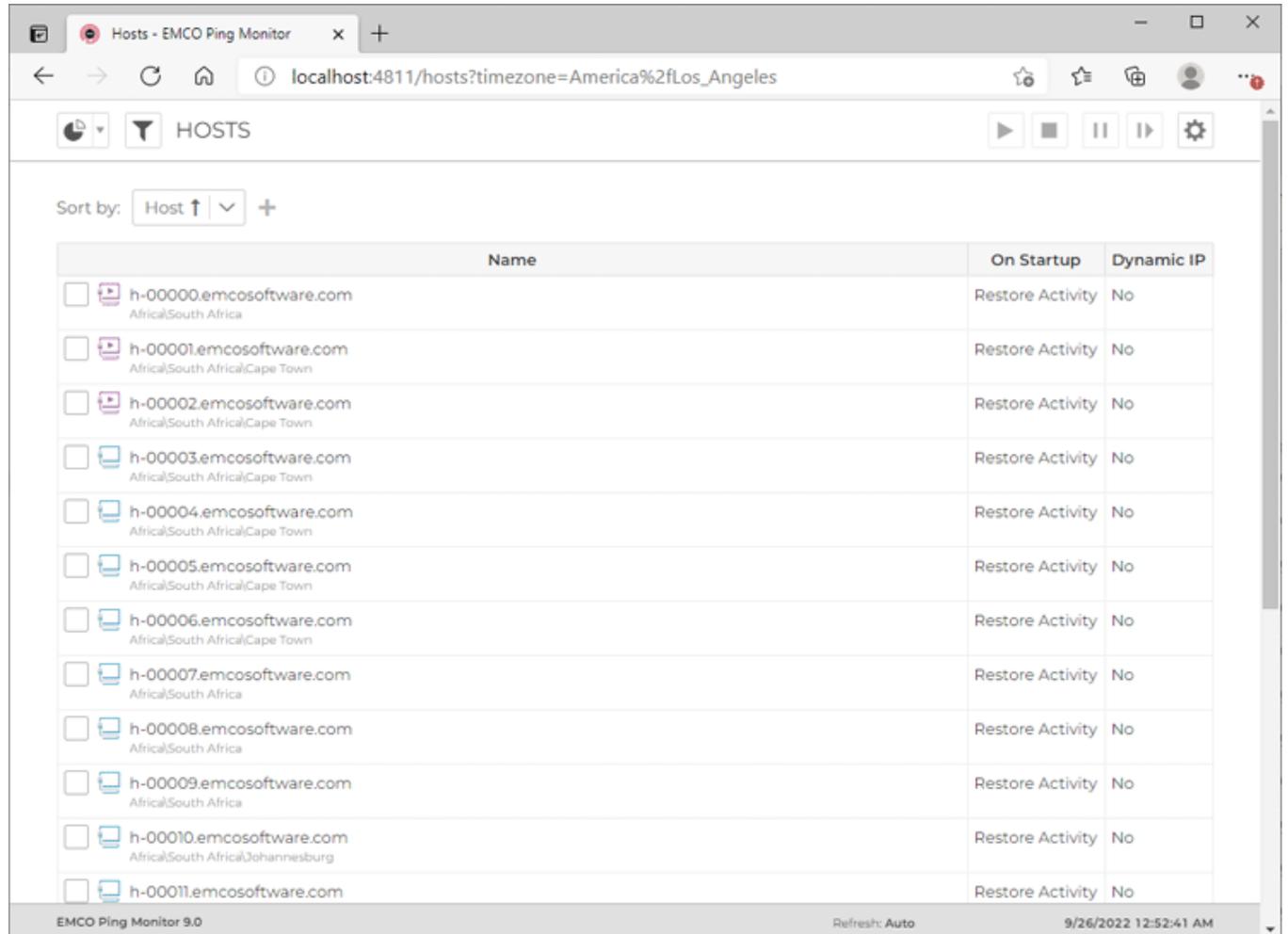
Pic 1. The Hosts page

On the **Hosts** page you can find the current monitoring activity for each host. For all hosts the monitoring is currently active, you can see its state and connection quality, as well as the connection quality characteristics. The host state, connection quality and the characteristics used for quality calculation are underlined with the severity color.

You can configure the **Hosts** page to show information only for specific hosts and/or groups using the filter editor that is reached using the **Filter** button next to the navigation menu in the left top corner of the page. Using the filter editor, you can also filter the page by monitoring activity, hosts state and connection quality. The refresh interval is configured within the **Advanced Options** drop-down button from the right top corner.

> ▶ **Start**
>
> The **Start** button from the **Hosts** page header can be used to start the monitoring process for the checked hosts.

	Stop The **Stop** button from the **Hosts** page header allows you to stop the monitoring process for the checked hosts.
	Pause The **Pause** button from the **Hosts** page header can be used to pause the monitoring process for the checked hosts.
	Resume The **Resume** button from the **Hosts** view toolbar is used to resume the monitoring process for the checked hosts.
	List The **List** button from the **Hosts** page toolbar switches the page to the list representation of hosts providing you with maximum details.
	Table The **Table** button from the **Hosts** page toolbar switches the page to the compact table representation of hosts.

To control the monitoring activity, check the hosts in the view and use the **Start**, **Stop**, **Pause** and **Resume** buttons from the page header. It is possible to switch between the list and table representations of hosts using the **List** and **Table** items on the toolbar and in the popup menu. These representations provide different level of detail.

Chapter 8: Using Placeholders

Ping Monitor supports a flexible configuration of custom actions definitions, report file names and e-mail message templates - this flexibility is achieved by allowing the use of placeholders to form the templates and command line parameters of actions. This part of the guide describes the placeholders that can be used in templates for notification messages sent by e-mail in case of certain events, in report file names and in definitions of custom actions.

Notification E-mail Placeholders

This part of the guide describes the placeholders that can be used in the templates for the notification messages sent by e-mail in case of certain events. There are state and quality notification messages, summary report messages and detailed report messages. Each of them is described below. Along with the described placeholders, you can use the custom fields, if defined.

Host State Notifications

Host state notification placeholders can be used for notification messages that are sent when the host state changes. The following placeholders can be used:

%REMOTE_HOST%	the remote host being monitored, including the host label, if defined;
%REMOTE_HOST_ADDRESS%	the address of the remote host being monitored;
%REMOTE_HOST_LABEL%	the label of the remote host being monitored;
%REMOTE_HOST_IP%	the resolved IP address of the remote host;
%REMOTE_HOST_GROUP%	the group the remote host belongs to;
%REMOTE_HOST_DESCRIPTION%	the description of the remote host being monitored;
%STATE%	the current host state, either Up or Down;
%CONNECTION_STATUS%	the current connection status. It can be either 'lost', or 'restored'. For the 'lost' status, the reason for ping failure is added. If you do not want to see the reason, use the '%SHORT_CONNECTION_STATUS%' placeholder;
%SHORT_CONNECTION_STATUS%	the current connection status. It can be either 'lost', or 'restored'. The reason for ping failure is never added;
%CHANGE_TIME%	the date and time the connection status was changed at;
%OCCURRENCE%	the number of notification sent for this event (useful for recurring notifications);
%LOCAL_HOST%	the machine name;
%RUNNING_PRODUCT%	the running program name;
%PRODUCT_VERSION%	the current version of the running program;
%TIME%	the current time;
%DATE%	the current date;
%DATETIME%	the current date and time;
%UTC_OFFSET%	the current UTC offset;

%YEAR%	the current year.

In case of the **On Connection Restore** notification, you can use the following additional placeholders:

%OUTAGE_DURATION%	the duration of the outage that has ended;
%OUTAGE_START_TIME%	the start time of the outage that has ended;
%OUTAGE_END_TIME%	the end time of the outage that has ended.

Connection Quality Notifications

Connection quality notification placeholders can be used for notification messages that are sent when the connection quality changes. The following placeholders can be used:

%REMOTE_HOST%	the remote host being monitored, including the host label, if defined;
%REMOTE_HOST_ADDRESS%	the address of the remote host being monitored;
%REMOTE_HOST_LABEL%	the label of the remote host being monitored;
%REMOTE_HOST_IP%	the resolved IP address of the remote host;
%REMOTE_HOST_GROUP%	the resolved IP address of the remote host;
%REMOTE_HOST_DESCRIPTION%	the description of the remote host being monitored;
%QUALITY%	the current connection quality, one of the following: Good, Warning, Bad or Critical;
%CHANGE_TIME%	the date and time the connection status was changed at.
%OCCURRENCE%	the number of notification sent for this event (useful for recurring notifications);
%LOCAL_HOST%	the machine name;
%RUNNING_PRODUCT%	the running program name;
%PRODUCT_VERSION%	the current version of the running program;
%TIME%	the current time;
%DATE%	the current date;
%DATETIME%	the current date and time;
%UTC_OFFSET%	the current UTC offset;
%YEAR%	the current year.

Summary Report

For the e-mail messages, sent as summary reports you can use the following placeholders:

%REPORT_NAME%	the name of the generated report;
%REPORT_DESCRIPTION%	the description of the generated report;
%REPORT_TYPE%	the type of the generated report;
%REPORT_PERIOD%	the period the report is generated for;

%SUMMARY_TABLE%	the table with the summary information on hosts availability and ping performance;
%LOCAL_HOST%	the machine name;
%RUNNING_PRODUCT%	the running program name;
%PRODUCT_VERSION%	the current version of the running program;
%TIME%	the current time;
%DATE%	the current date;
%DATETIME%	the current date and time;
%UTC_OFFSET%	the current UTC offset;
%YEAR%	the current year.

Detailed Report

For the detailed report, the message body is generated for each host separately, and the header and footer are generated only once. So, the placeholders standing for any information on a single host can be used only within the message body. The following placeholders are available:

%REPORT_NAME%	the name of the generated report;
%REPORT_DESCRIPTION%	the description of the generated report;
%REPORT_TYPE%	the type of the generated report;
%REPORT_PERIOD%	the period the report is generated for;
%REMOTE_HOST_EXT%	the remote host being monitored, including the host label, if defined, and footnote sign, if required;
%REMOTE_HOST%	the remote host being monitored, including the host label, if defined;
%REMOTE_HOST_ADDRESS%	the address of the remote host being monitored;
%REMOTE_HOST_LABEL%	the label of the remote host being monitored;
%REMOTE_HOST_GROUP%	the group the remote host belongs to;
%REMOTE_HOST_DESCRIPTION%	the description of the remote host being monitored;
%ACTIVITY_TIME%	the time span the host was monitored for during the report period;
%PAUSE_TIME%	the time span the host monitoring was paused for during the report period;
%MIN_LATENCY%	the smallest value from all round-trip times of packets successfully delivered during the report period in milliseconds;
%MAX_LATENCY%	the largest value from all round-trip times of packets successfully delivered during the report period in milliseconds;
%AVG_LATENCY%	the arithmetic mean of all round-trip times of packets successfully delivered during the report period in milliseconds;

%LATENCY_DEVIATION%	the standard deviation from the average latency value for all round-trip times of packets successfully delivered during the report period in milliseconds;
%LATENCY_CV%	the percentage ratio of the latency deviation to the average latency calculated for all round-trip times of packets successfully delivered during the specified time period;
%UPTIME%	the percentage ratio of the host uptime to the whole non-pending time during the report period;
%OUTAGES_COUNT%	the number of outages that took place during the report period;
%UPTIME_INTERVAL%	a time span the connection to the host was up during the report period;
%DOWNTIME_INTERVAL%	a time span the connection to the host was down during the report period;
%SHORTEST_OUTAGE%	the shortest outage that took place during the report period;
%LONGEST_OUTAGE%	the longest outage that took place during the report period;
%PACKET_LOSS%	the percentage ratio of the number of lost packets to the number of packets being sent during the report period;
%LOST_PACKETS_COUNT%	the number of lost packets during the report period;
%DELIVERED_PACKETS_COUNT%	the number of delivered packets during the report period;
%MOS%	the mean opinion score, a well-established metric for obtaining the quality of VoIP based on the latency characteristics and packet loss percentage for all packets sent during the report period;
%GOOD_QUALITY_PERCENTAGE%	the percentage ratio of the time with good connection quality to the whole non-pending time during the report period;
%WARNING_QUALITY_PERCENTAGE%	the percentage ratio of the time with warning connection quality to the whole non-pending time during the report period;
%BAD_QUALITY_PERCENTAGE%	the percentage ratio of the time with bad connection quality to the whole non-pending time during the report period;
%CRITICAL_QUALITY_PERCENTAGE%	the percentage ratio of the time with critical connection quality to the whole non-pending time during the report period;
%GOOD_QUALITY_INTERVAL%	a time span the connection quality to the host was good during the report period;
%WARNING_QUALITY_INTERVAL%	a time span the connection quality to the host was warning during the report period;
%BAD_QUALITY_INTERVAL%	a time span the connection quality to the host was bad during the report period;
%CRITICAL_QUALITY_INTERVAL%	a time span the connection quality to the host was critical during the report period;
%UPTIME_COLOR%	the color used to draw the uptime box;

%PACKET_LOSS_COLOR%	the color used to draw the packet loss box;
%OUTAGES_COLOR%	the color used to draw the outages box;
%DEVIATION_COLOR%	the color used to draw the deviation box;
%CV_COLOR%	the color used to draw the CV box;
%AVERAGE_COLOR%	the color used to draw the average latency box;
%GOOD_QUALITY_COLOR%	the color used to draw the good quality box;
%WARNING_QUALITY_COLOR%	the color used to draw the warning quality box;
%BAD_QUALITY_COLOR%	the color used to draw the bad quality box;
%CRITICAL_QUALITY_COLOR%	the color used to draw the critical quality box;
%PERFORMANCE_INFO%	the information on performance calculated for the report period;
%STATE_INTERVALS_TABLE%	detailed information on host state intervals for the report period in a form of a table, where each row stands for the interval of the specific type;
%QUALITY_INTERVALS_TABLE%	detailed information on connection quality intervals for the report period in a form of a table, where each row stands for the interval of the specific type;
%EVENTS_TABLE%	detailed information on monitoring events taken place during the report period in a form of a table;
%MOS_RATING_IMAGE%	the content ID of the image for the 5-star rating representation of MOS (HTML message format only);
%STATISTICS_ANALYSIS_CHART%	the content ID of the image with latency and uptime chart (HTML message format only);
%INTERVALS_ANALYSIS_CHART%	the content ID of the image with state and quality chart (HTML message format only);
%LOCAL_HOST%	the machine name;
%RUNNING_PRODUCT%	the running program name;
%PRODUCT_VERSION%	the current version of the running program;
%TIME%	the current version of the running program;
%DATE%	the current date;
%DATETIME%	the current date and time;
%UTC_OFFSET%	the current UTC offset;
%YEAR%	the current year.

Custom Actions Definition Placeholders

This part of the guide describes the placeholders that can be used in custom actions definitions. You can use these placeholders for forming both the path to the action to be executed and the command line parameters of the action. Do not forget to quote the placeholder or the combination of placeholders used as a command line parameter. The following placeholders can be used for the custom actions definition:

%REMOTE_HOST%	the remote host being monitored, including the host label, if defined;
%REMOTE_HOST_ADDRESS%	the address of the remote host being monitored;
%REMOTE_HOST_LABEL%	the label of the remote host being monitored;
%REMOTE_HOST_IP%	the resolved IP address of the remote host;
%REMOTE_HOST_GROUP%	the group the remote host belongs to;
%REMOTE_HOST_DESCRIPTION%	the description of the remote host being monitored;
%CHANGE_TIME%	the date and time the notification is triggered at;
%OCCURRENCE%	the number of action called for this event (useful for recurring notifications);
%LOCAL_HOST%	the name of the machine on which the product is running;
%RUNNING_PRODUCT%	the running product name;
%PRODUCT_VERSION%	the current version of the running product;
%TIME%	the current time in a long format;
%DATE%	the current date in a short format;
%DATETIME%	the current date with the current time;
%UTC_OFFSET%	the current UTC offset;
%YEAR%	the current year.

For the actions handling host state changes, you can also use the following placeholders:

%STATE%	the current host state, either Up or Down;
%CONNECTION_STATUS%	the current connection status. It can be either 'lost', or 'restored'. For the 'lost' status, the reason for ping failure is added. If you do not want to see the reason, use the '%SHORT_CONNECTION_STATUS%' placeholder;
%SHORT_CONNECTION_STATUS%	the current connection status. It can be either 'lost', or 'restored'. The reason for ping failure is never added.

In case of the **On Connection Restore** action, you can use the following additional placeholders:

%OUTAGE_DURATION%	the duration of the outage that has ended;
%OUTAGE_START_TIME%	the start time of the outage that has ended;
%OUTAGE_END_TIME%	the end time of the outage that has ended.

And for the actions handling connection quality changes, the following placeholder can be used:

%QUALITY%	the current connection quality, one of the following: Good, Warning, Bad or Critical.

Report Name Template Placeholders

Ping Monitor allows you to use placeholders when defining a name template for the file output of monitoring data reports. You can use the following placeholders when specifying the template:

%REPORT_NAME%	the name of the report being generated;
%REPORT_DATE%	the report generation date in the 'yyyy.MM.dd' format;
%REPORT_TIME%	the report generation time in the 'HH.mm.ss' format;
%FORMAT_EXTENTION%	the default file system extension of the report format.

Report Footer Placeholders

Ping Monitor allows you to use placeholders when defining a template for the report footer while configuring options on the **Reports Customization** preference page. You can use the following placeholders when specifying the footer template:

%LOCAL_HOST%	the name of the machine on which the product is running;
%RUNNING_PRODUCT%	the running product name;
%PRODUCT_VERSION%	the current version of the running product;
%TIME%	the report generation time in a long format;
%DATE%	the report generation date in a short format;
%DATETIME%	the report generation date with the report generation time;
%UTC_OFFSET%	the current UTC offset;
%REPORT_TIME_ZONE%	the time zone the report is generated for;
%YEAR%	the current year.

External Tools Placeholders

Ping Monitor allows you to use placeholders when defining a command to be launched as the external tool from the host's pop-up menu. You can use the following placeholders when specifying the command:

%REMOTE_HOST%	the remote host being monitored, including the host label, if defined;
%REMOTE_HOST_ADDRESS%	the address of the remote host being monitored;
%REMOTE_HOST_LABEL%	the label of the remote host being monitored;
%REMOTE_HOST_IP%	the resolved IP address of the remote host;
%REMOTE_HOST_GROUP%	the group the remote host belongs to;
%REMOTE_HOST_DESCRIPTION%	the description of the remote host being monitored;
%LOCAL_HOST%	the name of the machine on which the product is running;
%RUNNING_PRODUCT%	the running product name;

%PRODUCT_VERSION%	the current version of the running product;
%TIME%	the report generation time in a long format;
%DATE%	the report generation date in a short format;
%DATETIME%	the report generation date with the report generation time;
%YEAR%	the current year.

Chapter 9: Events Logging

Ping Monitor stores the events taken place during hosts monitoring and when executing generic operations. The monitoring events are stored per host and are available for reviewing in the Event table of the detailed host statistics. Those events, that are not directly connected to hosts monitoring, are displayed within the **Log** view.

Both the event viewers and the log are designed in a manner that helps you easily analyze the monitored host status changes and troubleshoot problems taking place while the program is in use. The events databases may grow continually, thus slowing down the program loading and response time. To prevent this, you can either clear the event logs manually, or allow the program to perform the clean-up automatically on a regular basis. The options for automatic events deletion are available on the **Monitoring Statistics** and **Log Configuration** preference pages.

In this chapter, we will explain how to analyze the events views and the log and describe the option of exporting events to a simple format.

Reviewing Monitoring Events

Ping Monitor allows you to review each and every event that has happened while monitoring connection to a remote host. The per-host events are available in the **Events** table displayed on the detailed host statistics `Pic 1`. Each entry has a severity icon, a title and a description. From the title, you can understand which event is logged; the description provides you with the detailed message; and the severity icon can be used to quickly understand if the event needs high level of attention.

Pic 1. Host monitoring events

The events in **Statistics** cover all aspects of host monitoring. They state when the monitoring was started and stopped, displaying brief session statistics on stop; they show when the host state or connection quality has changed, and display if there any problems with sending notifications and performing custom actions for the host being reviewed.

Exporting Monitoring Events

With Ping Monitor, you can easily export the monitoring events to the CSV file format for future analysis or processing by an automated tool. You can export events displayed in the Events table of **Statistics**. To export the events, click the **Export** button from the toolbar. You are proposed to choose between exporting the selected events and all displayed events. Also can you press the **Export** button from the **Organize** Ribbon group on the **Program** page, when the view is focused. It is also possible to use the pop-up menu of the view to export events. The **Export Events Wizard** will appear on the screen Pic 1.
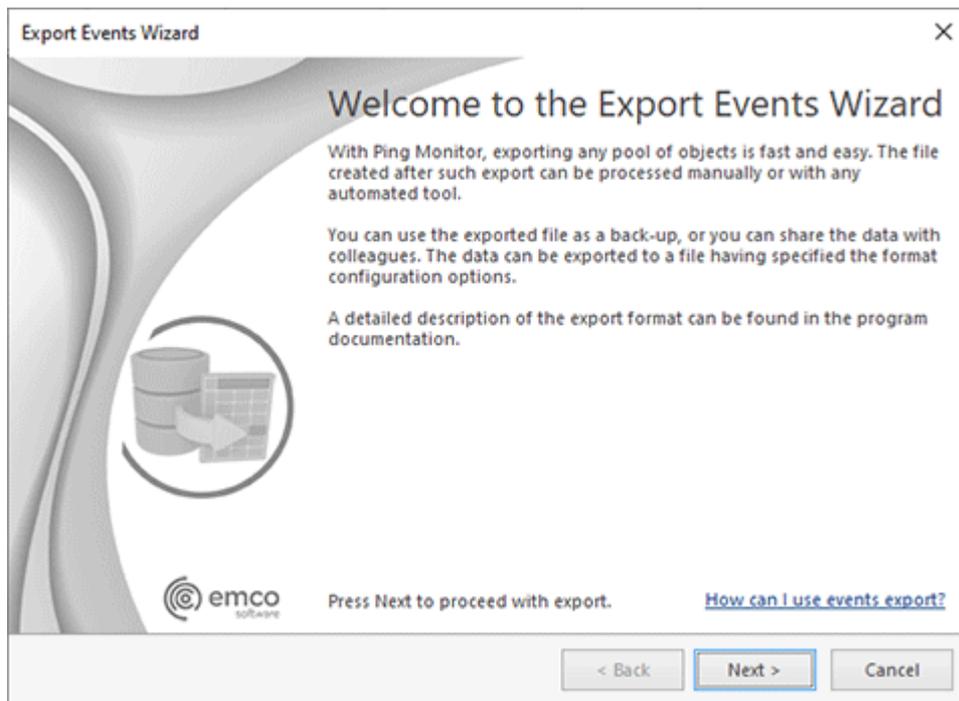
Pic 1. The Export Events Wizard welcome page

The first page of the **Export Events Wizard** is the welcome page used to introduce you to the feature the wizard is supposed to help you with. After reading the welcome information, press **Next** to continue with export.

On the next page of the **Export Events Wizard**, you are offered to choose a file you are going to save the events to and the CSV format options. The file path should be provided to the **Export To** field `Pic 2`. You can choose the encoding to be used for saving the data as well as the field delimiter and the text qualifier. While performing export, you may also define if you would like the column header to be present in the resulting file, which would make it easier for you to identify each column – this feature can be enabled using the **Include column header** option.
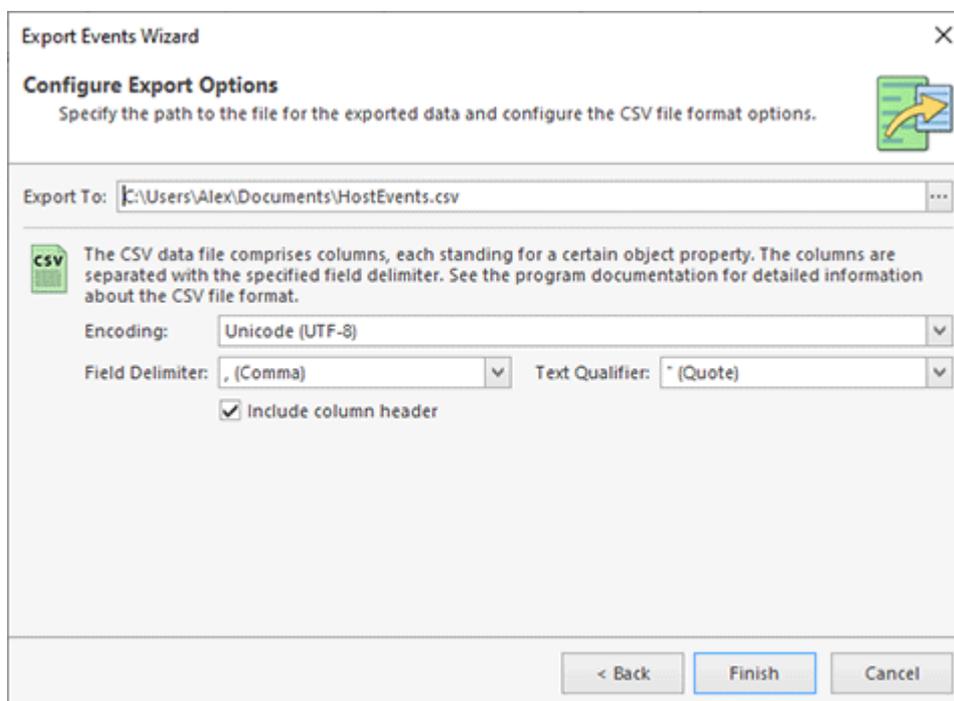
Pic 2. Configuring the export options

After you are ready with configuring the export options, press **Finish** to proceed with export. The file containing the events will be created in the path specified.

The CSV file with the connectivity events consists of four columns, which are the following:

Index	Header	Description
1	Type	The type of the generated connectivity event.
2	Host	The host the event is generated for.
3	Description	The logged event description.
4	Time	The time when the event was logged.

Sample exported data in the CSV format

"Type","Host","Description","Time"

"Up","h-00632.emcosoftware.com","The state of the 'h-00632.emcosoftware.com' host was changed to 'Up'. The connection was restored after being down for 00:00:19.","2019-08-05 02:12:19"

"Down","h-00632.emcosoftware.com","The state of the 'h-00632.emcosoftware.com' host was changed to 'Down'. The connection was lost. Ping reply was not received within the allotted time (IP status: 11010).","2019-08-05 02:12:00"

"Up","h-00261.emcosoftware.com","The state of the 'h-00261.emcosoftware.com' host was changed to 'Up'. The connection was restored after being down for 00:00:09.","2019-08-05 02:11:55"

"Down","h-00261.emcosoftware.com","The state of the 'h-00261.emcosoftware.com' host was changed to 'Down'. The connection was lost. Ping reply was not received within the allotted time (IP status: 11010).","2019-08-05 02:11:46"

"Down","h-00434.emcosoftware.com","The state of the 'h-00434.emcosoftware.com' host was changed to 'Down'. The connection was lost. Ping reply was not received within the allotted time (IP status: 11010).","2019-08-05 02:11:45"

"Up","h-00986.emcosoftware.com","The state of the 'h-00986.emcosoftware.com' host was changed to 'Up'. The connection was restored after being down for 00:00:18.","2019-08-05 02:11:38"

"Up","h-00632.emcosoftware.com","The state of the 'h-00632.emcosoftware.com' host was changed to 'Up'. The connection was restored after being down for 00:00:39.","2019-08-05 02:11:29"

"Down","h-00986.emcosoftware.com","The state of the 'h-00986.emcosoftware.com' host was changed to 'Down'. The connection was lost. Ping reply was not received within the allotted time (IP status: 11010).","2019-08-05 02:11:20"

"Up","h-00897.emcosoftware.com","The state of the 'h-00897.emcosoftware.com' host was changed to 'Up'. The connection was restored after being down for 00:00:09.","2019-08-05 02:11:14"

"Down","h-00897.emcosoftware.com","The state of the 'h-00897.emcosoftware.com' host was changed to 'Down'. The connection was lost. Ping reply was not received within the allotted time (IP status: 11010).","2019-08-05 02:11:05"

"Down","h-00632.emcosoftware.com","The state of the 'h-00632.emcosoftware.com' host was changed to 'Down'. The connection was lost. Ping reply was not received within the allotted time (IP status: 11010).","2019-08-05 02:10:50"

"Up","h-00484.emcosoftware.com","The state of the 'h-00484.emcosoftware.com' host was changed to 'Up'. The connection was restored after being down for 00:00:09.","2019-08-05 02:10:36"

The CSV file with the host monitoring events consists of five columns, which are the following:

Index	Header	Description
1	Title	The logged event title.
2	Severity	The logged event severity level.
3	Description	The logged event description.
4	Time	The time when the event was logged.
5	Error Code	The error code for the event, if any.

Sample exported data in the CSV format

"Title","Severity","Description","Time","Error Code"

"Connection Quality","Information","The connection quality for the 'h-00020.emcosoftware.com' host was changed to 'Warning'.","2019-08-05 01:43:50",

"Host State","Information","The state of the 'h-00020.emcosoftware.com' host was changed to 'Up'. The connection was restored after being down for 00:00:09.","2019-08-05 01:41:40",

"Host State","Warning","The state of the 'h-00020.emcosoftware.com' host was changed to 'Down'. The connection was lost. Ping reply was not received within the allotted time (IP status: 11010).","2019-08-05 01:41:31",

"Connection Quality","Information","The connection quality for the 'h-00020.emcosoftware.com' host was changed to 'Bad'.","2019-08-05 01:41:21",

"Connection Quality","Information","The connection quality for the 'h-00020.emcosoftware.com' host was changed to 'Warning'.","2019-08-05 01:38:40",

"Host State","Information","The state of the 'h-00020.emcosoftware.com' host was changed to 'Up'. The connection was restored after being down for 00:00:09.","2019-08-05 01:37:00",

"Host State","Warning","The state of the 'h-00020.emcosoftware.com' host was changed to 'Down'. The connection was lost. Ping reply was not received within the allotted time (IP status: 11010).","2019-08-05 01:36:51",

"Connection Quality","Information","The connection quality for the 'h-00020.emcosoftware.com' host was changed to 'Bad'.","2019-08-05 01:36:46",

"Connection Quality","Information","The connection quality for the 'h-00020.emcosoftware.com' host was changed to 'Warning'.","2019-08-05 01:31:04",

"Host State","Information","The state of the 'h-00020.emcosoftware.com' host was changed to 'Up'. The connection was restored after being down for 00:00:59.","2019-08-05 01:28:29",

Analyzing Log

The main purpose of the **Log** view is to help you understand if the execution has succeeded and troubleshoot problems if any have occurred. Each entry in the log has a severity icon, a title, and a description, and possibly a hint on solving the problem, if any. From the title, you can understand which operation has been performed and which resource has been operated; the description provides you with the result message, a hint is used to provide you with an advice on solving the problem, if any; and the severity icon can be used to quickly understand if the operation has fully succeeded.

For example, let us take a closer look at the following result set in the log **Pic 1**.
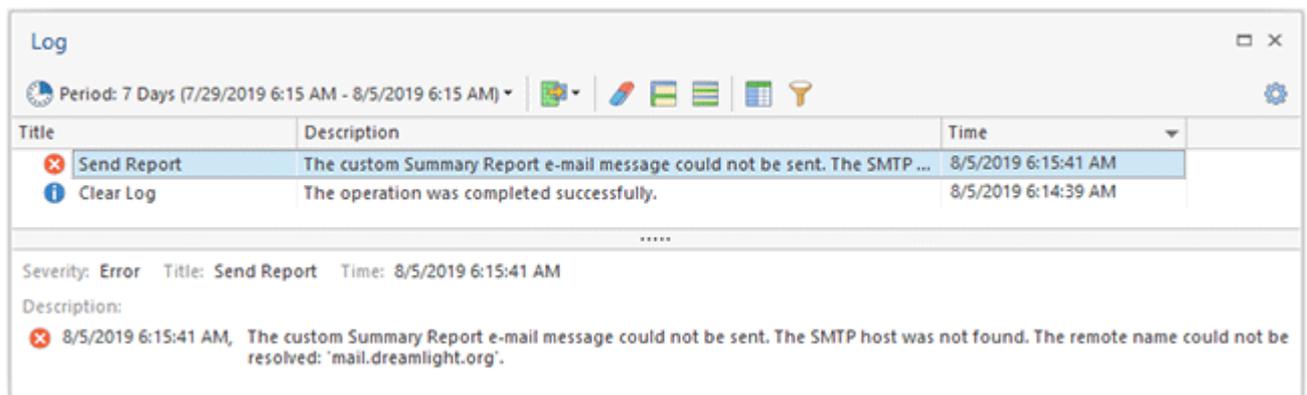
Pic 1. Sample logged events

The picture above shows the set of result we received after performing an operation. As we can see, most of the logged events are informational, but some stand for problems. We need to find out what caused the problem and what should be done to avoid it in future. Also, it may be interesting to go through the warnings to see if anything wrong is going on.

After the events have been reviewed and all the problems have been solved, you can run the operation again and ensure that it completes successfully.

Exporting Log

With Ping Monitor, you can easily export the log to the CSV file format for future analysis or processing by an automated tool. To export the logged events, click the **Export** button from the **Log** view toolbar. You are proposed to choose between exporting the selected events and all events. You can also press the **Export** button from the **Organize** Ribbon group on the **Program** page when the Log view is in focus. It is also possible to use the pop-up menu of the Log view to export logged events. The **Export Log Wizard** will appear on the screen **Pic 1**.

Pic 1. The Export Log Wizard welcome page

The first page of the **Export Log Wizard** is the welcome page used to introduce you to the feature the wizard is supposed to help you with. After reading the welcome information press **Next** to continue with export.

On the next page of the **Export Log Wizard**, you are offered to choose a file you are going to save the logged events to and the CSV format options. The file path should be provided to the **Export To** field Pic 2. You can choose the encoding to be used for saving the data as well as, the field delimiter and the text qualifier. While performing exporting, you may also define if you would like the column header to be present in the resulting file, which would make it easier for you to identify each column – this feature option can be enabled using the **Include column header** option.
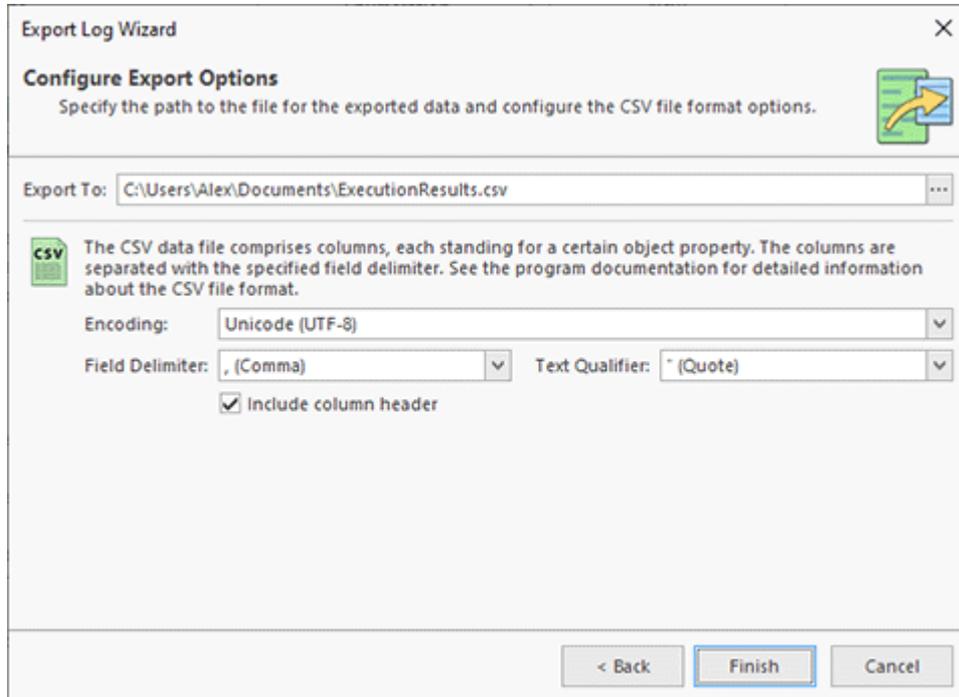
Pic 2. Configuring the export options

After you are ready with configuring the export options, press **Finish** to proceed with export. The file containing the logged events will be created in the path specified.

The CSV file with the exported data consists of six columns, which are the following:

Index	Header	Description
1	Path	The path to the logged event in the log tree.
2	Title	The logged event title.
3	Severity	The logged event severity level.
4	Description	The logged event description.
5	Time	The time when the event occurred.
6	Error Code	The error code for the event, if any.

Sample exported logged events in the CSV format

"Path","Title","Severity","Description","Time","Error Code"

"Clear Application Log","Clear Application Log","Information","The operation was completed successfully.","2015-09-14 13:47:40",

"Save Report","Save Report","Error","The 'News Providers' report could not be saved to the 'F:
\Reports\' folder with the 'News Providers (2015.09.14).pdf' name. The system cannot find the path
specified. Error code: 3.","2015-09-14 13:47:46",

Now you are introduced to the log export and export data file format and can use the export feature
for the log analysis without any misunderstanding.

Chapter 10: Program Preferences

Ping Monitor comes with a wide range of settings that users can adjust to suit their needs. Every preference page has a detailed description of its content and of the feature it is used to configure. You can configure almost everything: the program behavior in respect to the System Tray, the database location, the proxy settings to be used to connect to the Internet, etc. To reach the program preferences, click the **Preferences** button available from the **Application Menu**. Also, the clickable **Ribbon** groups' glyphs open the preference pages that configure the functionality encapsulated by this group.

Monitoring Part

The **Monitoring** part of the program preferences should be used to configure the monitoring process settings. It is possible to configure the connection monitor behavior, gateway options, monitoring intervals and automation settings. To open the **Preferences** dialog, click the **Preferences** button available from the **Application Menu**. Configure the available settings to suit your needs best.

Monitor Settings

Ping Monitor monitors the remote host availability using the specified monitor settings. These settings can be specified on the **Monitor Settings** preference page Pic 1 . You can activate this page by clicking the glyph of the **Activity** Ribbon group on the **Home** Ribbon page, or clicking the **Preferences** button from the **Application Menu** and selecting the **Monitor Settings** link on the navigation bar on the left in the opened dialog.
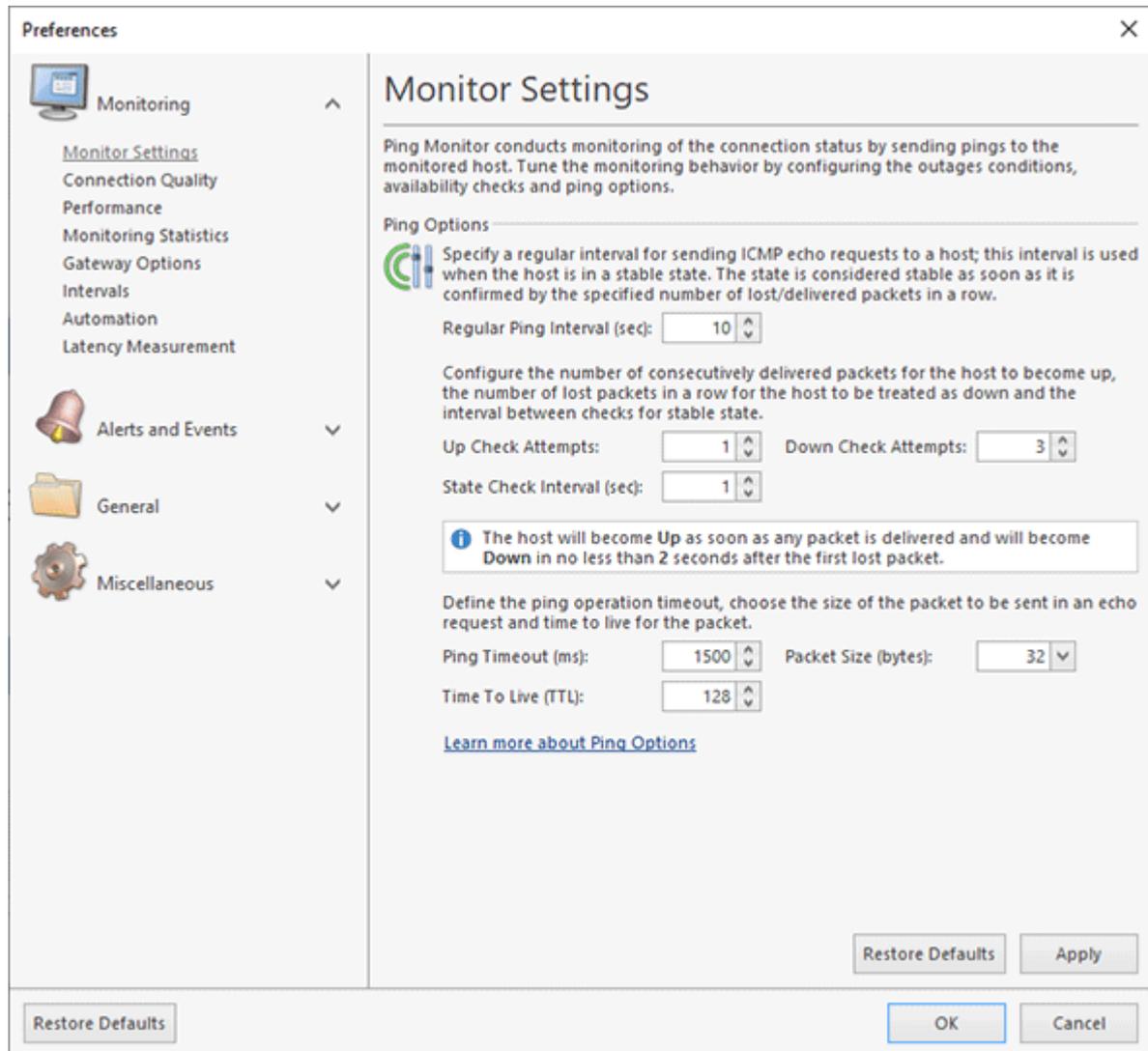
Pic 1. Configuring the Monitor Settings

The following ping options can be configured:

- **Regular Pings Interval** is the time span in seconds between pings if the host is currently in a stable state. The state is considered stable as soon as it is confirmed by the specified number of lost/delivered packets in a row;

- **Up Check Attempts** is the number of delivered packets in a row that could be interpreted as an established connection to a remote host;

- **Down Check Attempts** is the number of lost packets in a row that could be interpreted as a lost connection to a remote host;

- **State Check Interval** is the time span in seconds between pings if host sate is currently unstable, i.e. not confirmed as up or down;

- **Ping Timeout** is the time span in milliseconds for the ping command to wait for a response from a remote host;

- **Packet Size** is the size in bytes of the packet sent with an ICMP echo request;

- **Time To Live (TTL)** is the time-to-live for the packet being sent. It is reduced by every host on the route to the destination. If the TTL field reaches zero before the packet arrives, such packet is discarded and an error is sent back. The purpose of the TTL field is to avoid a situation in which an undeliverable packet would keep circulating in the Internet.

With EMCO Ping Monitor, it is possible not only to set a common monitoring configuration, but also to provide a specific configuration for each host individually. See the Overriding Common Settings part of this document for details.

Connection Quality

Along with host state monitoring, Ping Monitor allows you to monitor the quality of connection to remote hosts, based on the set of the latest ping replies. The parameters used for connection quality calculation can be specified on the **Connection Quality** preference page `Pic 1`. To reach this page, click the **Preferences** button from the **Application Menu** and selecting the **Connection Quality** link on the navigation bar on the left in the opened dialog.
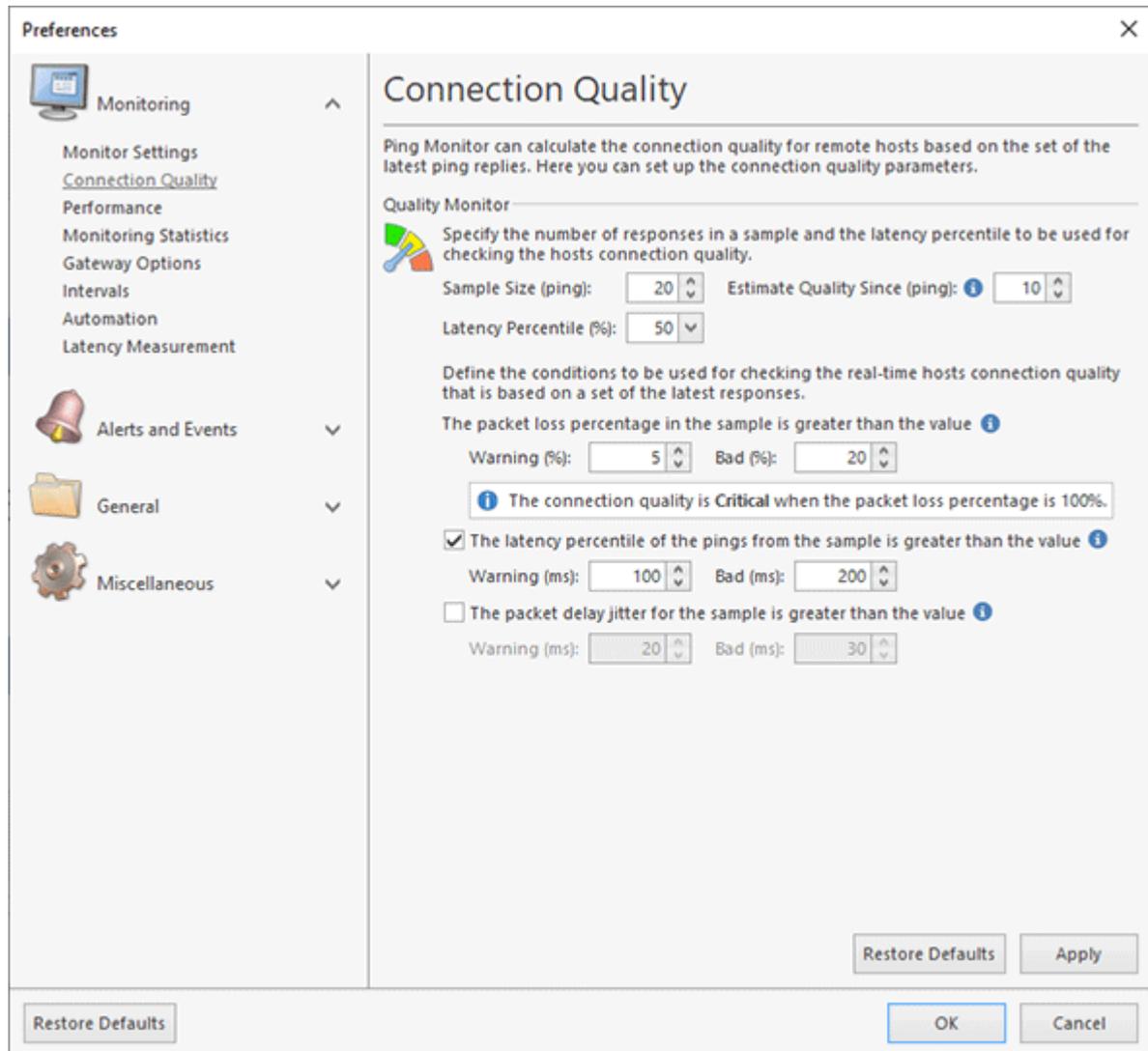
Pic 1. Specifying connection quality monitoring configuration

When calculating a connection quality, Ping Monitor can use such characteristics as the percentage of lost packets, the latency percentile and the latency jitter. The **Sample Size** field is used to specify the number of most latest pings to be used for quality calculation. Ping Monitor can estimate the connection quality when the sample is incomplete, i.e. the number of responses in the sample is below its size. The **Estimate Quality Since** field is used to specify the minimum number of responses sufficient to estimate the connection quality, while it will be considered **Pending** with a lower number of responses.

A connection quality is considered **Critical** in case all packets from the sample are lost. For the **Bad** and **Warning** quality, you can specify the conditional values to check for packet loss percentage, latency and jitter. In case no condition is reached, the connection quality is treated as **Good**.

The packet loss percentage is a ratio of the number of lost packets from the sample to the number of packets sent within the same sample. The latency percentile separates the greater and lesser parts of a round-trip times data set. The percentile specified in the **Latency Percentile** field is used. The sample for calculation is built from a specified number of the latest delivered packets. The jitter is calculated as a packet delay variation for a sample of delivered packets of a specified length with reference to the specifications defined in RFC-1889. If you prefer not to use latency percentile or jitter in quality calculation, you can uncheck the appropriate options.

With EMCO Ping Monitor, it is possible not only to set a common connection quality monitor configuration, but also to provide a specific one for each host individually. See the Overriding Common Settings part of this document for details.

Performance

Ping Monitor calculates remote hosts' performance based on their monitoring statistics for specific time periods. The conditions used for calculating the performance are defined on the **Performance** preferences page Pic 1 . You can reach this page by clicking the **Preferences** button from the **Application Menu** and selecting the **Performance** link on the navigation bar on the left in the opened dialog.
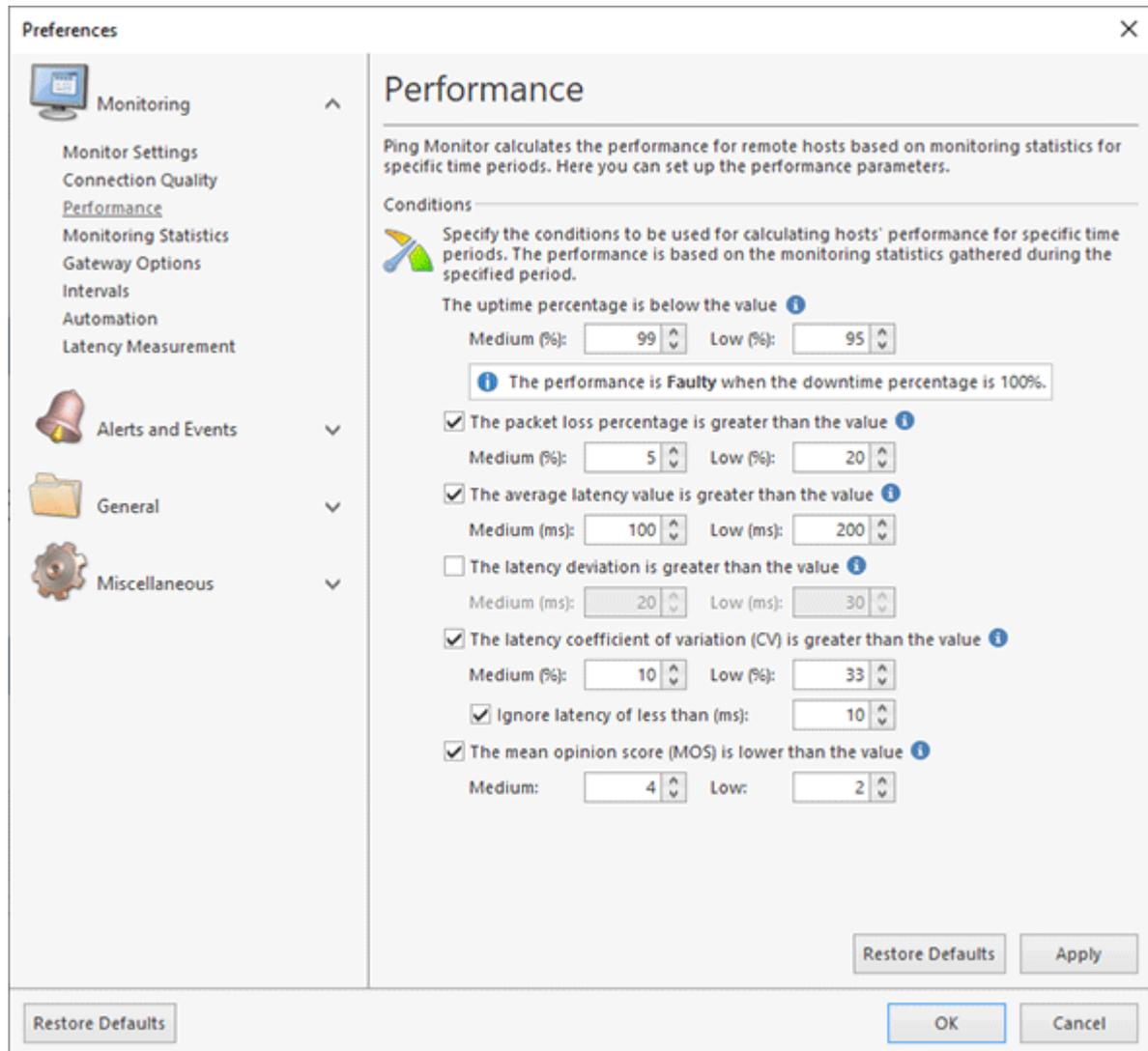
Pic 1. Specifying performance calculation settings

You can choose from the following characteristics to be used for calculating the performance:

- **Uptime** - a percentage ratio of the host uptime to the whole non-pending period of the host;

- **Packet Loss** - a percentage ratio of the number of lost packets to the number of packets being sent during the specified time period;

- **Average Latency** - an arithmetic mean of all round-trip times of packets successfully delivered during the specified time period;

- **Latency Deviation** - a standard deviation from the average latency value for all round-trip times of packets successfully delivered during the specified time period;

- **Latency Coefficient of Variation** - a percentage ratio of the latency deviation to the average latency calculated for all round-trip times of packets successfully delivered during the specified time period;

- **Mean Opinion Score** - a well-established metric for obtaining the quality of VoIP based on the latency characteristics and packet loss percentage for all packets sent during the specified time period.

In case any of the **Low** conditions is met, the performance is considered **Low**. Next the **Medium** conditions are checked, and if any is met, the performance is **Medium**. If no conditions are met, the performance is treated as **High**. It is possible to disable the performance calculation by unchecking all characteristics.

As for the coefficient of variation (CV), it becomes too sensitive when the average latency is small. It is possible to define the minimum average latency for CV calculation within the **Ignore latency of less than** field.

Monitoring Statistics

Ping Monitor gathered and stores per host performance and availability data, which is called monitoring statistics, while monitoring remote hosts connectivity. This data consists of the live data, historical data and overall data. The intervals for storing and displaying live data as well as the historical data storing options are available on the **Monitoring Statistics** preference page `Pic 1`. To reach this page, you should open the program preferences using the **Preferences** button from the **Application Menu**, and click the **Monitoring Statistics** link in the navigation bar on the left of the **Preferences** dialog within the **Events and Statistics** group.
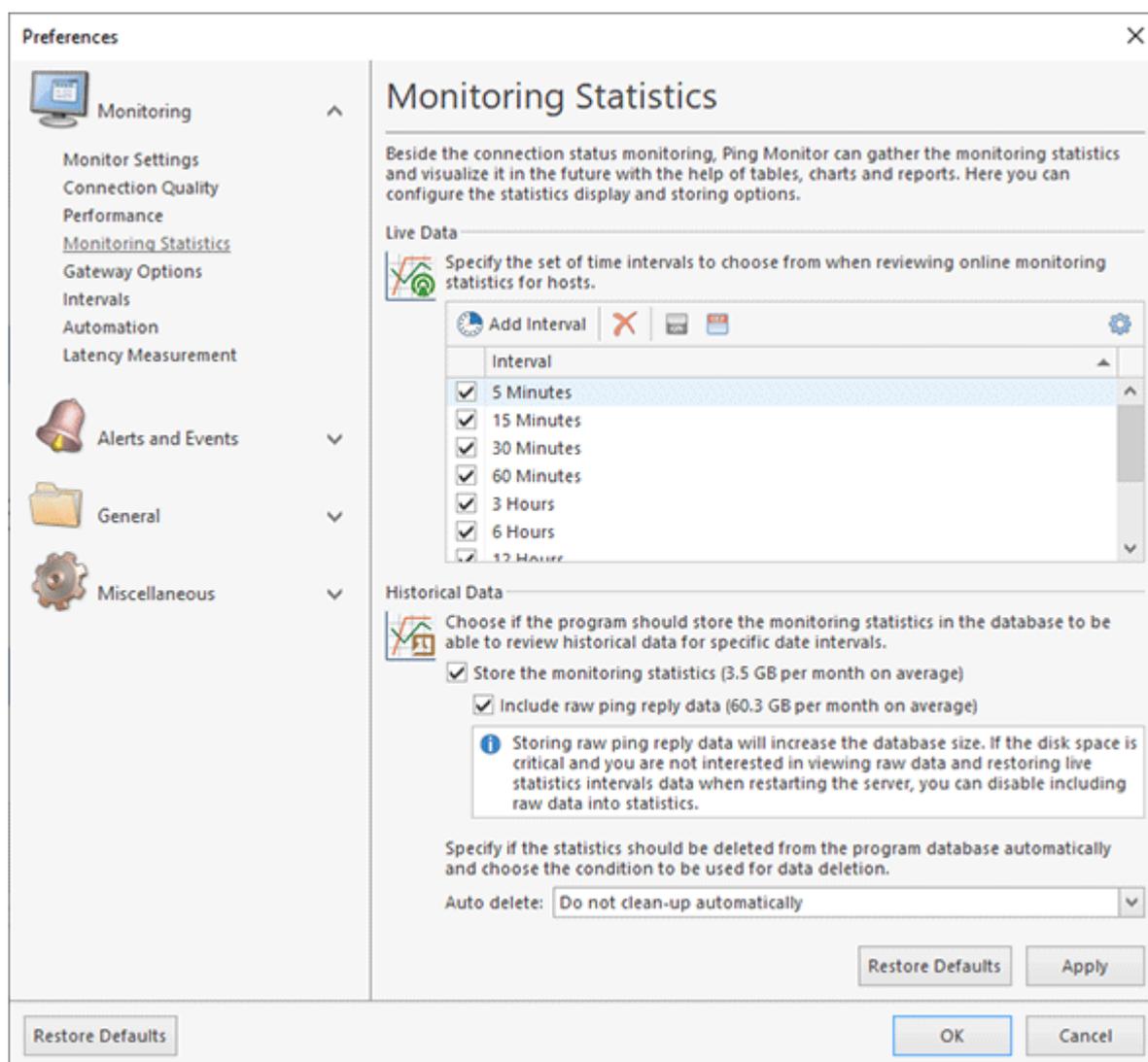
Pic 1. Configuring live and historical monitoring data options

Within the **Live Data** group, you can choose the time intervals to be used for storing and displaying the statistics. It is possible to create and delete intervals, as well as enable or disable existing ones. It is possible to define an interval from 5 minutes to 3 days. Specifying large focus intervals will lead to a higher consumption of the system memory and the processor resources while preparing statistics for each host.

The **Historical Data** group contains the options for historical data storing and automatic deletion. If you do not want to store the historical data at all, you can disable the **Store the historical data** option. Please take into account that as long as this option is disabled it is not possible to review historical data and generate statistical reports for future monitoring sessions. In case you are not interested in raw ping replies data, you can disable its storing by unchecking the **Include raw ping**

reply data box. When this option is disabled, it won't be possible to export raw data, view pings timeline and restore live statistics when restarting the server.

The options for historical data auto remove, allow you to prevent the monitoring data database from continuous growing. You can enable the automatic removal of the historical data that is older than a specific age within the **Auto delete** drop-down list.

Gateway Options

Ping Monitor can check that either a packet sent to remote host has been lost or the PC hosting the monitoring software has lost connection to the network the host is located in by pinging a specific gateway. This feature is provided to protect the user from a false-positive detection of outages and connection quality problems. In case the gateway is unreachable, the host state and quality is not changed until it is confirmed by a successful ping to the gateway.

The gateway configuration is set up on the **Gateway Options** preference page `Pic 1`. To access the **Gateway Options** preference page, press the **Preferences** button from the **Application Menu** and select the **Gateway Options** link in the navigation bar on the left in the dialog that opens.
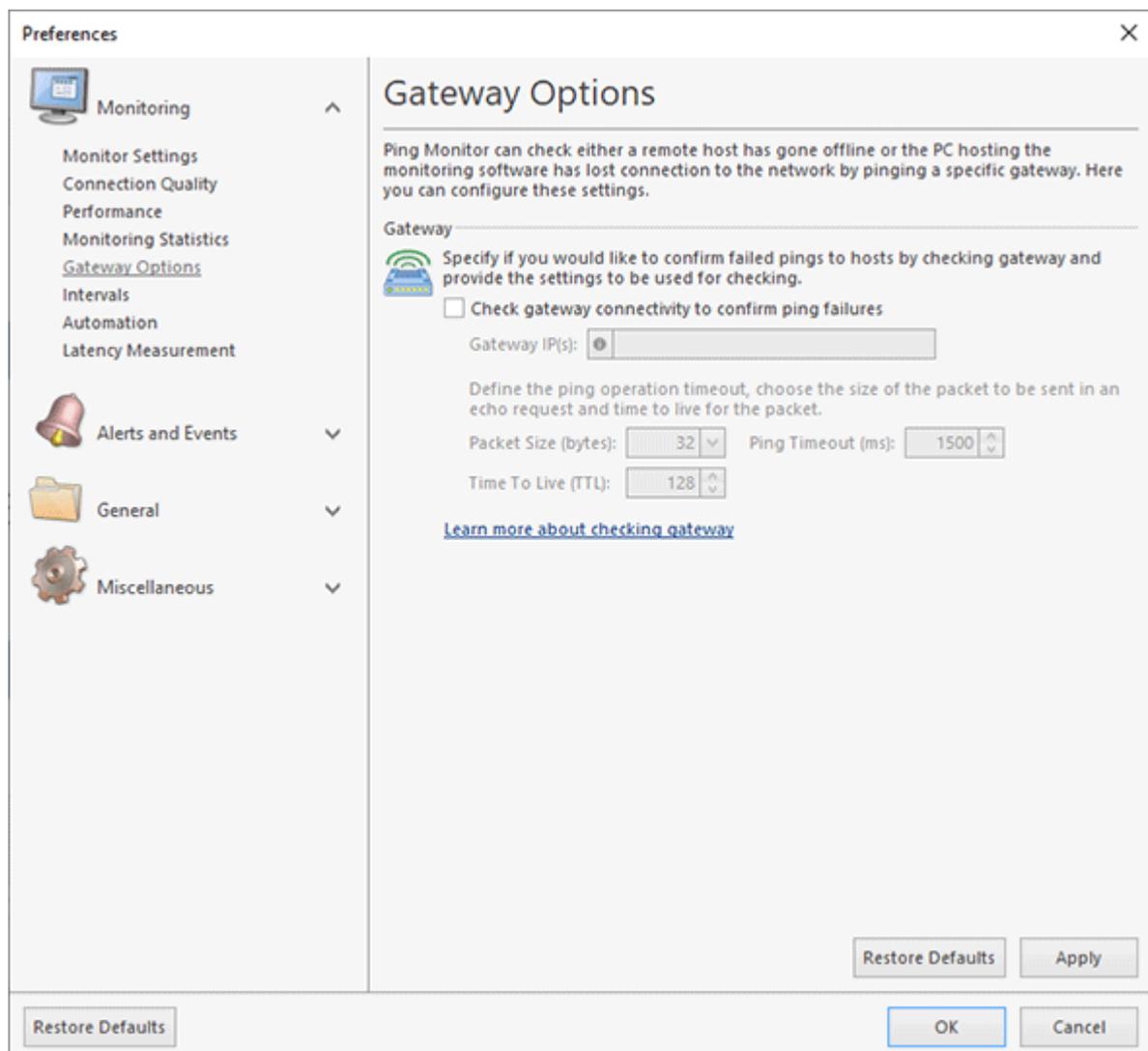
Pic 1. Setting up the gateway options

If you want to enable the failed pings confirmation by checking a specific gateway for accessibility, you should check the **Check gateway connectivity to confirm ping failures** option and provide

the address of the gateway to ping to the **Gateway IP** field. The size of the packet to send to the gateway, the ping operation timeout and the time-to-live for the ping packet can be specified in the appropriate fields, if required. As soon as this check is enabled, a ping to a remote host will be treated as failed only if the gateway is reachable.

With EMCO Ping Monitor, it is possible not only to set a common gateway options, but also to provide a specific one for each host individually. See the Overriding Common Settings part of this document for details.

Intervals

Ping Monitor allows you to restrict the monitoring time to specific time intervals on certain week days, thus you can configure the monitoring to pause automatically when it is not required. This configuration is available on the **Intervals** preference page Pic 1 . You can activate this page by clicking the **Preferences** button from the **Application Menu** and selecting the Intervals link on the navigation bar on the left in the opened dialog.
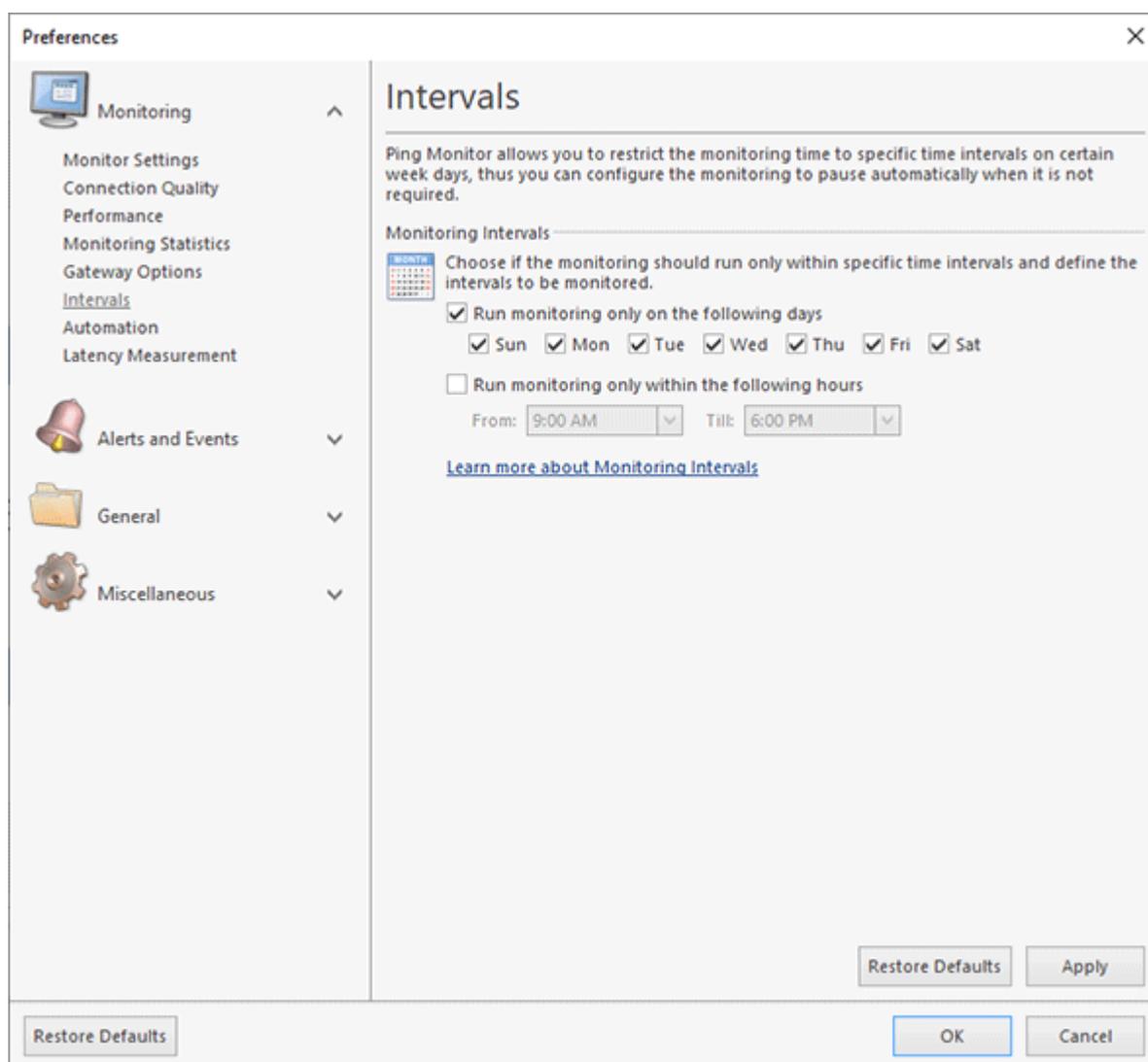
Pic 1. Configuring monitoring intervals

You can choose if you would like the hosts to be monitored only on specific week days and/or within specific hours. After you start the monitoring process, it is managed by the program automatically: if the current time is not within the monitoring intervals, monitoring is automatically paused until the monitoring interval is reached again.

Automation

Ping Monitor comes with a range of automation features that allow you to start, stop and pause monitoring automatically. The configuration of such features is available on the **Automation** preferences page `Pic 1`. You can activate this page by clicking the **Preferences** button from the **Application Menu** and selecting the **Automation** link in the navigation bar on the left in the opened dialog.
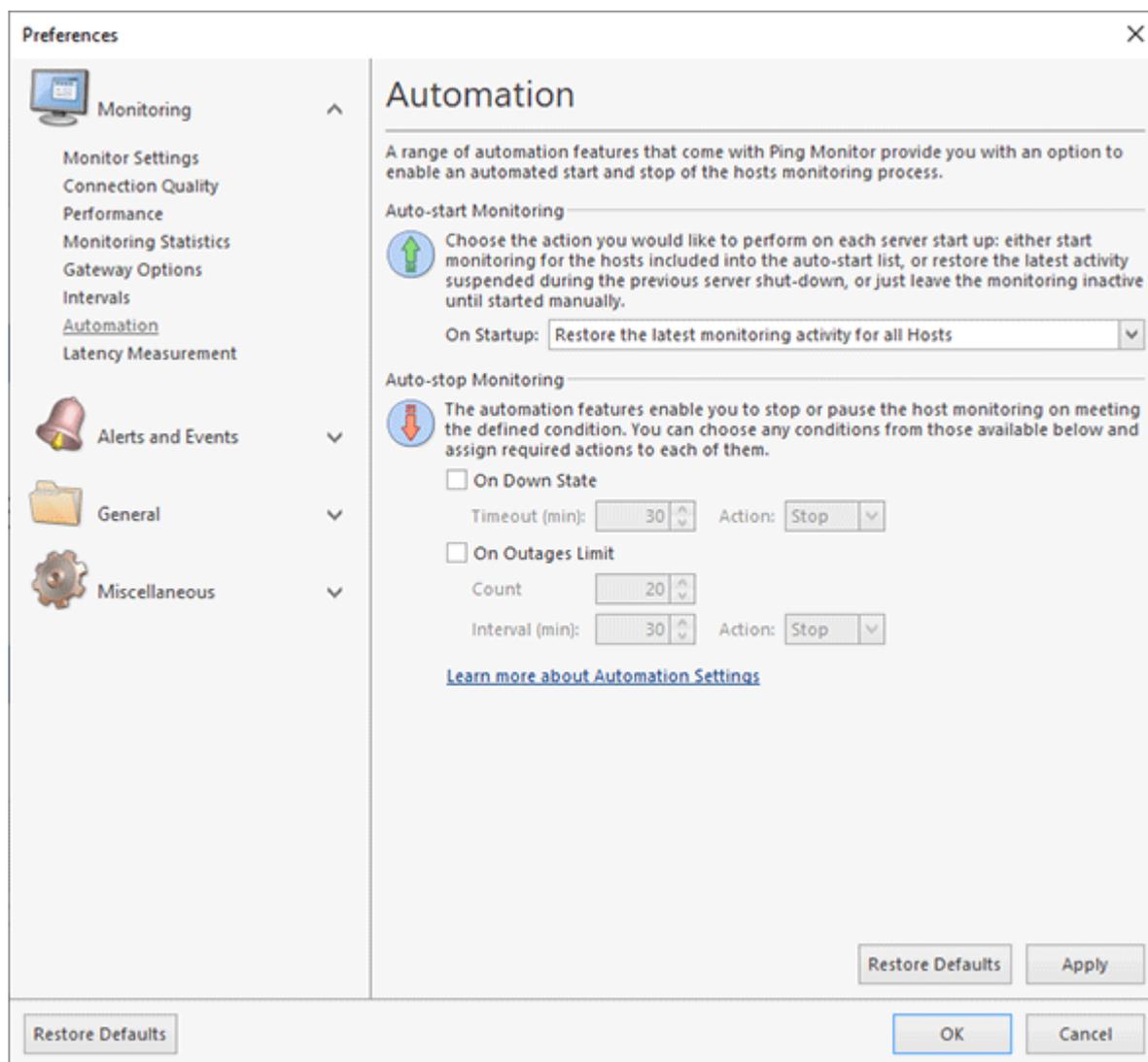
Pic 1. Configuring the automation features

Within the **Auto-Start Monitoring** group, you can choose the action you would like to perform on each server start up: either start monitoring for the hosts included into the auto-start list, or restore the latest monitoring activity suspended during the previous server shut-down, or just leave the monitoring inactive until started manually.

The **Auto-stop Monitoring** group is designed for you to define the conditions to be used to stop or pause monitoring of a single host. There are two conditions available, namely: **On Down State** and **On Outages Limit**. For each condition, you can choose the action to perform in case of this condition between **Stop** and **Pause**. For the **Pause** action, you should define the pause timeout. Let us take a closer look on each condition.

The **On Down State** condition should be enabled if you would like the host monitoring process to stop/pause automatically if the connection to the host is lost and not reestablished during the interval specified in the **Timeout** field next to the **On Down State** option.

The **On Outages Limit** condition provides you with an option to stop/pause the host monitoring process automatically if a defined number of outages have been registered during the specified time interval. The number of outages is defined in the **Count** field, and the time interval to be applied should be provided in the **Interval** field.

With EMCO Ping Monitor, it is possible not only to set a common **Auto-stop Monitoring** configuration, but also to provide a specific configuration for each host individually. See the Overriding Common Settings part of this document for details.

Latency Measurement

Ping Monitor can monitor hosts in low-latency networks if the high-precision latency measurement is enabled. In this case, the program uses a special ICMP network filter driver to measure the ping latency with 0.01ms precision. On the **Latency Measurement** page, you can switch the program to use the Windows standard measurement with 1ms precision or high-precision measurement Pic 1.
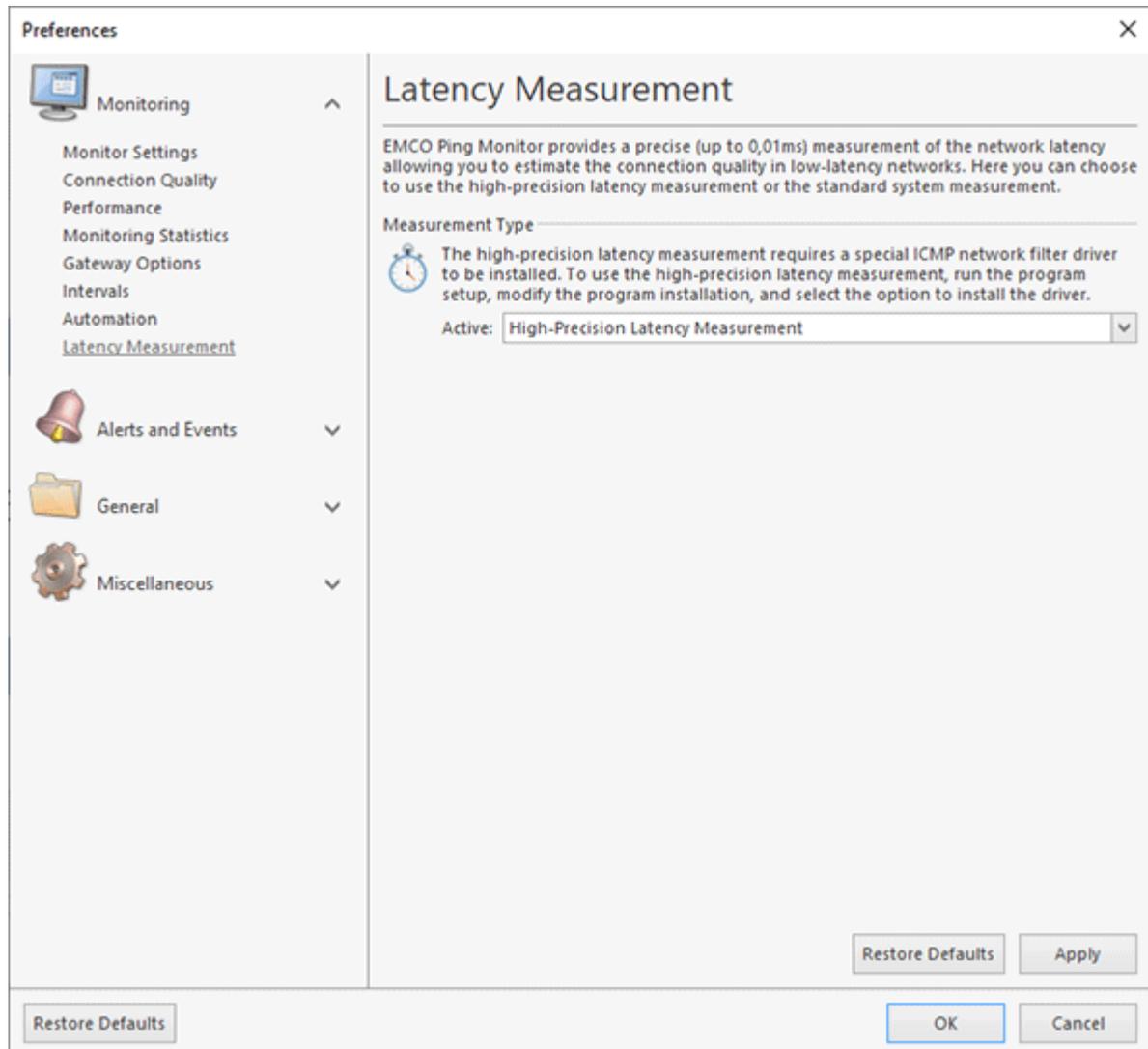
Pic 1. Configuring latency measurement precision

To use the high-precision latency, you need to install a special ICMP network filter driver on the machine where the Ping Monitor server is installed. Run the program setup to modify the server installation and select the option to install the driver. The server should be rebooted after the driver is installed.

Alerts and Events Part

The Alerts and Events part of the program preferences should be used to configure the alerts, notifications and custom actions to be performed upon discovery of certain events during monitoring, statistics and events storing, etc. To open the **Preferences** dialog, click the **Preferences** button available in the **Application Menu**. Configure the available settings to suit your needs best.

Alerts and Notifications

The **Alerts and Notifications** preference page allows you to configure alerts in the program. You can learn more about alerts in the **Using Alerts** chapter of this manual. On the **Alerts and Notifications** preference page you can create alerts, configure alerts conditions and configure email notifications and custom messages that should be executed on alerts and events.

In the **Notifications Configuration** section of the dialog you can create, review and edit alerts and events configured in the program. You can also review and edit e-mail messages and custom actions assigned to alerts and events. To manage alerts, events and their notifications you can use actions available on the toolbar **Pic 1**.
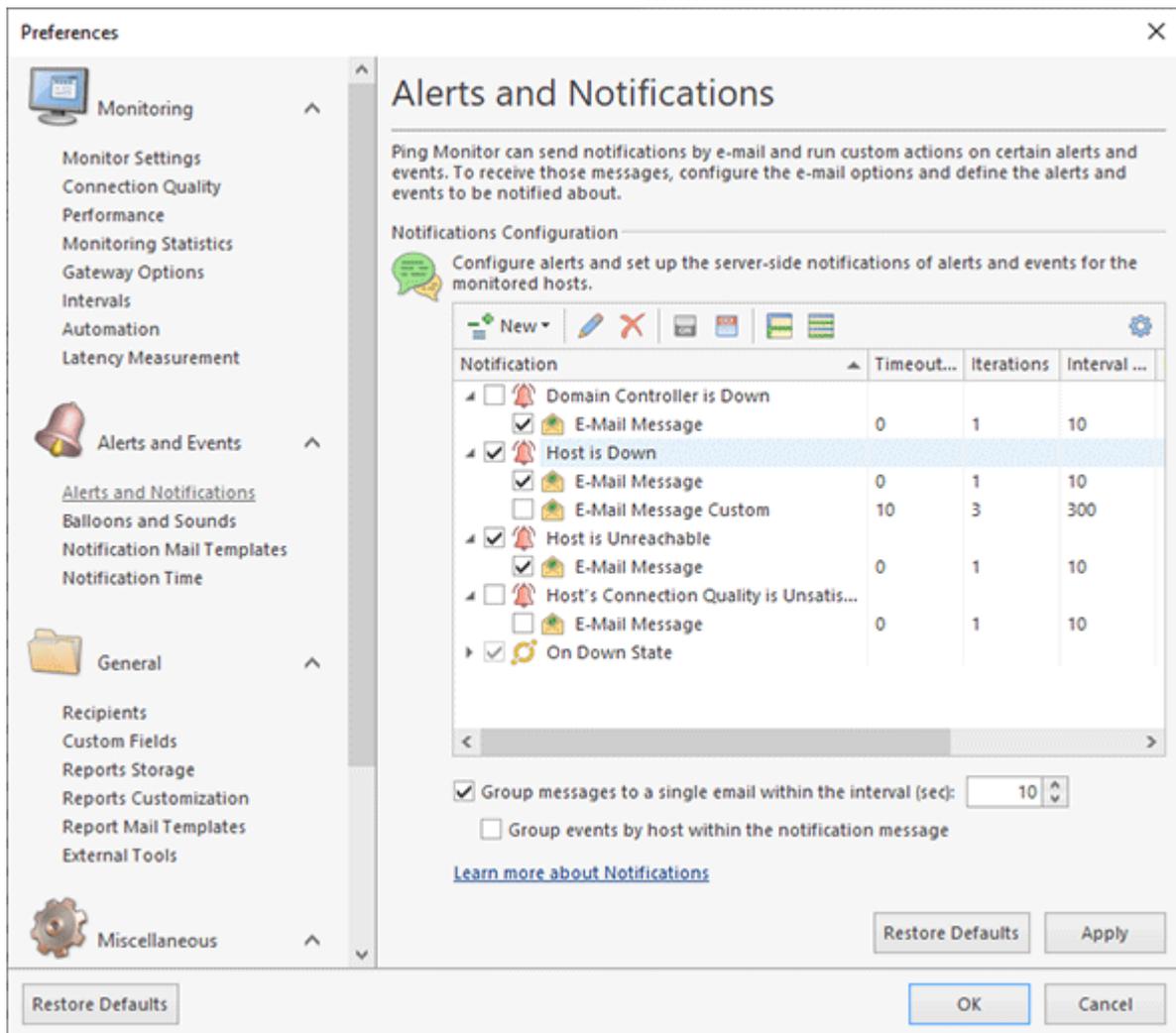
Pic 1. Configuring alerts, events and notifications

You can use checkboxes to enable or disable alerts, events and notifications. When configuring e-mail notifications or custom actions it is possible to specify the number of iterations and interval between iterations for notifications. So you can choose to loop the notification for a specific number of times or until the host state or connection quality changes again.

To create alerts and events use the corresponding items displayed in the **New** menu item. When creating an alert you need to specify an alert condition. Once this condition is reached the alert is activated. You can use logical operators to combine conditions as you need. As condition parameters you can use any real-time value, including host state, quality, packet loss, latency, jitter and other values Pic 2.
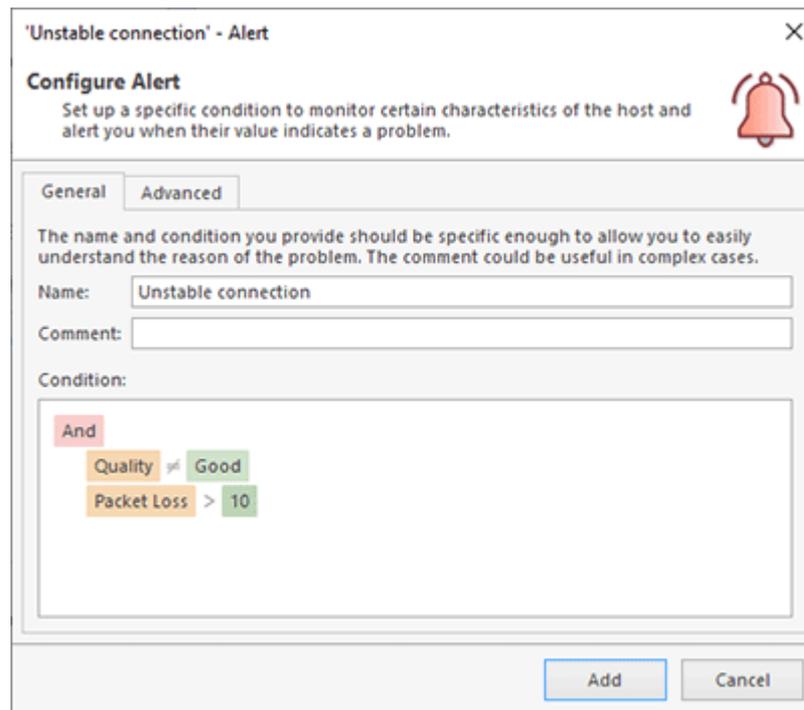
Pic 2. Configuring alert condition

For each alert you can specify its severity, so when multiple alerts are reported you can sort and filter them by severity. It is also possible create already acknowledged alert for a specified period of time and assign a notification for the alert **Pic 3**.
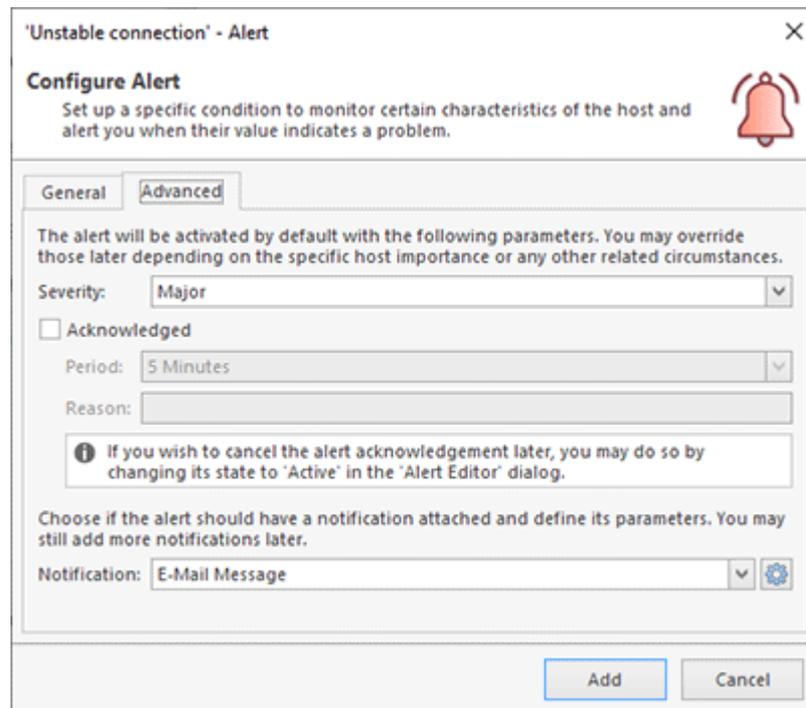
Pic 3. Configuring alert options

You can assign one or multiple e-mail notifications for an alert. To assign you need to select the alert in the list and choose **New** and **E-Mail Message** in the context menu. In the appeared dialog you can specify custom e-mail recipients, if required, otherwise the program will use a list of recipients specified on the **Recipients** page of preferences. On the **Advanced** tab of the dialog you can override the global notification configuration that is specified on the **Notification Time** page of the program preferences.

With EMCO Ping Monitor, it is possible not only to set a common **Notifications** configuration, but also to provide a specific configuration for each host individually. See the **Overriding Common Settings** part of this document for details.

Balloons and Sounds

The program allows you to play sound notifications and show Windows Tray balloons on alerts and events. On the **Balloons and Sounds** page of preferences you can configure notification settings. Note that sounds and balloons notifications are client-specific, so each client may have its own settings and the settings of one client aren't applied to other clients.

You can enable balloons and sounds notifications for alerts and events configured on the **Alerts and Notifications** page in preferences. Alerts and events configured there are displayed in the list, so you can use checkboxes to enable balloons and sounds assigned to them **Pic 1**.
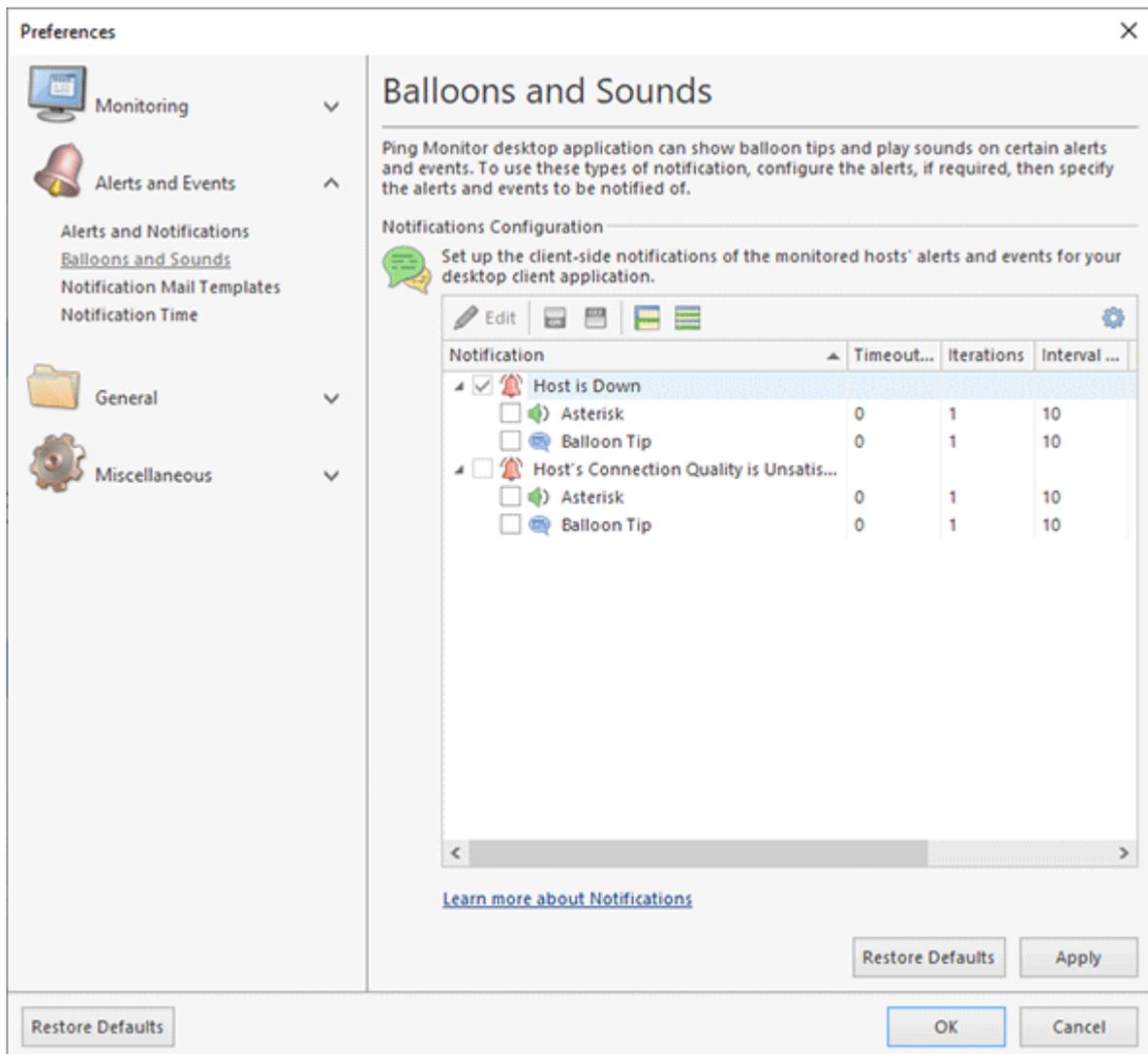
Pic 1. Balloons and Sounds notifications

Sound notifications can be edited to configure sounds that should be played on occurred and on resolved cases. On the **Advanced** tab of the displayed dialog you can specify custom notification settings, including timeout, number of iterations and interval between the iterations as well as date and time range when notifications can be activated `Pic 2`.

Pic 2. Sound notification settings

You can specify custom notification settings by overriding global settings configured on the **Notification Time** page of preferences.

Notification Mail Templates

Mail Templates are used to form e-mail messages sent by Ping Monitor. They can be configured on the **Mail Templates** preference page Pic 1. To access this page, click the **Preferences** button from the **Application Menu** and select the appropriate link in the navigation bar on the left of the **Preferences** dialog within the Alerts and Events group.
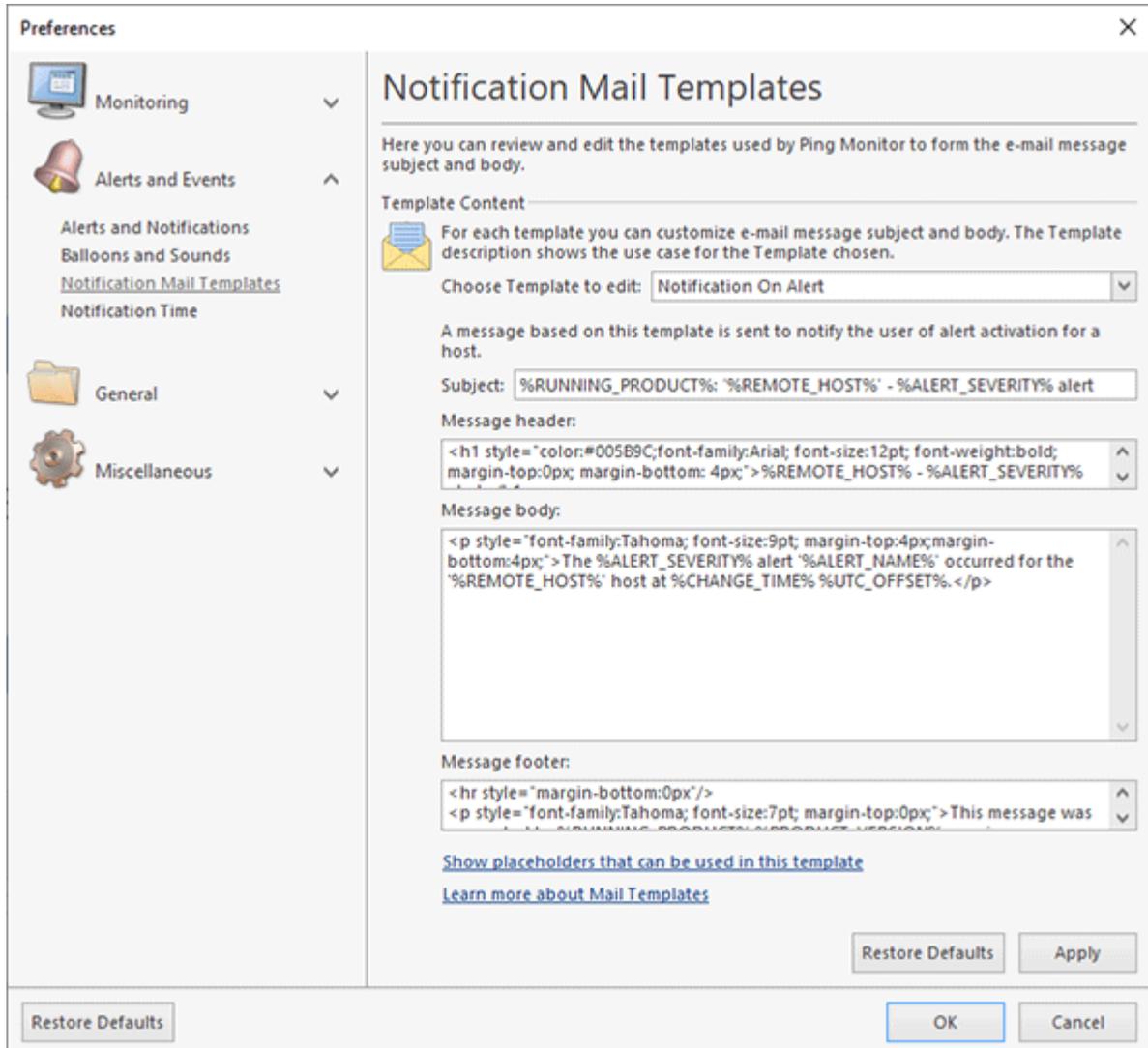
Pic 1. Configuring Mail Templates

On this page, you are offered to choose a template that you want to review and edit. The template description shows you the use case of the chosen template, and if there are placeholders available for this template, a link to a detailed placeholders description is shown under the template description. For a selected template you can see a text that should be used in e-mail subject, body, header and footer. You can edit it if required.

Notification Time

In the Notification Time page of preferences you can configure notification options and acceptable times and hours for notifications **Pic 1**. These settings are applied by default for custom actions, e-mail notifications, sound notifications and balloons. You can override these default settings and set custom settings in each notification, if required.
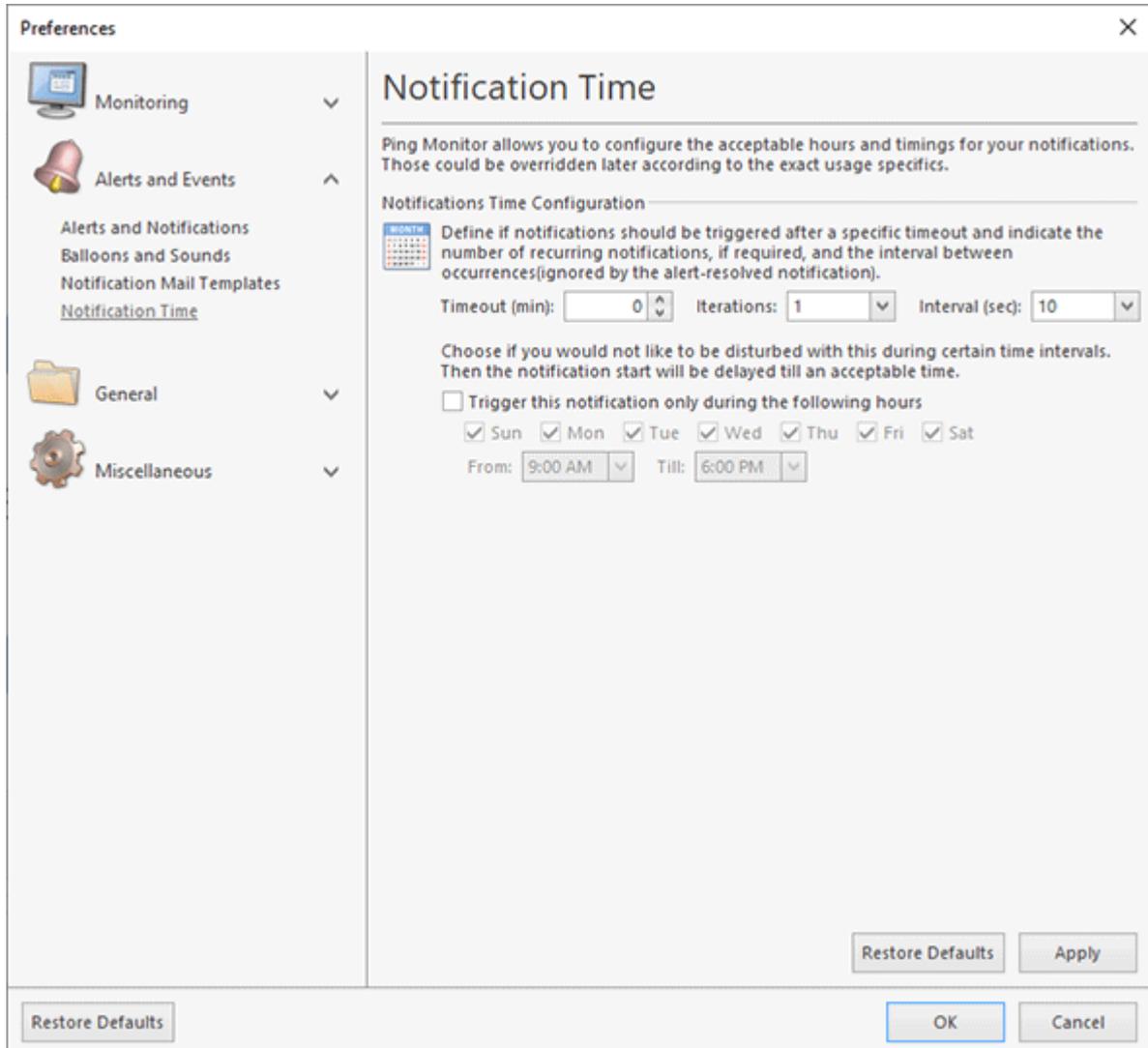
Pic 1. Notification time settings

Notification time configuration allows you to specify a timeout for a notification, so the program will send the notification with a time shift. For example, you can set a 5 minutes timeout, so the program will send you an e-mail notification after 5 minutes, since the alert is detected. If the alert is shorter than 5 minutes the program doesn't send a notification. In the configuration you can also specify a number of iterations and interval between iterations. If a number of iterations is greater than one, the program will send you repetitive notifications until an alert is ended.

If you want to be notified at specific days of the week and at a specific time, you can configure date and time range. Notifications will be not sent at the time out of the configured range.

General Part

The General part of the program preferences should be used to configure reports, custom fields and external tools. To open the **Preferences** dialog, click the **Preferences** button available in the **Application Menu**. Configure the available settings to suit your needs best.

Recipients

On the **Recipients** page of preferences you can specify recipients of e-mail notifications sent by the program. You can specify To, Cc and Bcc fields `Pic 1`. If you need to specify multiple recipients in the same field, you can separate e-mail addresses by a semicolon.
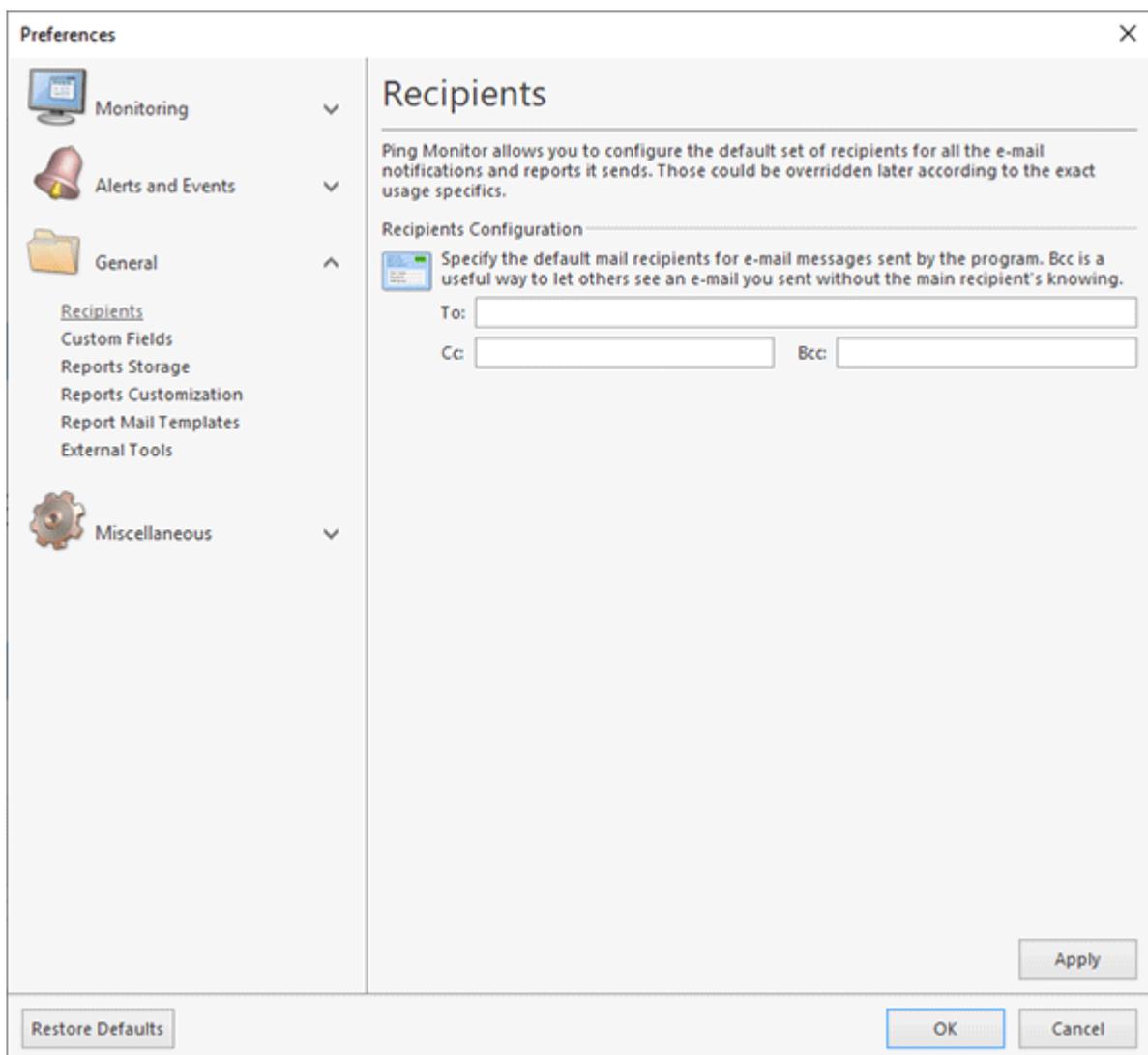
Pic 1. Recipients configuration

Recipients specified in preferences are used by default for all e-mail notifications in the program. You can override them and specify custom recipients for e-mail configuration of alerts and events. You can also configure custom recipients for a specific host or a group.

Custom Fields

The custom fields are additional host properties that are defined by end users. You can use the values defined for those properties in the notifications by specifying the custom field name in the pair of '*%*' signs, e.g. *%CUSTOMER_NAME%*. The set of available custom fields is specified on the **Custom Fields** preferences page **Pic 1**. To access this preference page, press the **Preferences** button from the **Application Menu** and select the **Custom Fields** link in the navigation bar on the left in the opened dialog.
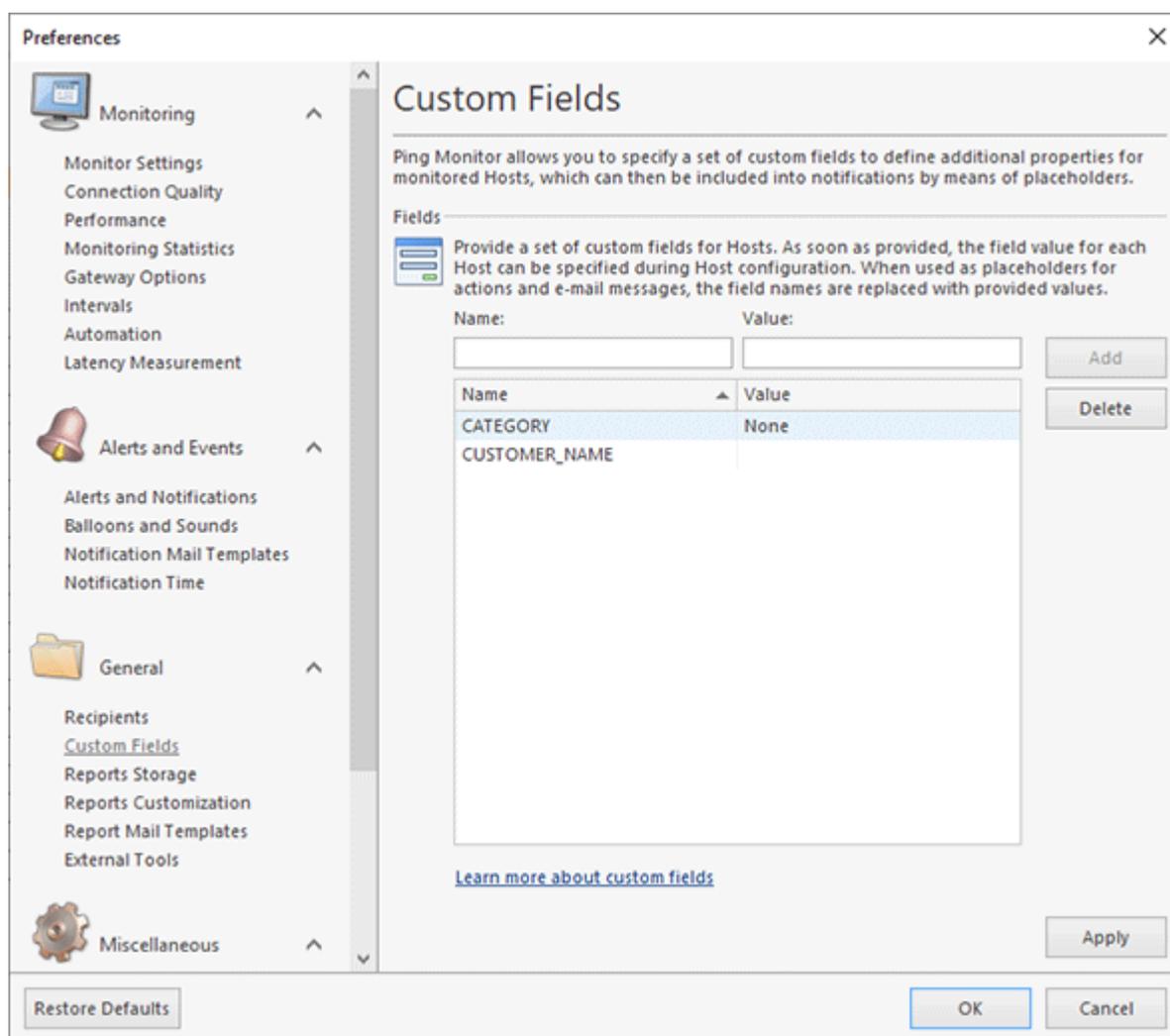
Pic 1. Providing custom fields

To add a new field, just type its name to the **Name** edit box and press the **Add** button. You can configure also a value for a field by specifying it in the **Value** edit box. As the result all hosts in the program will have the specified value. You can override the value and specify a custom one for a host or for a group of hosts. If you want to delete any field, select it in the list and press the **Delete** button. The field will be deleted and the **Field Name** input will filled with its name.

Reports Storage

Ping Monitor allows you to save performance and availability reports to the reports storage. This storage can be located either locally or on an FTP server. The report storage is configured on the **Reports Storage** preference page **Pic 1**. To reach this page, you should open the program preferences using the **Preferences** button from the **Application Menu**, and click the **Reports Storage** link in the navigation bar on the left of the Preferences dialog within the **Events and Statistics** group.
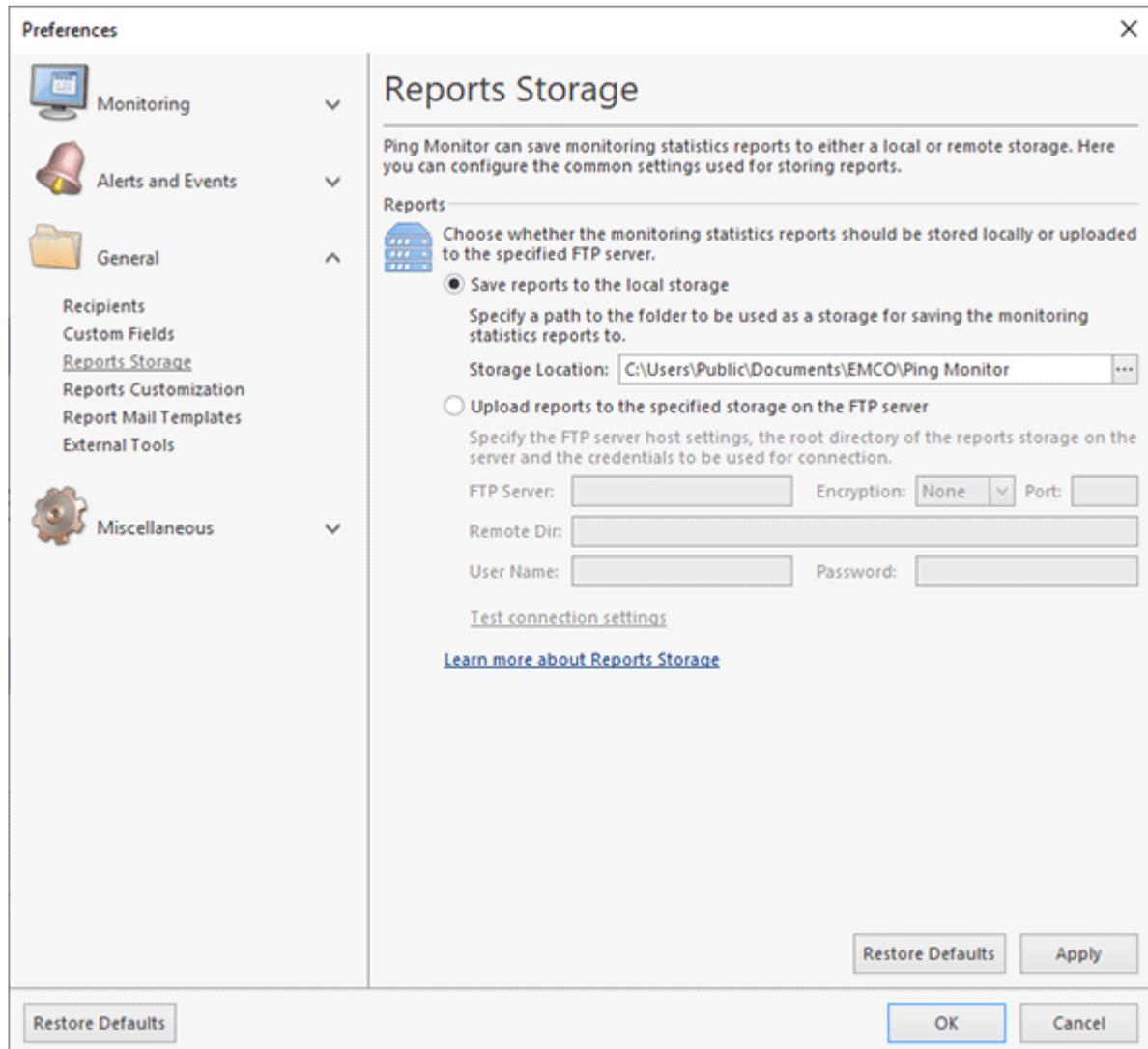
Pic 1. Configuring reports storage

Firstly, you should decide if you would like the reports to be stored in a local storage or uploaded to an FTP server. The **Save reports to the local storage** radio button should be checked for using the local storage, and the **Upload reports to the specified storage on the FTP server** – for uploading reports to the server. For the local storage, you can specify a path to the folder to be used for saving reports to in the **Storage Location** field. It is possible to provide the path manually or pick it from the file system browser, using the button on the right of the editor. The FTP configuration is slightly more complex. The server address should be provided to the **FTP Server** field. You can use both the host name and the IP address for specification. The next step is to choose if the connection should be encrypted in the **Encryption** field. In case the server is using a custom port for files transfer, you should provide the port number to the **Port** field. The **Remote Dir** field is used to specify the location on the FTP server to upload files to. The credentials for

accessing the server are provider to the Username and the **Password** fields respectively. After the settings are provided, you can check if the program is able to access the server using the **Test connection settings** hyperlink.

The report storage settings defined in a program preferences are used by default for all generic and preconfigured reports when generating a file report output. For the preconfigured reports, the settings can be overridden for a specific report during the outputs configuration.

Reports Customization

Ping Monitor enables you to customize the header and the footer of the PDF, HTML and MHT reports generated by the program. The configuration options are available on the **Reports Customization** preference page. To reach the **Reports Customization** page, you should open the program preferences using the **Preferences** button from the **Application Menu** and click the **Reports Customization** link in the navigation bar on the left of the **Preferences** dialog within the **Events** and **Statistics** group.
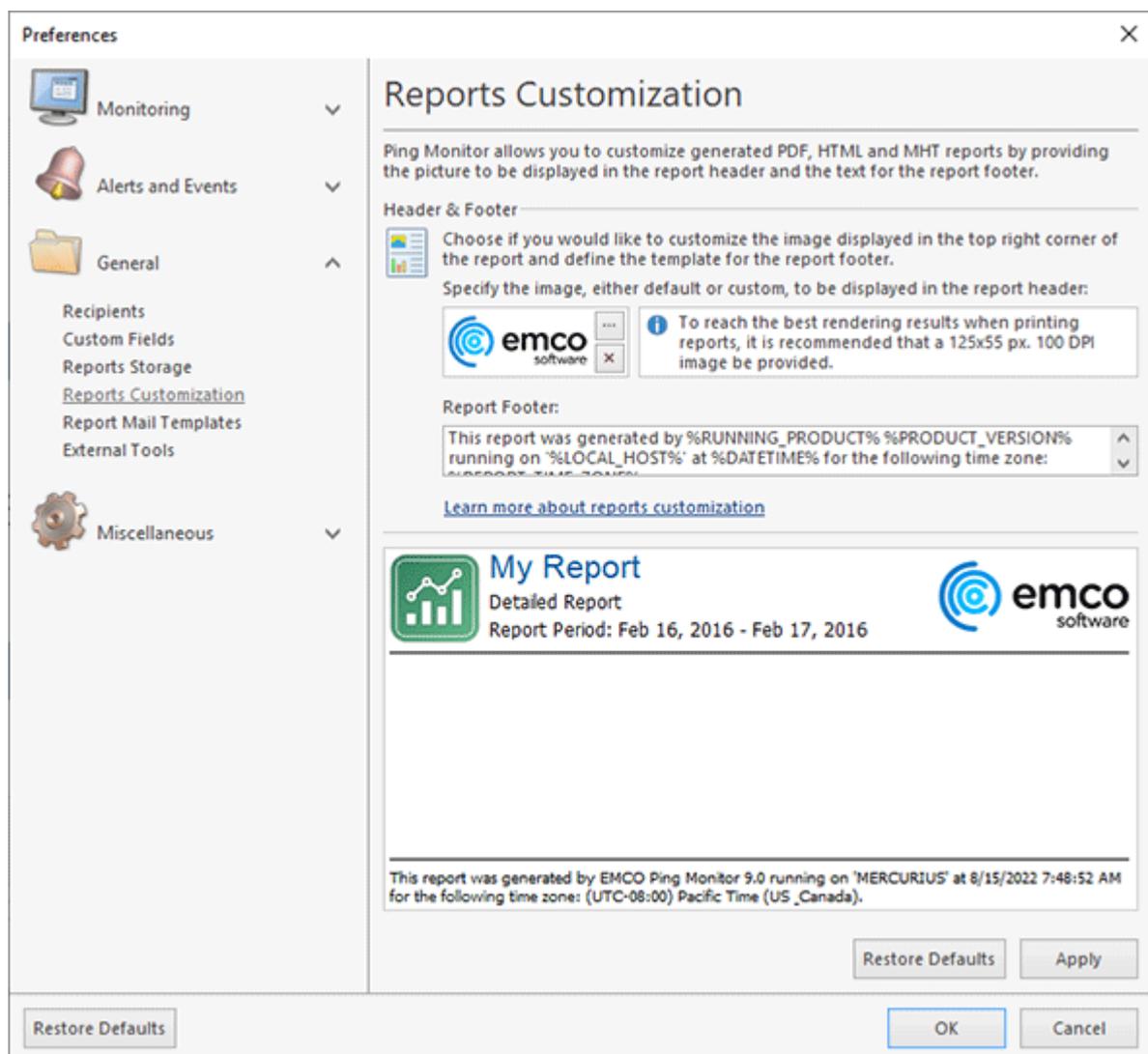
Pic 1. Reports customization

For the report header, you can choose if you would like a custom image to be displayed in the right top corner instead of the EMCO Software logo, and for the footer, you can define a text template. At the bottom of the page, you can see the preview for the header and the footer of a report generated using the defined settings.

To use a custom image, you should use the [...] button of the picture edit. To reach the best rendering results when printing reports, it is recommended that a 125x55 px. 100 DPI image be provided. Smaller images will be centered in the logo area and lager ones will be scaled down to fit the logo area. If you would like to revert to the default header image, you can use the [×] button of the edit.

The report footer template is provided to the **Report Footer** field. When providing a template, you can use placeholders that are replaced with actual values during the report generation. Refer to the Report Footer Placeholders section of the document.

Report Mail Templates

Report Mail Templates are used to form e-mail reports sent by Ping Monitor. They can be configured on the **Report Mail Templates** preference page **Pic 1**. To access this page, click the **Preferences** button from the **Application Menu** and select the appropriate link in the navigation bar on the left of the **Preferences** dialog within the Alerts and Events group.
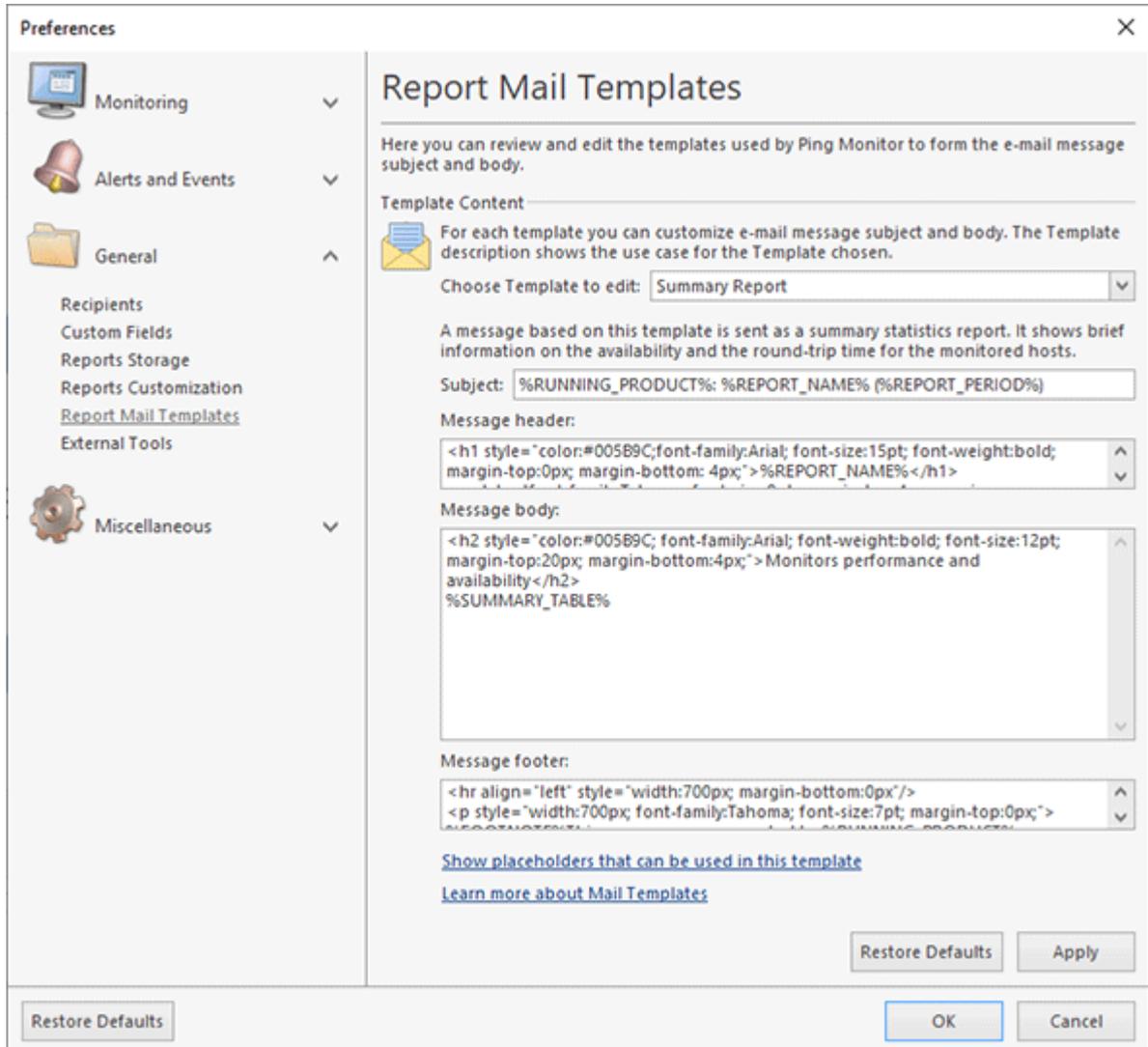

Pic 1. Configuring Report Mail Templates

On this page, you are offered to choose a template that you want to review and edit. The template description shows you the use case of the chosen template, and if there are placeholders available for this template, a link to a detailed placeholders description is shown under the template description. For a selected template you can see a text that should be used in e-mail subject, body, header and footer. You can edit it if required.

External Tools

EMCO Ping Monitor comes with a built-in feature of launching external tools for hosts selected in the **Hosts** view. A set of available tools is provided on the **External Tools** preference page **Pic 1**. You can reach this page by choosing the **Configure External Tools** menu item from the **External Tools** menu on the host or clicking the **Preferences** button from the **Application Menu** and selecting the **External Tools** link on the navigation bar on the left in the opened dialog.
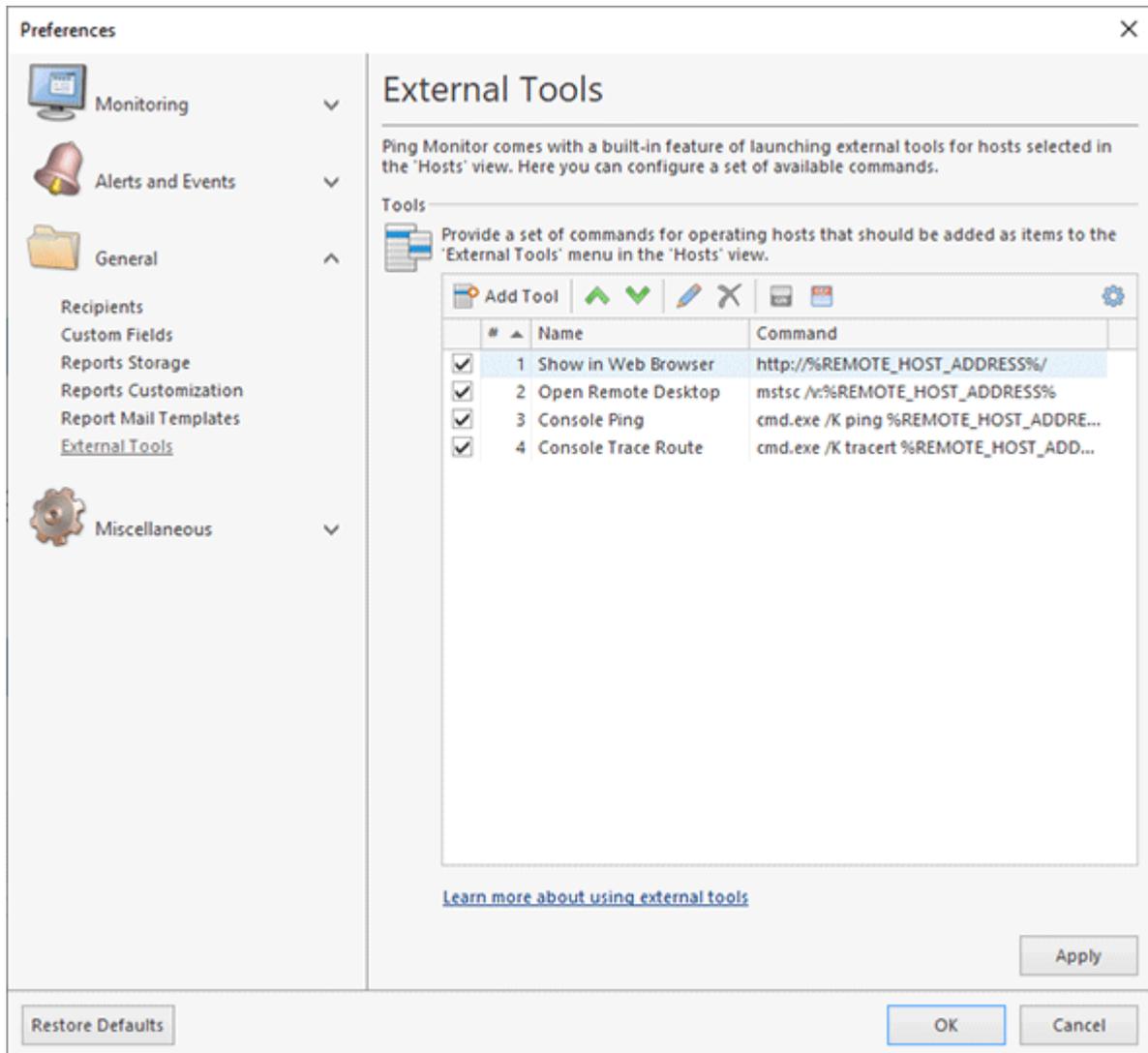
Pic 1. Providing external tools

Ping Monitor is shipped with several predefined tools. You cannot change the command for those tools, but can rename them, if required. Also you can disable any or all of those tools if not found useful. It is possible to create your own commands. Just press the **Add Tool** button and proceed with the required configuration `Pic 2`.
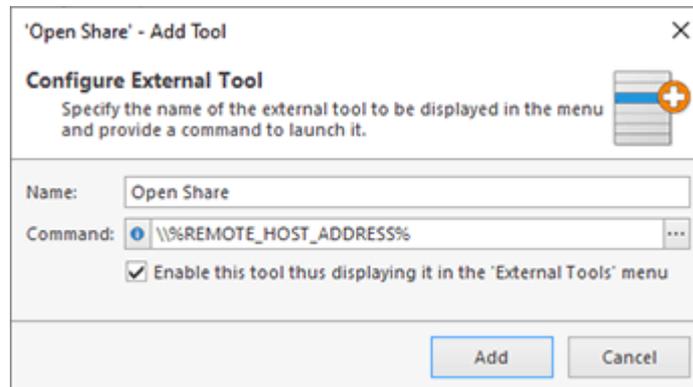
Pic 2. Creating a user-defined external tool

When configuring a tool, you can provide a name to be displayed in the pop-up menu and the command to be launched when the menu is clicked. You can use custom fields and other common placeholders when specifying the command.

The commands order in the menu is controlled via the **Move Up** and **Move Down** buttons. To edit the command, use the **Edit** button, and the **Delete** button should be used to delete the selected external tools.

Miscellaneous Part

The **Miscellaneous** part of the program preferences should be used to configure the common Ping Monitor options, such as the program behavior in respect to the System Tray, the proxy settings to be used to connect to the Internet, etc. To open the **Preferences** dialog, click the **Preferences** button available from the **Application Menu**. Configure the available settings to best suit your needs.

General Settings

Ping Monitor can automatically check for updates for you to always have the latest version of the program and can be added to the Windows startup. You can configure this features from the **General Settings** preference page. To open this page, click the **Preferences** button from the **Application Menu** and select the **General Settings** link in the navigation bar on the left in the **Preferences** dialog within the **Miscellaneous** group `Pic 1`.
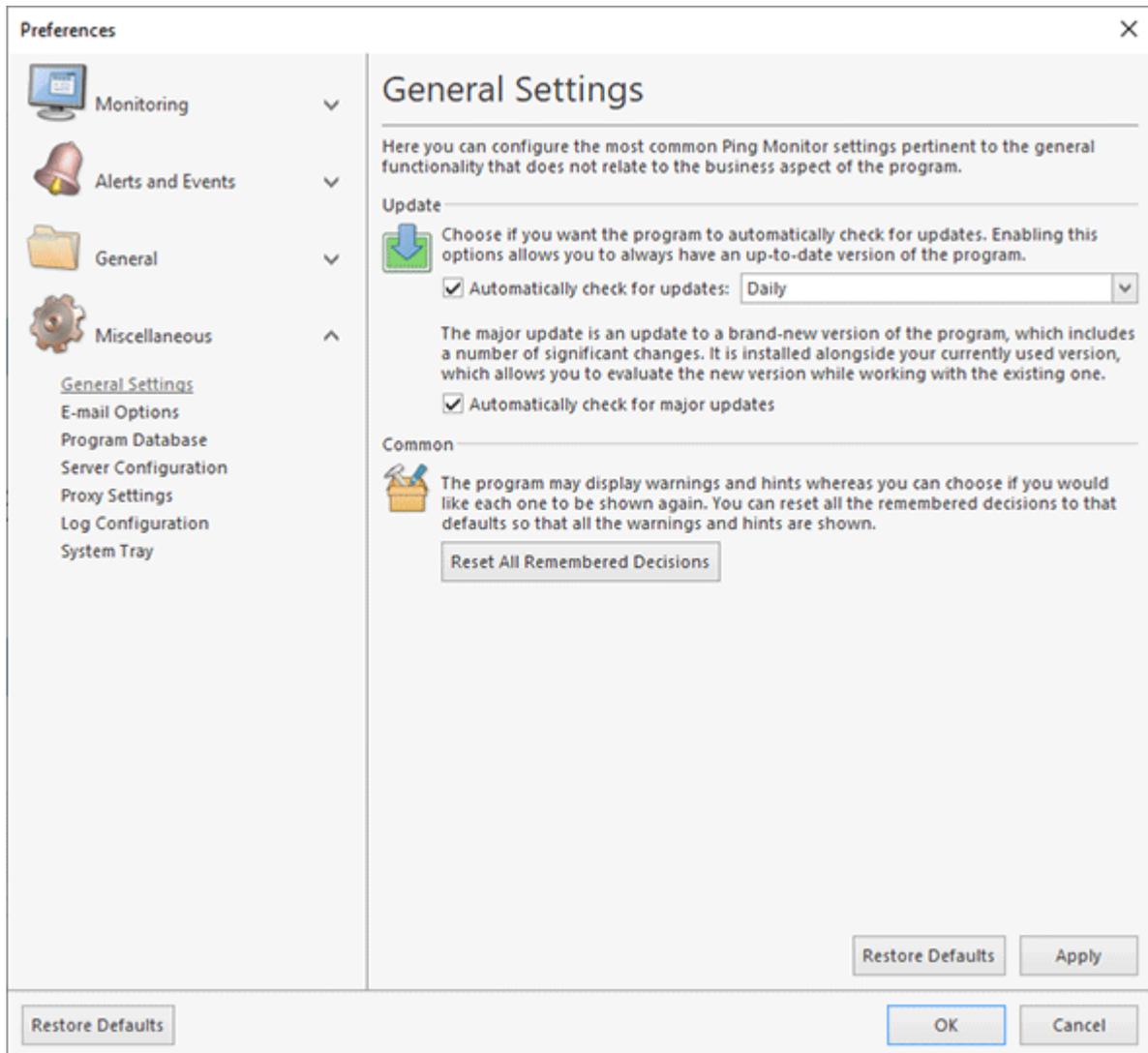
Pic 1. Configuring general settings

Ping Monitor can check for updates automatically every day or once a week. To enable an automatic checking for updates, check the **Automatically check for updates** option and choose the checking frequency between **Daily** and **Weekly**. You can also define if the program should check for major updates by changing the **Automatically check for major updates** option value.

> ℹ️ If you use a proxy server to connect to the Internet and the required proxy settings are not provided, an automatic check for updates will not take place.

If you want Ping Monitor to be automatically started right after you are logged on to the underlying operating system, enable the **Launch at Windows startup** option.

E-mail Options

Ping Monitor can send notification e-mails only after your mailbox settings have been configured properly. To perform the mailbox configuration click the Preferences button from the **Application Menu** and select the **E-mail Options** link in the navigation bar on the left in the **Preferences** dialog within the **Miscellaneous** group.

Pic 1. Configuring a mailbox

You should specify the mail server host, the encryption type the port to be used for connection to the mail server, the e-mail address to send e-mail messages from, the e-mail message format and the credentials to be used to access the mail server.

> Although Ping Monitor supports both explicit and implicit SSL/TLS encryption, it is strongly recommended that explicit SSL/TLS be preferred due to its optimized performance and security. Thus, implicit SSL/TLS should only be used for compatibility with servers that do not support explicit SSL/TLS.

The **Mail Server (SMPT)** value can be provided both as an IP address and as a host name `Pic 1`.

> Ping Monitor supports mail servers that run using SMTP. A mail server configuration may be quite complex. Contact your system administrator to get proper configuration details to be used for accessing your mailbox.

You can send a test e-mail to check the settings provided using an appropriate hyperlink. In the next section, it is described how the settings test works and how you can tell if the e-mail options are configured properly.

How does the test work?

After you have configured the e-mail options you can send a test e-mail to check the mail server settings. A test message is generated and sent to the specified recipients and the e-mail address specified in the **E-mail Address** field. If you and the other recipients receive the message, it is assumed that the mail options are configured properly, and there will be no problems with sending notification e-mail messages.

Program Database

The program database is a storage used by Ping Monitor to keep all business data and logged events. The program database configuration can be changed on the **Program Database** preference page. To access this page, click the **Preferences** button from the **Application Menu** and select the corresponding link in the navigation bar on the left of the **Preferences** dialog within the **Miscellaneous** group.

By default, Ping Monitor uses the SQLite database management system to store the data within the common application data folder. Using this concept as default, allows you to start using the program without performing additional data storage configuration. The program also supports the Microsoft SQL Server database management system. You can choose the database engine to be used within the **Database Management System** drop-down list.
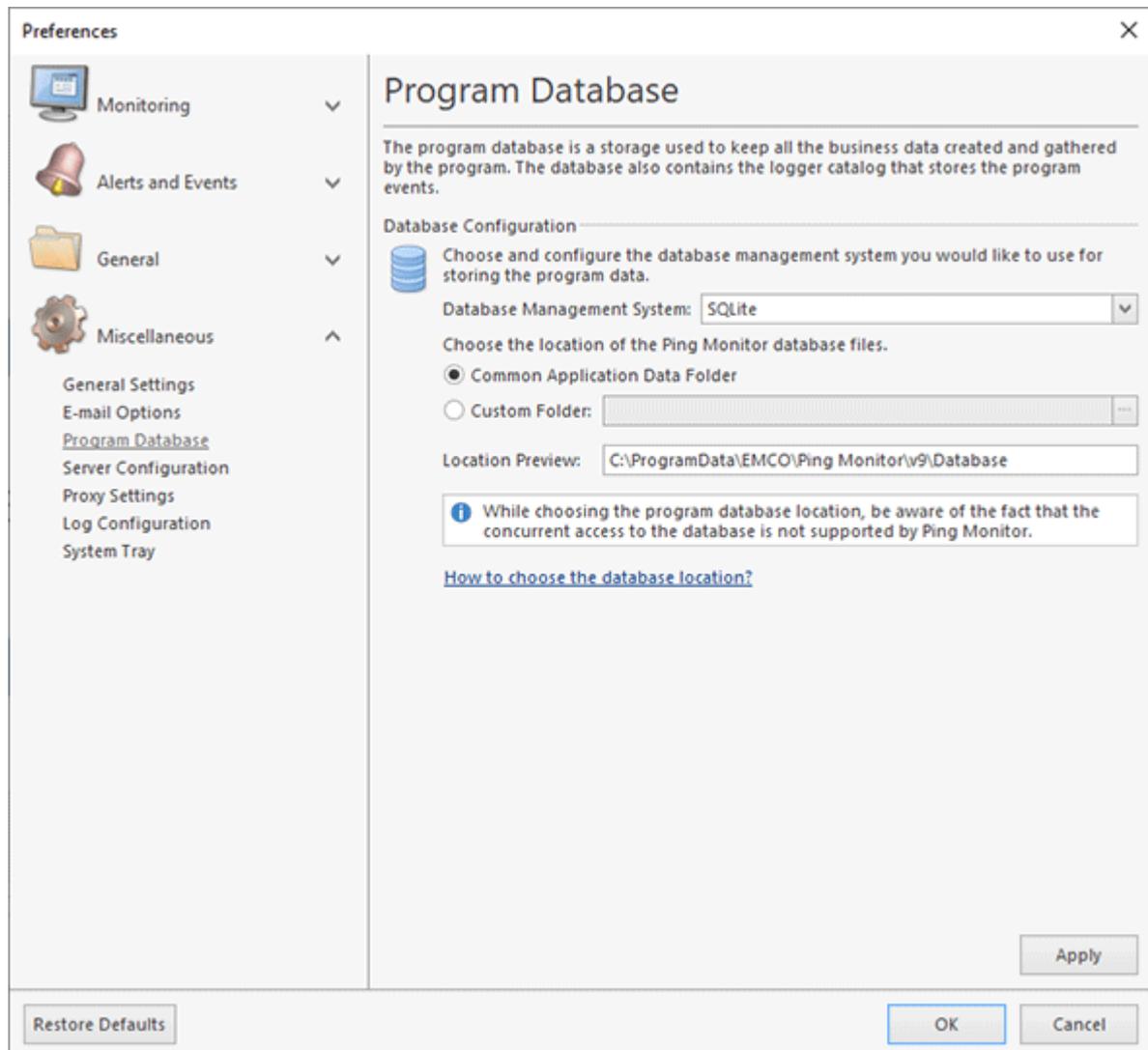
Pic 1. Configuring the SQLite database

For the SQLite database, you can choose a new database location `Pic 1`. You can either choose the predefined database location or provide a path to the database files manually. While choosing the program database location, be aware of the fact that the concurrent access to the database is not supported by Ping Monitor. Please also take into account that full access to the database location folder should be granted to the program for it to operate correctly.

Although the SQLite database is preconfigured and set by default, it is recommended to use the Microsoft SQL Server database if you are going to operate in an enterprise environment, because it provides you with a much higher performance and reliability `Pic 2`.
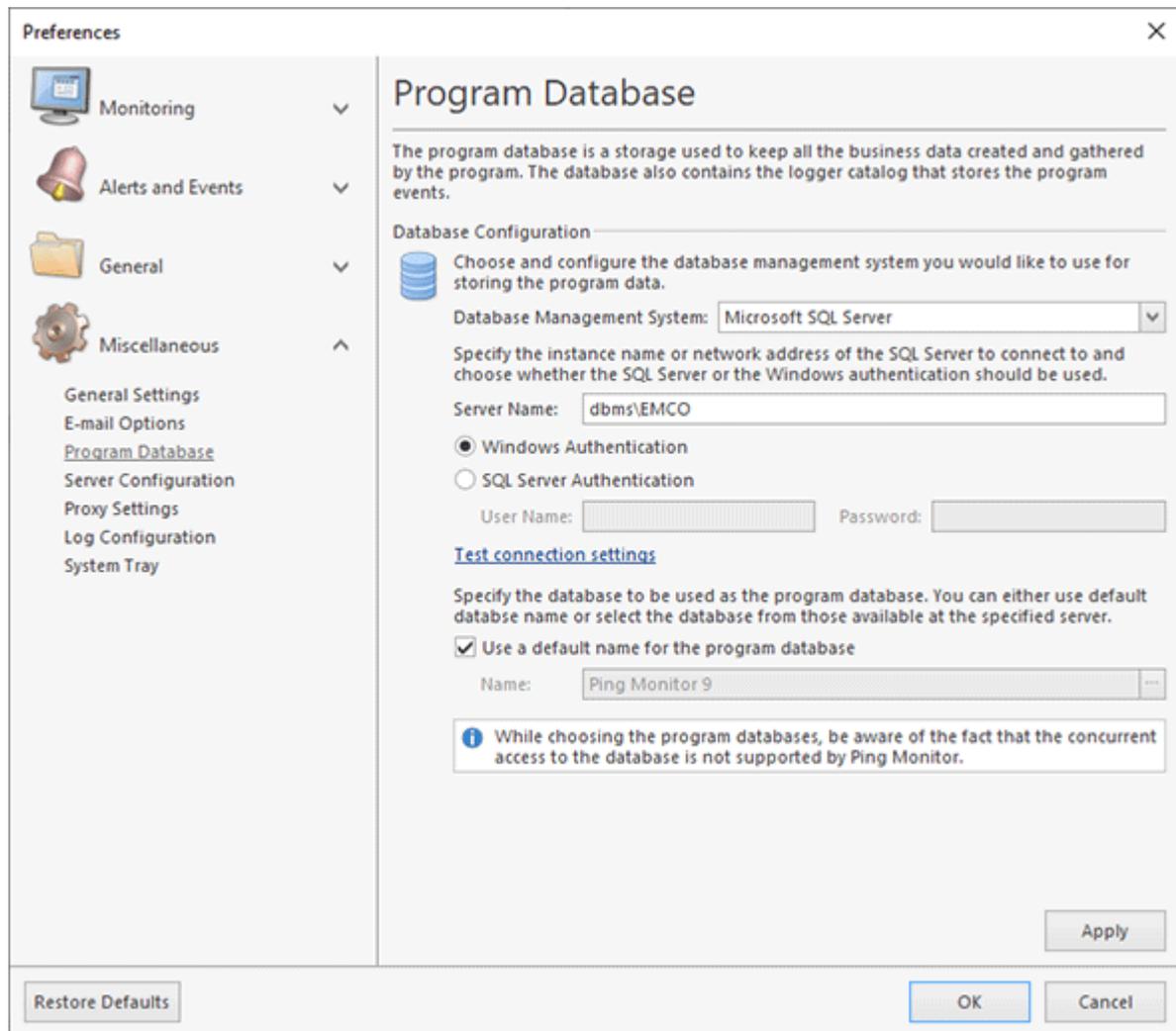
Pic 2. Configuring the Microsoft SQL Server database

While choosing the Microsoft SQL Server database to be used by Ping Monitor, you should provide the database server name to the **Server Name** field and configure the authentication options. You can choose between **Windows Authentication** and **SQL Server Authentication**. It is strongly recommended by Microsoft that integrated security via **Windows Authentication** be preferred. As soon as you have completed this configuration step, you can press the **Test Connection Settings** hyperlink to check if the database server is accessible.

The next step is choosing the database to store data in. You can either use the default configuration or define the required database manually. When choosing a database from those available on the server, it is also possible to create a new one with default settings having provided its name.

When you apply changes to the program database configuration, the program checks the provided settings for validity. If the specified database is empty, you are proposed to fill it with the data available in the database currently used by the program. This feature allows you to switch to the Microsoft SQL Server database from the SQLite database you are using easily and at any time. Besides, if the server restart is required for the applied changes to take effect, you are immediately prompted to restart the server.

Server Configuration

EMCO Ping Monitor server allows connection from both local and remote clients, including those from other Windows domains and those reachable through the Internet only. When connecting to the EMCO Ping Monitor server using the windows credentials of the session run by the client, the integrated security is used for authentication and communication processes. In a cross-domain case, the client is authenticated to the server using the specified windows credentials, and the server is authenticated with the help of a domain identification certificate enabling communication over a secure socket layer of a TCP channel. This process can be configured on the **Connection Options** preference page `Pic 1`. This page is also used to enable the e-mail notifications on issues with the server, if required. To open the **Server Configuration** page, click the Preferences button in the Application Menu and press the corresponding link in the navigation bar on the left of the **Preferences** dialog within the **Miscellaneous** group.
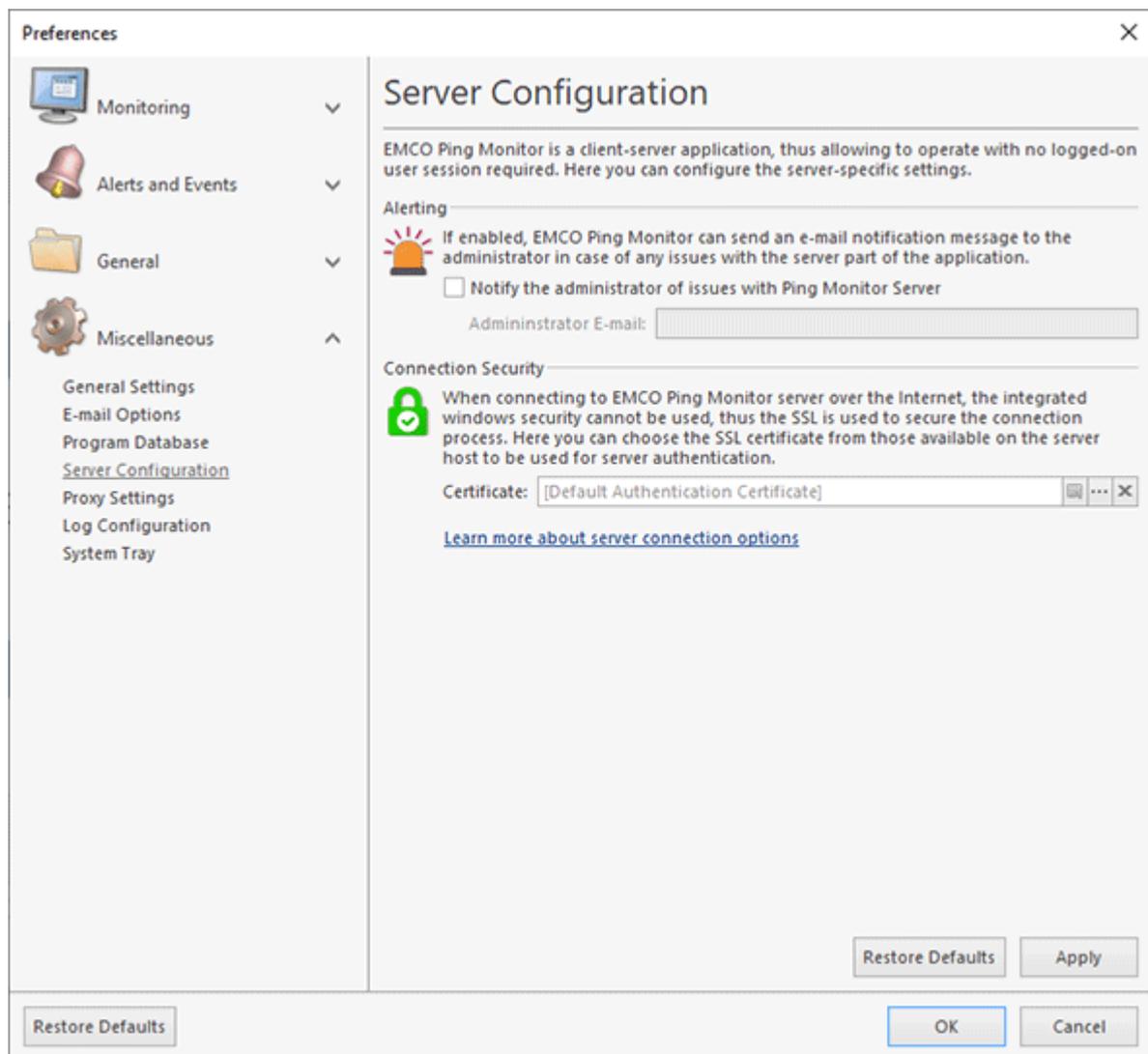
Pic 1. Specifying Server Configuration

If enabled, the server part of Ping Monitor can send e-mail notification messages to the administrator in case of any issues with the server. If you are interested in such notifications, just check the corresponding checkbox and provide the administrator e-mail address to the **Administrator E-mail** field.

By default, the server uses a self-signed custom certificate issued to PingMonitorServer.exe, thus there is actually no identification of the server host. It is possible to accept this certificate when

connecting to the server; however, it is strongly recommended to use a certificate that actually identifies the server. Such a certificate should be issued to the specific server host by a certification authority trusted in your organization.

For a digital certificate to be used by Ping Monitor for authenticating the server, the following set of requirements must be met:

1. The certificate must include the **Server Authentication (1.3.6.1.5.5.7.3.1)** within its Intended Purpose.

2. The certificate's **Valid From** date must be earlier and the **Valid To** date must be later than the connection date.

3. The digital certificate must be placed in the **Local Computer** certificates storage.

4. The private key must be available together with the signing certificate in the certificates storage. In case you have a private key in a separate file, please use the tool provided by Microsoft for preparing a private & public key pair to be imported into the certificates storage as described here: Pvk2Pfx, Combine PVK + SPC to PFX.

To choose a certificate, you should use the **Select Certificate** button in the **Certificate** field. A dialog will be displayed showing you the server authentication certificates available on the PC hosting the service. You can review detailed information on each of the available certificates using the **View Certificate** button. The same button is also available in the **Certificate** field when a server authentication certificate is already selected. The **Reset Certificate** button in the **Certificate** field should be used to discard the selected certificate and use the default one.

To start using the selected certificate for securing communication, it is required to restart the server. The program will notify you of it and prompt for an immediate server restart.

Proxy Settings

Ping Monitor requires an Internet connection to support the **Live Update** and **Feedback** features, as well as be able to upload reports to an FPT server. Therefore, if a proxy server has to be used to connect to the Internet, it should be configured on the **Proxy Settings** preference page `Pic 1`. To access this page, click the **Preferences** button from the **Application Menu** and select the appropriate link in the navigation bar on the left in the **Preferences** dialog within the **Miscellaneous** group.
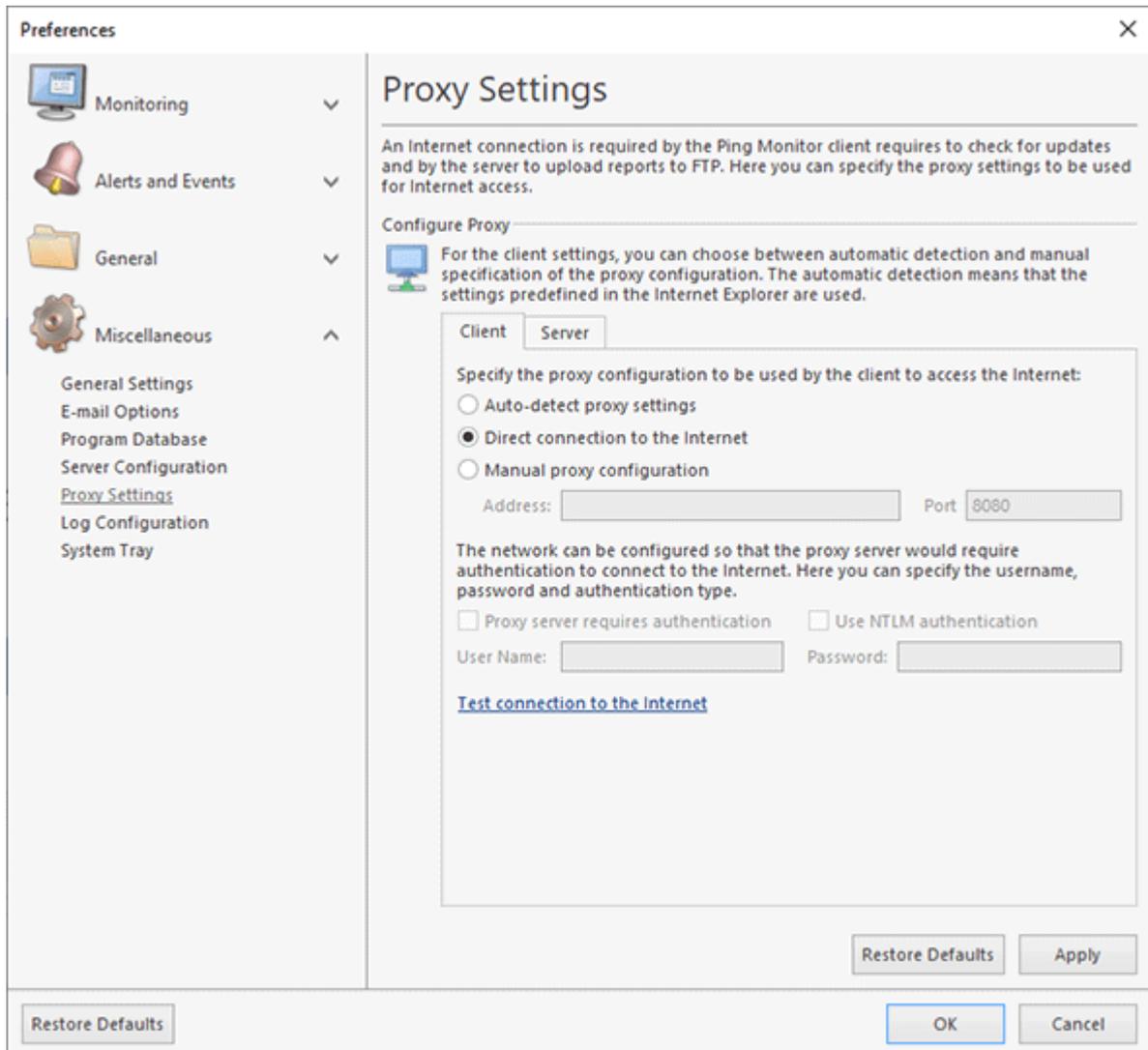
Pic 1. Proxy Settings

On this page, you can configure client and server proxy settings. The client settings are used when checking for updates and providing feedback, the server settings are applied when uploading reports to an FTP server. For the client settings, you may choose among three variants of the proxy configuration. If **Auto-detect proxy settings** is chosen, the program uses the settings predefined in the **Internet Explorer**. If Ping Monitor does not have to use a proxy server to connect to the Internet, the **Direct connection to the Internet** option should be chosen. The **Manual proxy configuration** option allows you to provide the proxy server address and port manually.

Both for the automatic detection and manual configuration, it is possible to specify if the proxy server requires authentication and what credentials should be used to connect to the proxy server. For the manual configuration, an NTLM authentication can be used (i.e. connection to the proxy

228

server takes place using the credentials of the user currently logged on) by enabling the **Use NTLM authentication** option.

As for the server settings `Pic 2`, the configuration process is the same. The difference is only that it is not possible for the server side to detect proxy settings automatically and use NTLM authentication.
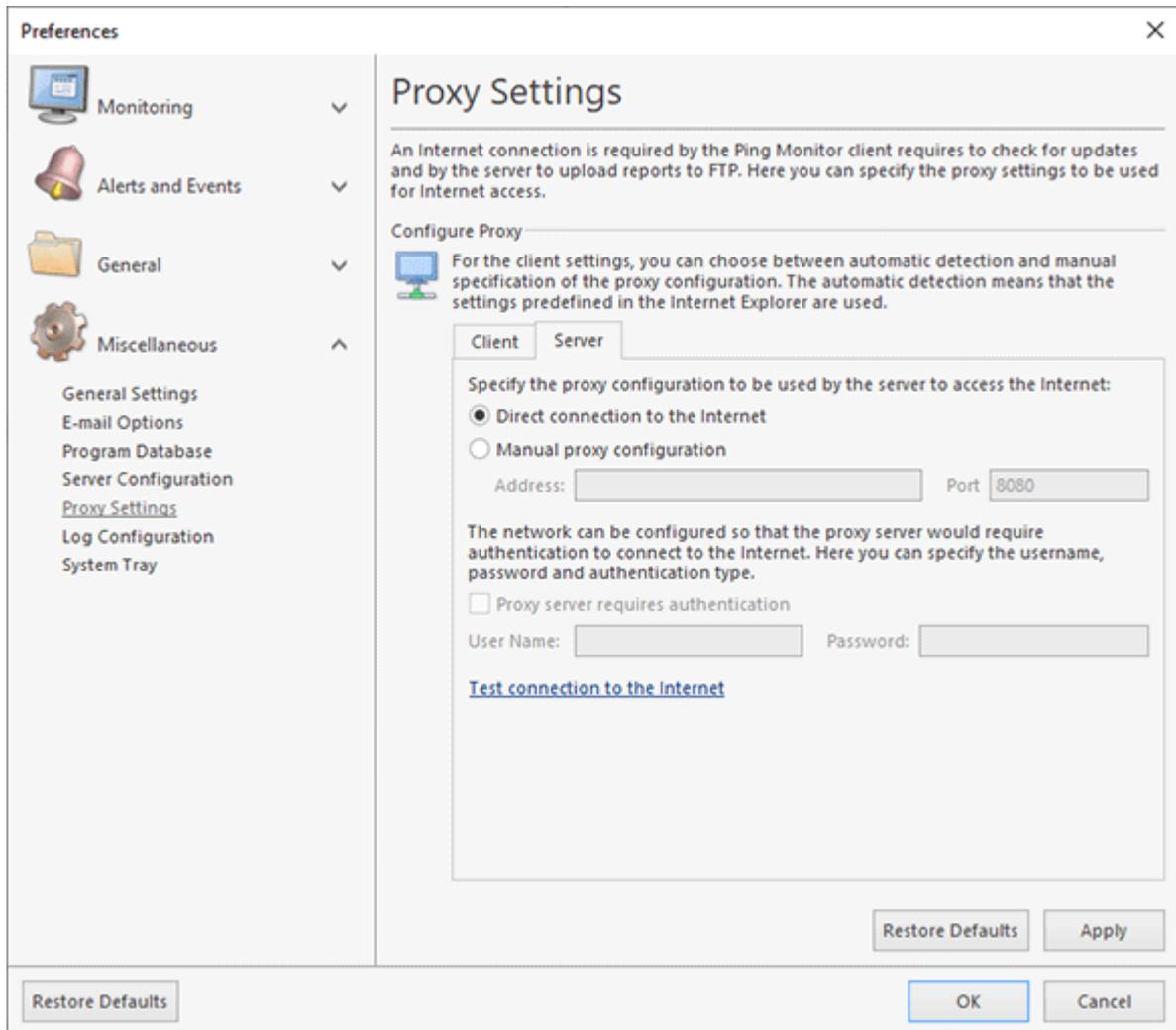
Pic 2. Server proxy settings

After the proxy settings have been configured, it is possible to test if the Internet connection is available by using the corresponding hyperlink on the bottom of the settings page.

Log Configuration

To configure the **Log** behavior, click the Preferences button from the **Application Menu** and switch to the Log Configuration preference page using the appropriate link in the navigation bar on the left in the Preferences dialog within the Miscellaneous group. Here, you can specify the logged events auto-removal options `Pic 1`.
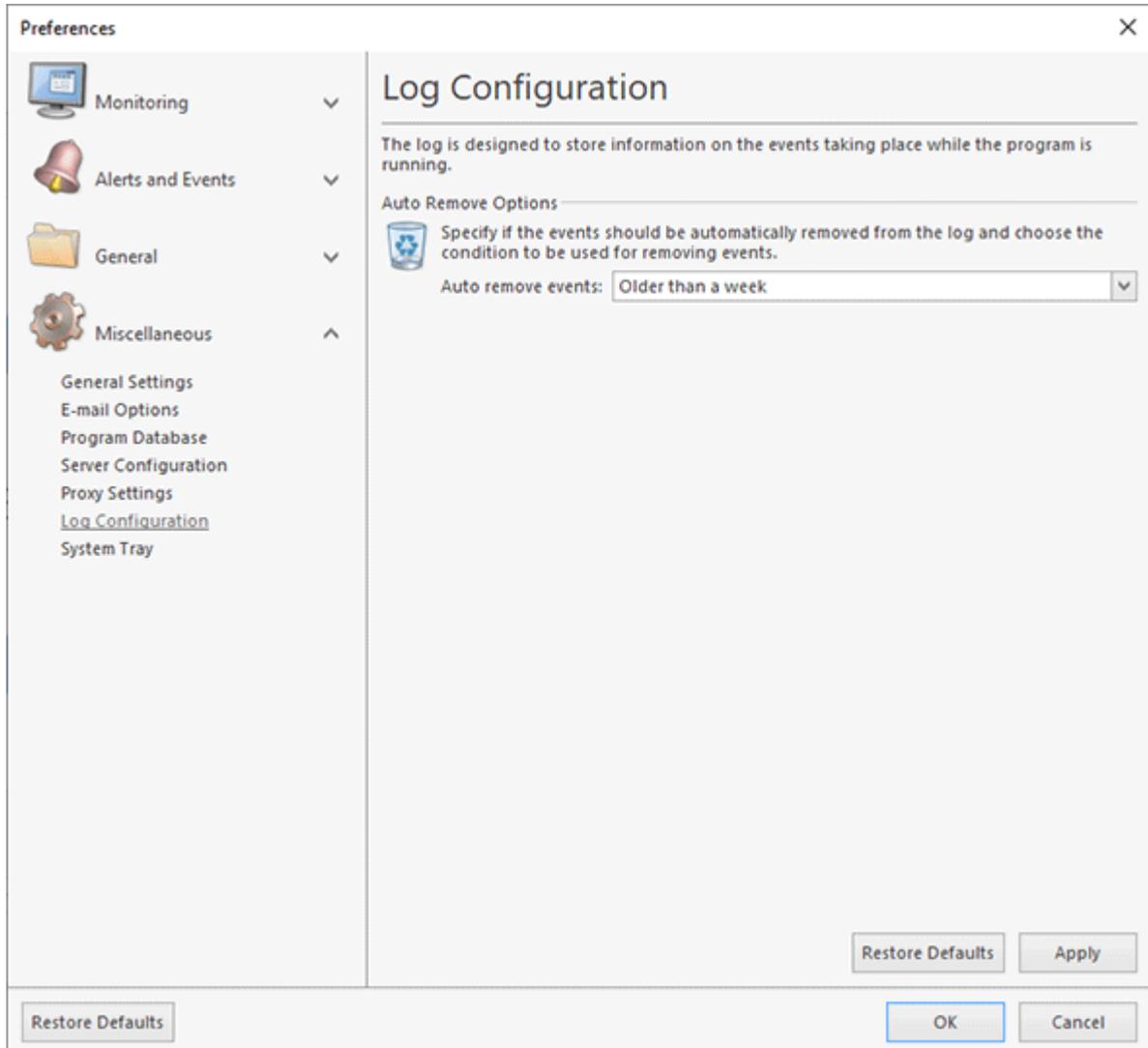
Pic 1. The log configuration

Ping Monitor gives you an option of an automatical removal of logged events from its database. The maximum event age can be specified by the **Auto remove events** option. Choose **Do not remove events** if you do not want any events to be removed automatically. Anyway, it is always possible to remove logged events by clearing log manually.

System Tray

The Tray icon provides a quick access to some of the program functionality and serves to notify you of any significant changes taking place while the program is running when the main program window is minimized or hidden behind other windows. To configure the program behavior regarding the **System Tray**, click the **Preferences** button from the **Application Menu** and switch to the **System Tray** preference page using the corresponding link on the navigation bar to the left in the **Preferences** dialog within the **Miscellaneous** group `Pic 1`.
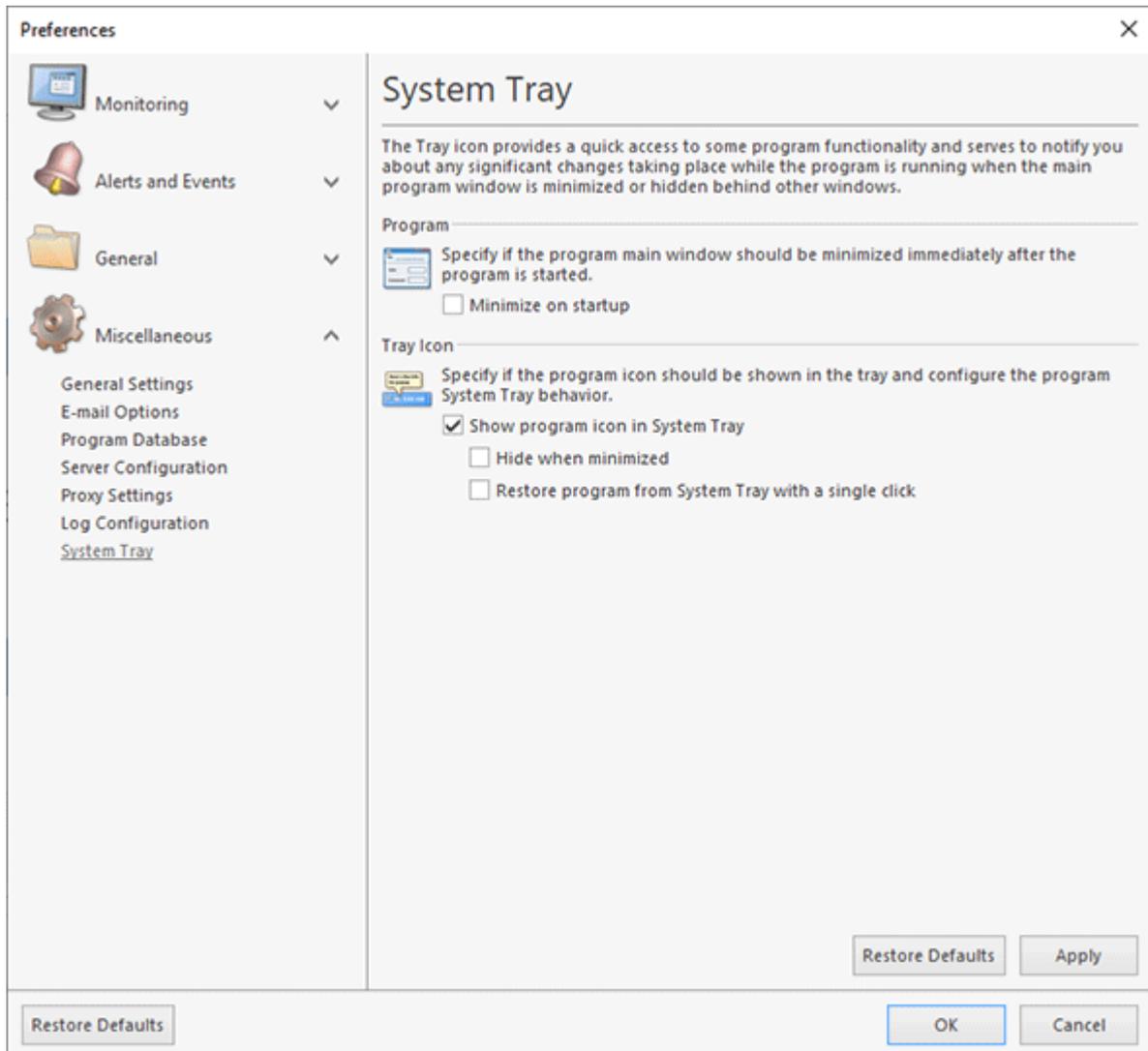
Pic 1. Configuring the System Tray behavior

If you prefer the program main window to be minimized during the program start, you should check the **Minimize on startup** option.

The **Show program icon in System Tray** option allows you to choose if the program icon should be shown in the tray. If it is enabled, you may also specify if the program should be hidden from the Windows taskbar when it is minimized to System Tray, and if the main window should be restored from the tray with a single or double click.

Chapter 11: Evaluation of the Program

Ping Monitor is a shareware product, so you can try it before ordering a license. The download includes a free 30-days trial of the Enterprise edition of the program. It provides access to all the available features. After the trial expires, the program reverts to the Free edition, and you can keep using it as long as you like. You can order a license for a commercial edition of the program to register it and use the program's commercial features.

This chapter will cover the particularities of the evaluation mode, tell you how and where you can get the license code and how you can request the extended evaluation. Read this chapter carefully to face no difficulties during the EMCO Ping Monitor evaluation.

Evaluation Wizard

As long as the EMCO Ping Monitor is not activated on each program startup the **Evaluation Wizard** `Pic 1` is displayed on the screen, showing you the information about the evaluation process and providing with quick links for the program activation, purchase and extended evaluation request.
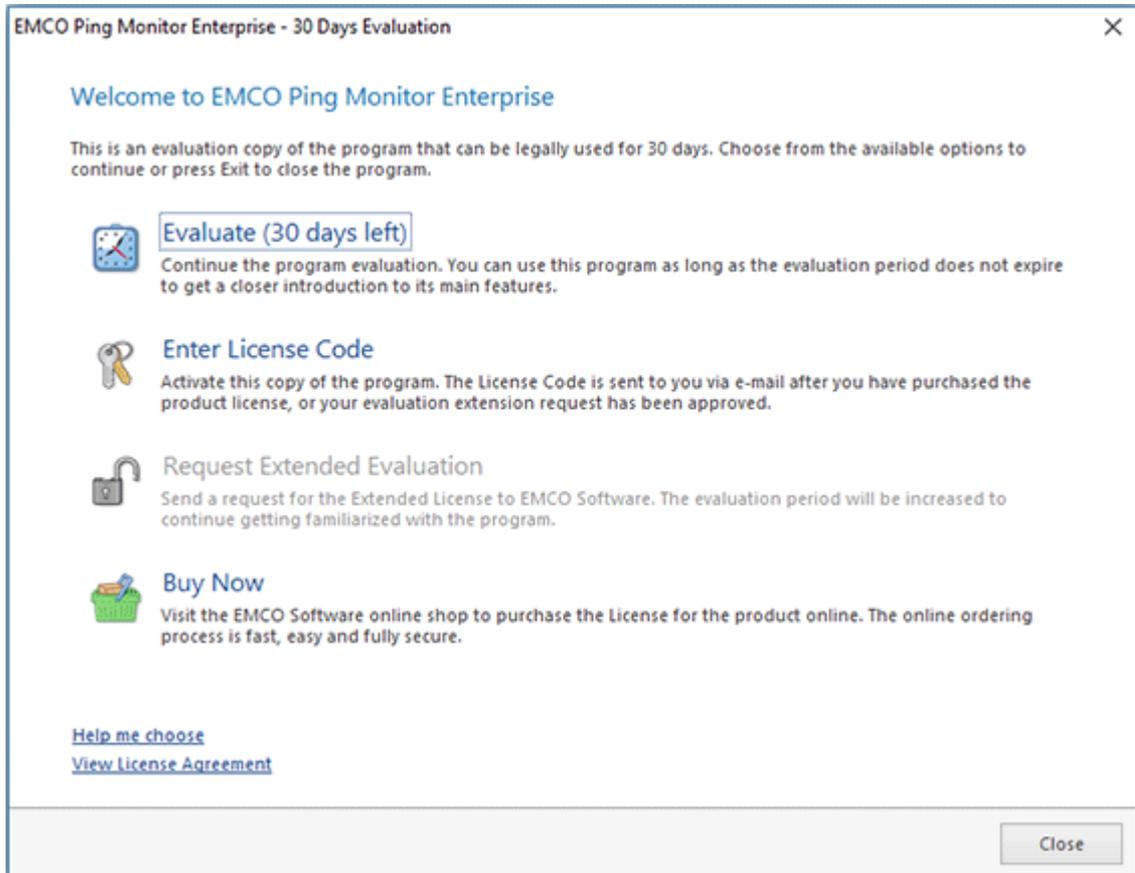
Pic 1. The EMCO Ping Monitor Evaluation Wizard welcome page

The welcome page of the **Evaluation Wizard** allows you to choose between four options to continue. Those are **Evaluate**, **Enter License Code**, **Request extended evaluation** and **Buy now**. Optionally you can press **Exit** button to close the program. In this section we will help you to choose the option that will best fit your needs.

The **Evaluate** option shows you the time left until the evaluation period expires. You should choose this option to continue the evaluation process – the wizard will be closed and you can start working with Ping Monitor. You can use the program as long as the evaluation period does not expire to get a closer introduction to its main features.

It you have already purchased the license for using the EMCO Ping Monitor you should choose the **Enter License Code** option to activate the program. This options also should be chosen if the extended evaluation request has been approved by EMCO Software and you have been provided with the Extended License. If you are having problems with finding the License Code refer to the Where can I get my License Code? section of this document. After choosing the **Enter License Code** option the program activation page is displayed on the screen Pic 2.
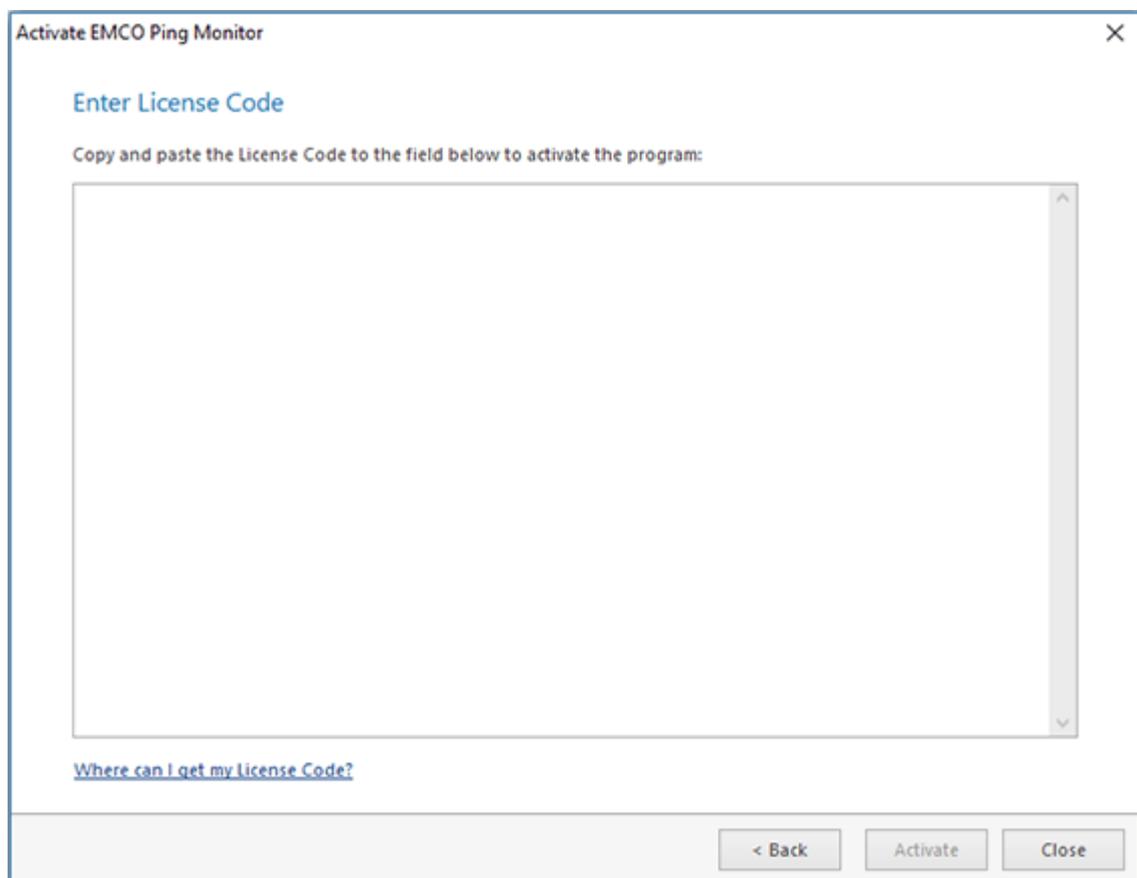
Pic 2. Activating EMCO Ping Monitor

To activate EMCO Ping Monitor copy and paste the License Code to the input field on this page and press **Activate**.

If the evaluation period has expired and you are not sure you have fully introduced yourself to EMCO Ping Monitor main features you can once request the extended evaluation. As soon as the request is processed by EMCO Software you are provided with the Extended License to prolong the evaluation period. To request the Extended License you should choose the **Request extended evaluation** option. After choosing this option the request form will appear on the screen `Pic 3`.

Pic 3. Requesting an extended evaluation

To request the Extended License fill the fields on the request form regarding the recommendations and press the **Send Request** button.

The **Evaluation Wizard** also provides you with the short cut action that allows you to visit EMCO Software web store. To use this feature choose the **Buy Now** option. The on-line ordering process is fast, easy, and fully secure.

Where can I get my License Code?

After you have purchased the license for using EMCO Ping Monitor our experts will generate the License Code and send it to you via e-mail to the address you have specified during the purchasing process. You are supposed to receive two e-mail messages – one with the License Code written in the message body and one with the attached text file (license.txt), containing the license. It is your choice to use any message because both License Codes are identical.

To activate the program the License Code received via e-mail should be copied and pasted to the program activation form `Pic 1`. This form can be reached using the **Enter License Code** button from the **Information** group on the Ribbon bar or by choosing the appropriate option in the **Evaluation Wizard**.
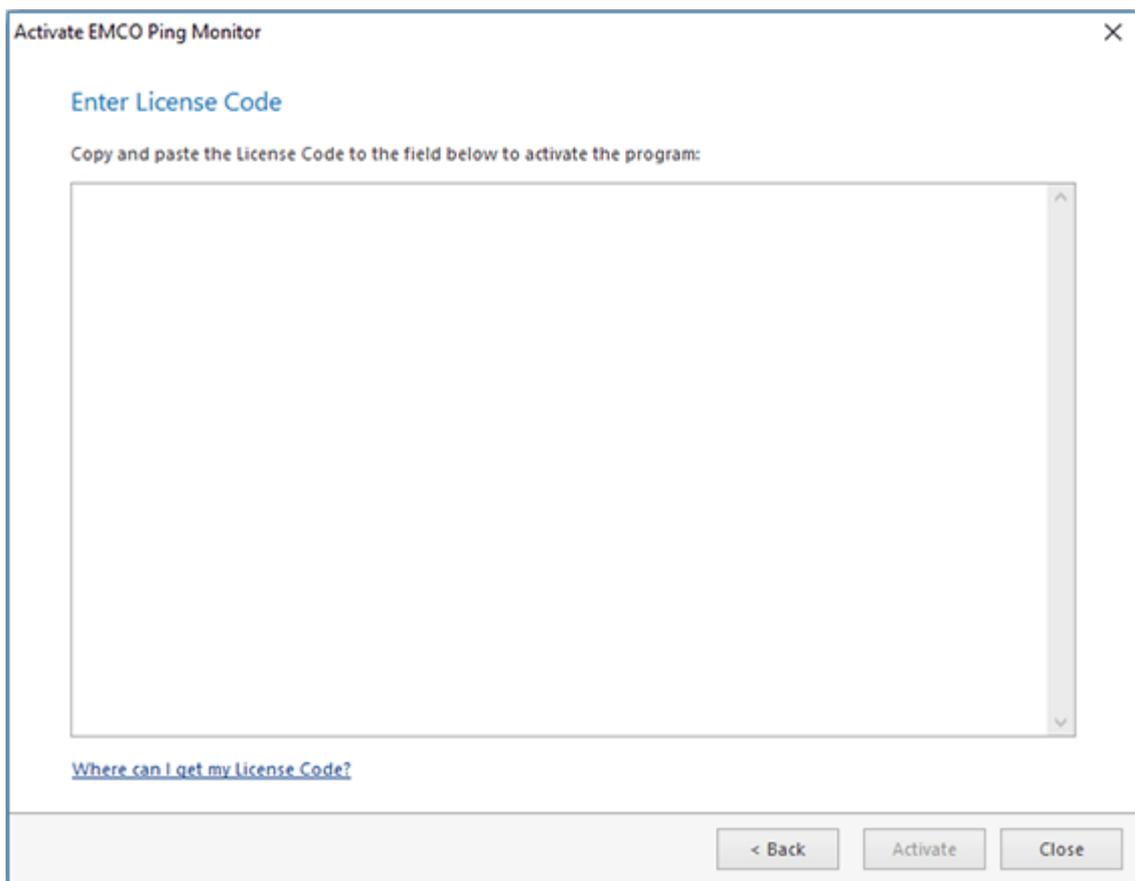
Pic 1. Activating EMCO Ping Monitor

To activate Ping Monitor, copy and paste the License Code to the input field and press **Activate**.

How should I formulate the Extended License request?

The Extended License is used to prolong the evaluation period to get a closer look at EMCO Ping Monitor. This feature can be reached by choosing the appropriate option in the **Evaluation Wizard**. Here we'll give you the recommendations on filling the **Request extended evaluation** form `Pic 1`.
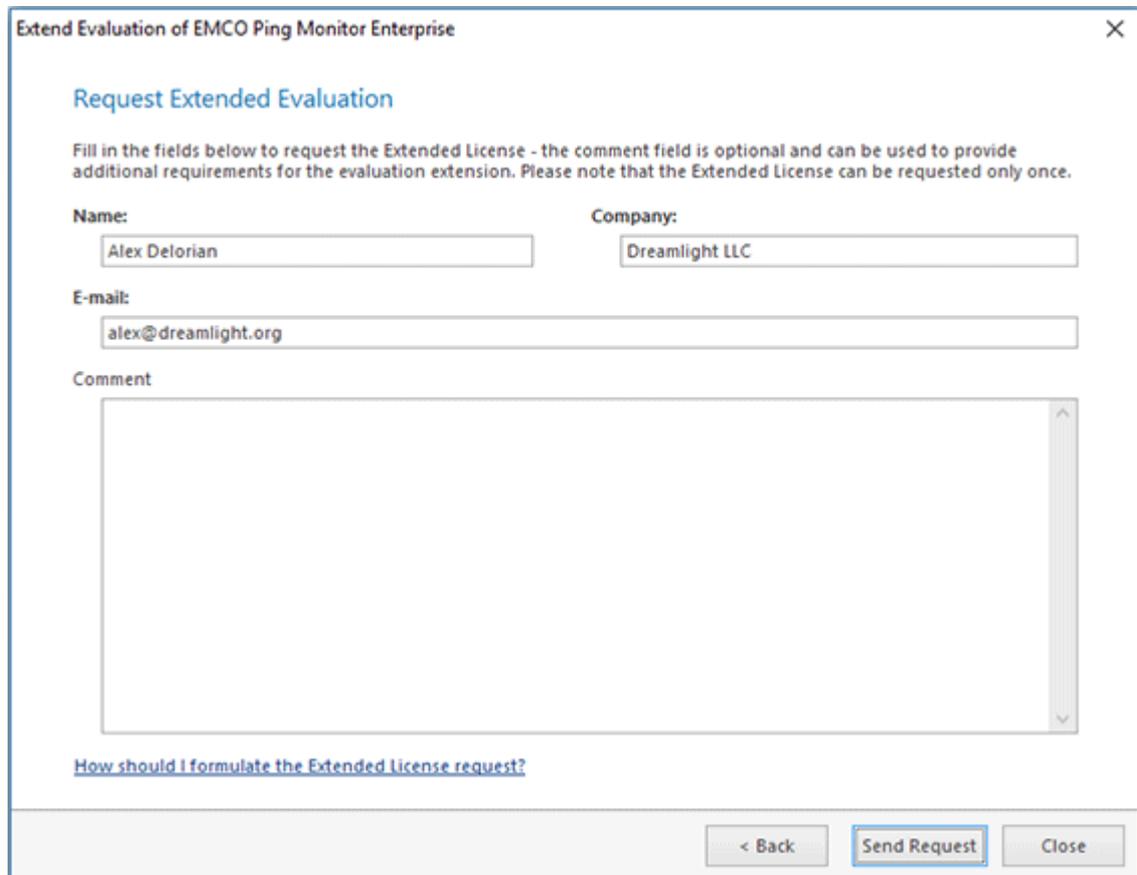
Pic 1. The Request Extended Evaluation form

In the **Request extended evaluation** form you should obligatory specify your name in the **Name** field, company name in the **Company** field and your e-mail address in the **E-mail** field.

> Though the **Comment** field is optional it is strongly recommended to use this field for providing EMCO Software with the reason of requesting the Extended License. Please notice that EMCO Software reserves the right to decline the request without providing a requester with any explanations.

If the extended license request is approved by EMCO Software experts you'll receive the License Code to the e-mail address specified.

Chapter 12: Program Updates

EMCO Software cares for versatile needs of the users of EMCO programs and fully understands their wish to have the most up-to-date software installed on there PCs. That is why we provide you with an easy update feature. You do not need to browse the Internet again and again to find out if any updates are available – Ping Monitor will do this work for you. Checking for updates can be performed both manually and automatically. This chapter describes the Live Update process for the current major version of the program and the Major Update feature which allows you to get a brand new version of Ping Monitor quickly and easily.

Live Update

Ping Monitor can be easily updated with just a few clicks. The update process is performed via an Internet connection using preconfigured proxy settings.

Check for Updates

The **Check for Updates** button from the **Update** Ribbon group should be used to check for new versions of Ping Monitor.

Ping Monitor can check for updates automatically. You can configure the program behavior regarding the automatic check for updates on the **General Settings** preference page.

To check for updates, click the **Check for Updates** button from the **Application Menu** or from the **Update** group of the **Program** Ribbon page. Ping Monitor will check if any updates are available and if so, the **Live Update Wizard** Pic 1 will appear on the screen.
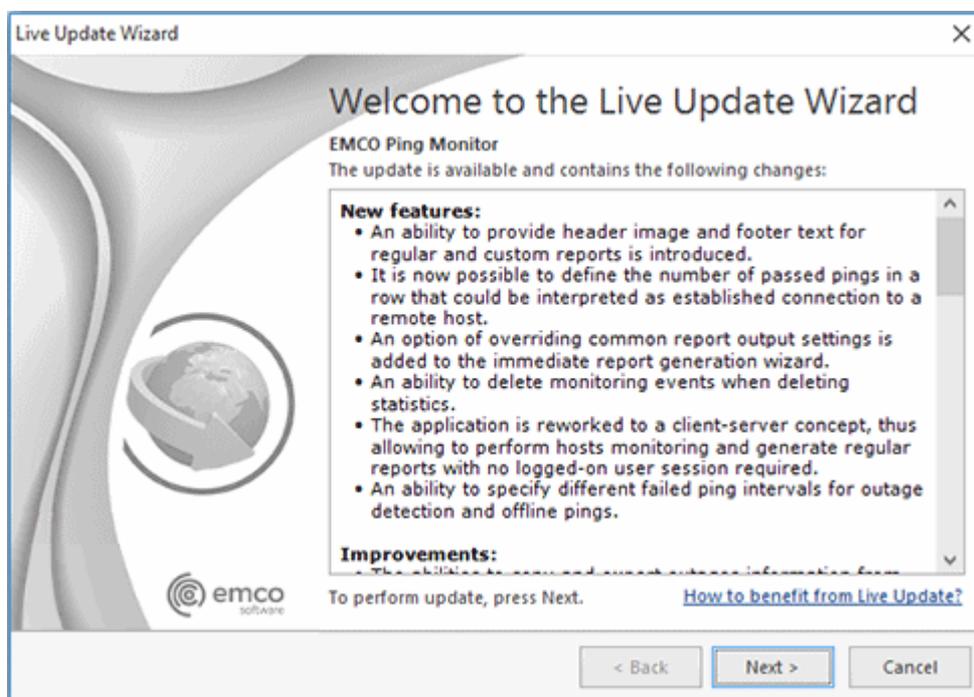
Pic 1. The Live Update Wizard welcome page

The **Live Update Wizard** will introduce you to the changes made in the newer version and guide you through the whole updating process while showing the detailed download progress. When the download is finished, the program will be restarted to perform the actual update.

Major Update

Along with the **Live Update** feature, Ping Monitor comes with a built-in function of automatic checking for Major Updates. The Major Update is an update to a brand-new version of Ping Monitor that includes a number of significant changes.

You can install this version alongside the version you are using now. It will import the settings and data from your current version, so that you won't need to configure the new version in the same way you configured the one you are using at the moment. Such parallel installation allows you to inspect the new version and compare it with the previous one in your environment with your data and settings.

> ℹ️ The Major Update is installed alongside the version you currently use. The existing version is not automatically uninstalled from your PC, and you can continue using the program version you are accustomed to while having a look at the brand new one.

If the program detects availability of a Major Update, the **Major Update Wizard** `Pic 1` will appear on the screen.
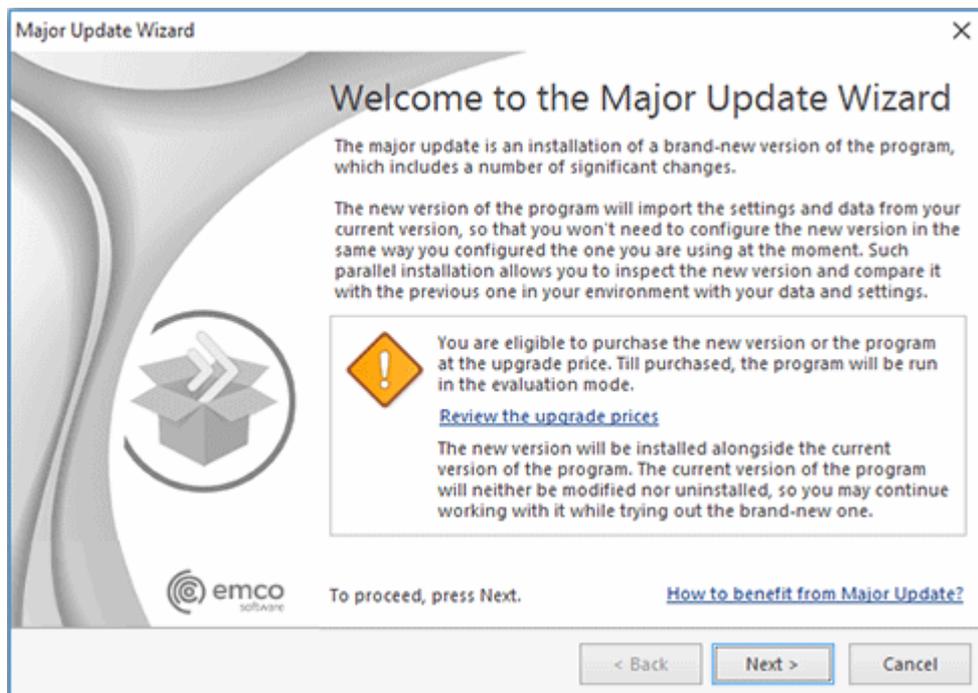
Pic 1. The Major Update Wizard welcome page

The **Major Update Wizard** will introduce you to the features available in the brand new version of Ping Monitor and guide you through the update process. The message displayed at the bottom of the welcome page will let you know if the current License allows you to install and use the Major Update for free. When the download is finished, the new version installation will be run automatically.

Chapter 13: Main Program Actions

The main program actions are all gathered on the **Ribbon** bar and are grouped by the functions performed into pages. There are static pages, that are always displayed, and categories, containing contextual pages, that are displayed only when a specific context is active. As for the static pages, they are the following: **Home**, **View** and **Program**. These static pages are filled up with the pages available in the **Hosts Tools**, **Alerts Tools Category**, **Reporting Tools** and **Publishing Tools** categories.

This chapter is to describe the actions available on all the pages and can be used as a glossary while working with Ping Monitor.

Home Ribbon Page

The **Home** Ribbon page contains all main actions related to the primary features of Ping Monitor. This chapter will describe each group and the actions available in it for the **Home** page.

Activity Ribbon Group

The **Activity** Ribbon group is used to control the monitoring process activity. The glyph of this group is used to open the **Monitor Settings** preference page.

Start	**Start** The **Start** button allows you to start monitoring for the currently selected hosts.
Stop	**Stop** The **Stop** button allows you to stop monitoring for the currently selected hosts.
Pause	**Pause** The **Pause** button allows you to pause monitoring for the currently selected hosts.
Resume	**Resume** The **Resume** button can be used to resume monitoring for the currently selected hosts.

Statistics Ribbon Group

The **Statistics** Ribbon group is used to manage the stored monitoring data.

Delete Statistics	**Delete Statistics** The **Delete Statistics** button should be used to delete all monitoring data for the selected hosts.

Reporting Ribbon Group

The **Reporting** Ribbon group allows you to create generic reports.

Generate Report	**Generate Report** The **Generate** Report button should be used to generate a performance and availability report for any period of time.

New Ribbon Group

The **New** Ribbon group contains the actions for creating new business objects within Ping Monitor.

Host	**Host** The **Host** button should be used to add a new host or a range of hosts to be monitored.
Group	**Group** The **Group** button allows you to create a new hosts group.
Summary Report	**Summary Report** The **Summary** Report button should be used to create a new preconfigured report with the brief information on monitors performance and availability.
Detailed Report	**Detailed Report** The **Detailed** Report button should be used to create a new preconfigured report with the detailed information on monitors performance and availability.

Web Ribbon Group

The **Web** Ribbon group allows you to access the program's web interface.

Web Interface	**Web Interface** The **Web Interface** button can be used to open the EMCO Ping Monitor program web site in the default browser.

View Ribbon Page

The **View** Ribbon page is used to control the program representation, such as the currently applied skin, visible views and their layout.

Layout Ribbon Group

The **Layout** Ribbon group should be used for a workspace layout management.

Reset Workspace	**Reset Workspace** The **Reset Workspace** action should be used to restore the default windows', views' and dock panels' layout.

Show Ribbon Group

The **Show** Ribbon group should be used for managing the currently visible Ping Monitor views.

☑ Hosts	**Hosts** Shows or hides the **Hosts** view. The **Hosts** view is used to display and manage a set of hosts and groups in the program.
☑ Reports	**Reports** Shows or hides the **Reports** view. The **Reports** view shows a set of monitoring performance and availability reports based on historical data, which can be generated automatically on a regular basis.
☑ Log	**Log** Shows or hides the **Log** view. The **Log** view shows information on the events taking place during the program execution.
☑ Access Control	**Access Control** The **Access Control** view is used to define roles used to control access to the Ping Monitor server and assign those roles to users and groups.
☑ Operations	**Operations** Shows or hides the **Operations** view. The **Operations** view shows detailed progress of each operation currently performed and allows canceling some or all running operations.

Skins Ribbon Group

The **Skins** Ribbon group provides you with an option of quick changing of the program skins.

Skin Chooser	**Skin Chooser** The **Skin Chooser** is a drop-down button that should be used to select the skin from the available skins to be applied to the program. The currently active skin is the highlighted one.

Program Ribbon Page

The **Program** Ribbon page contains service actions that are not connected to the business area of the program.

Server Ribbon Group

The **Server** Ribbon group contains actions for reconnecting the client to another server and reviewing information on the server the client is currently connected to.

Switch Server	**Switch Server** The **Switch Server** button should be used to connect to another Ping Monitor server.
Server Info	**Server Info** The **Server Info** button allows you to review information on the server the client is currently connected to, including information on other connected clients.

Organize Ribbon Group

The **Organize** Ribbon group contains the actions to be used for managing objects.

Import	**Import** The **Import** button should be used to import objects to Ping Monitor from a file.
Export	**Export** The **Export** button should be used to export objects from the currently focused view in Ping Monitor to a file.
Edit	**Edit** The **Edit** button allows you to edit the object selected in the currently focused view.
Delete	**Delete** The **Delete** button is used to delete the selected objects from the currently focused view in Ping Monitor.

Clipboard Ribbon Group

The **Clipboard** Ribbon group contains the actions to copy/move objects to the clipboard and paste data from the clipboard.

Paste	**Paste** The **Paste** button should be used to add the objects that are currently available from the clipboard to a selected location in the currently focused view.

Cut

The **Cut** button should be used to put the selected objects from the currently focused view to the clipboard and remove them from the source after pasting them to the destination.

Copy

The **Copy** button allows you to put the selected objects from the currently focused view to the clipboard to be copied to the destination when pasting.

Update Ribbon Group

The **Update** Ribbon group is responsible for the product updates function. The glyph of this group opens the **General Settings** preference page enabling you to configure the auto-update options.

Check for Updates

The **Check for Updates** button should be used to check for new versions of Ping Monitor.

Feedback Ribbon Group

You can use the **Feedback** Ribbon group to send EMCO Software a request for a new feature you are missing in Ping Monitor or to report on problems you faced while working with the program.

Suggest a Feature

The **Suggest a Feature** button should be used to suggest a functionality you would like to see in the next versions of Ping Monitor.

Report a Problem

The **Report a Problem** button should be used for reporting the problem you faced while working with Ping Monitor.

Information Ribbon Group

The **Information** Ribbon group has a range of useful actions to manage licensing issues, get help or information you may require.

Manage License

The **Manage License** action should be used to review the current licensing state and choose from different product licensing options.

Buy Now

The **Buy Now** button is only visible if Ping Monitor is not activated. It provides you with a quick access to the EMCO web store.

Edition Upgrade	**Edition Upgrade** The **Edition Upgrade** provides you with an ability of benefiting from update to a more comprehensive edition of Ping Monitor with a help of the **Edition Upgrade Wizard** that will help you choose an appropriate edition and purchase a license for using it.
Contact Support	**Contact Support** The **Contact Support** button should be used to get efficient technical assistance from EMCO Software support team.
EMCO on the Web	**EMCO on the Web** The **EMCO on the Web** button provides you with a short-cut to the EMCO website.
About	**About** It opens the **About** dialog to review the Ping Monitor information, licensing information and the End-User License Agreement.

Hosts Tools Category

The **Hosts Tools** Ribbon category is displayed when the **Hosts** view is active and contains the **Hosts** page with actions for monitoring activity and data management.

Hosts Contextual Ribbon Page

The **Hosts** contextual Ribbon page from the **Hosts Tools** category contains the actions for hosts and groups management.

New Ribbon Group

The **New** Ribbon group allows you to create hosts and groups of hosts.

Host	**Host** The **Host** button should be used to add a new host or a range of hosts to be monitored.
Group	**Group** The **Group** button allows you to create a new hosts group.

Auto-start Ribbon Group

The **Auto-start** Ribbon group can be used to include and exclude hosts to and from the auto-start list.

	Include
	The **Include** button should be used to add the selected hosts to the auto-start list.
	Exclude
	The **Exclude** button should be used to remove the selected hosts from the auto-start list.

Alerts Tools Category

The **Alerts Tools** Ribbon category is displayed when alerts summary or alerts details are active and contains the **Alerts** page with actions for alerts management.

Alerts Contextual Ribbon Page

The **Alerts** contextual Ribbon page from the **Alerts Tools** category contains the actions for alerts management.

State Ribbon Group

The **State** Ribbon group allows you to acknowledge alerts.

	Acknowledge
	The **Acknowledge** menu can be used to acknowledge a currently selected alert. Select a time period to acknowledge an alert – from 5 min to 1 day, or set a custom period. You can also acknowledge an alert permanently.

Severity Ribbon Group

The **Severity** Ribbon group can be used to set severity for a currently selected alert.

	Set Critical
	The **Set Critical** button should be used to set the critical severity for a selected alert.
	Set Major
	The Set Major button should be used to set the major severity for a selected alert.
	Set Minor
	The Set Minor button should be used to set the minor severity for a selected alert.

Reporting Tools Category

The **Reporting Tools** Ribbon category is displayed when the **Reports** view is active and contains the **Reporting** page with actions for working with preconfigured reports.

Reporting Contextual Ribbon Page

The **Reporting** contextual Ribbon page from the **Reporting Tools** category contains the actions for working with preconfigured reports.

New Ribbon Group

The **New** Ribbon group contains the actions for creating new preconfigured reports.

Summary Report	**Summary Report** The **Summary Report** button should be used to create a new preconfigured report with the brief information on monitors performance and availability.
Detailed Report	**Detailed Report** The **Detailed Report** button should be used to create a new preconfigured report with the detailed information on monitors performance and availability.

Reports Ribbon Group

The **Reports** Ribbon group contains the actions for working with already created predefined reports.

Generate	**Generate** The **Generate** button should be used to manually generate the selected preconfigured report.
Enable	**Enable** The **Enable** button allows you to turn on an ability of generating the selected reports.
Disable	**Disable** The **Disable** button allows you to turn off an ability of generating the selected reports.
Open Storage	**Open Storage** The **Open Storage** button should be used to open the local storage for the report the feature of storing the output locally is enabled for.

Publishing Tools Category

The **Publishing Tools** Ribbon category is displayed when the **Details** view is active and contains the **Publishing** page with actions for saving displayed content to different file formats and printing it.

Publishing Contextual Ribbon Page

The **Publishing** contextual Ribbon page from the **Publishing Tools** category contains the actions for saving displayed content to different file formats and printing it.

Report As Ribbon Group

The **Report As** Ribbon group contains the actions for saving displayed content to different file formats.

Adobe PDF File	**Adobe PDF File** The **Adobe PDF File** button should be used to export the displayed data to the portable document format.
HTML Web Page	**HTML Web Page** The **HTML Web Page** button should be used to export the displayed data to the HTML format.
MIME HTML Document	**MIME HTML Document** The **MIME HTML Document** button should be used to export the displayed data to the MIME HTML format.

Chapter 14: Ping Monitor Client-Server Concept

Ping Monitor is shipped as a client-server application, thus allowing to perform hosts monitoring and generate regular reports with no logged-on user session required. The server part is represented with the **Ping Monitor Server 9** Windows service, and the client part is the program that is running in a user session.

> The program allows multiple clients to connect to the server and work simultaneously with the same data. The number of connections depends on the used license. The Free edition of the program allows one connection only, the Professional edition allows two simultaneous connections, and the Enterprise edition doesn't limit the number of simultaneous connections.
>
> The Enterprise edition of the program allows connecting to servers running on the local or remote computers. The Professional and Free editions can connect to a server running on the same computer only.

By default, the service is configured to start together with the underlying operating system, thus allowing you to start monitoring as soon as the hosting PC is up and running provided that the corresponding automation option is enabled (it is enabled initially). When you launch the client program, it prompts you to choose if the server to connect to is located on the local or remote PC `Pic 1`.
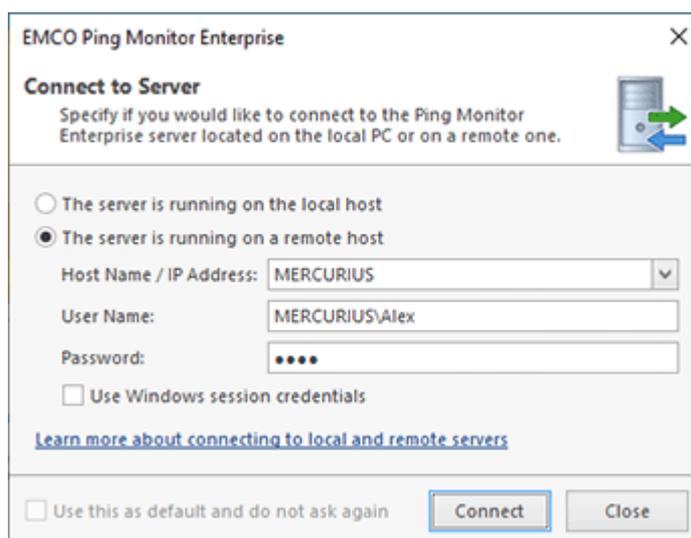
Pic 1. Choosing the server to connect to

For the server to accept remote connections, the following ports should be opened in the firewall for inbound TCP connections:

- **48019** – this port is used to connect to the remote server using the Windows session credentials;

- **48020** – this port is used to connect to the remote server via a SSL channel using the specified credentials.

> If you would like to use custom ports, you can define the required ports in the following key of the Windows Registry on the PC hosting the Ping Monitor server:
> *HKEY_LOCAL_MACHINE\SOFTWARE\EMCO\Ping Monitor\v9*

To override the port used for connection by using the Windows session credentials, you should specify it in the **Port** DWORD value. The **SSLPort** DWORD value should be defined to override the port used for connection via a SSL channel using the specified credentials. For the client to be able to connect to the server via a custom port, you should define this port in the server name, e.g. *emco-server.local:3112*.

After the connection is established, the client allows you to manage the monitoring process, the hosts and the reports if you account is authorized accordingly by the server access control configuration. You can disconnect from the current server and connect to another one at any time using the **Switch Server** button from the **Application Menu** or from the **Server** Ribbon group on the **Program** page.

When connecting to a remote server, you can choose if you would like to use the credentials of the Windows session the client program is executed in or to provide other credentials. When the current session credentials are used, all aspects of the Windows integrated security are applied to the client-server communication. Otherwise, when the credentials are provided manually, the transport layer of communication is secured with a SSL certificate provided by the server. By default, the self-signed certificate issued to **<%SHORT_NAME%>Server.exe** is used. It is not fully trusted, because the DNS match and the trusted root conditions are not met. Although it is possible to accept this certificate for communication, it is strongly recommended that you use the certificate issued to your server. It can be either your self-signed certificate issued by a certification authority trusted in your organization or the certificate issued to the server by one of the commonly known certification authorities. The certificate to be used by the server for authentication is selected on the **Server Configuration** page of the program preferences.

In the **Server** group, you can also find the **Server Info** button. When this button is pressed, a dialog is displayed containing information on the server and all the clients currently connected to it. Upon exiting the program, the client is disconnected from the server application that keeps running on the server PC.

In case the currently installed client is not compatible with the server you are connecting to, the program will prompt you that a compatible client needs to be installed, if it is not installed yet, otherwise the compatible client is automatically launched and connected to the specified server.

Chapter 15: Access Control

Ping Monitor server supports concurrent access by multiple users. Each user is authenticated by its Windows credentials, but for an enterprise solution it is not enough to authorize access since each action should also be authorized for specific users only so that a simple user cannot perform administrative tasks. In Ping Monitor the server access is controlled by means of roles.

The roles management is available only when running the Enterprise edition of Ping Monitor. With the Free and Professional editions, all users that are allowed to access the machine the Ping Monitor service is running on are granted administrative access to the program.

Each role defines a set of enabled privileges. There are three predefined user roles, which are **Administrator**, **Read-Only** and **No Access**. The **Administrator** role is used to grant users an unlimited access to the server. The **Read-Only** role allows the users in that role to access the server but does not allow performing any modifications to the server data and configuration. The **No Access** role should be used to disallow access for specific users that belong to the groups for which access is granted. In addition to these predefined roles, you can create custom roles enabling required privileges for those roles.

The roles may be assigned to users and groups thus granting or disabling access to Ping Monitor features for specific users. By default, users that are members of the built-in administrator groups on the PC hosting the server are assigned the **Administrator** role. Other users are not allowed to connect to the server.

It is possible to grant users administrative access without applying the **Administrator** role to them by adding those users to the **Ping Monitor Administrators** Windows group. This option can be used by the server administrator to get protected from losing the administrative role due to mistakes in roles configuration or manipulations performed by other administrators. Note that you need to re-authenticate your credentials (which typically means that you need to re-login) when adding a new group or changing group members.

The roles are managed and assigned within the **Access Control** view. To assign roles to users and/or groups, use the **Assign Permissions** button in the **Permissions** part of the **Access Control** view. A dialog will be opened where you can add a set of principals and choose a role for each one Pic 1 .
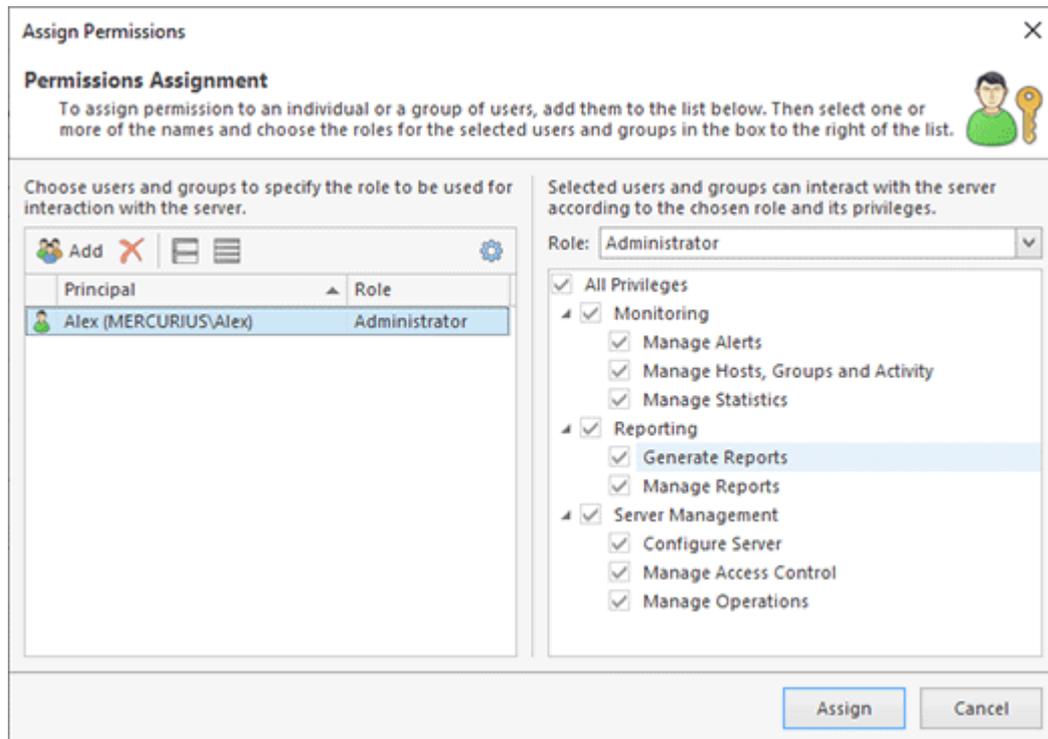
Pic 1. Permissions assignment

The assignment process is fast and easy. All you need is adding a list of principals for which you would like to assign roles in the table then selecting a role for each one on the right of the table. You may select multiple principals and assign them the same role. For each role, you can review the set of enabled privileges. To proceed with assignment, press the **Assign** button.

To assign another role to any principal, select it in the **Access Control** view and click the **Edit** button. Alternatively, you can use the corresponding item in the pop-up menu. A dialog will be opened where you can choose a new role for the selected user or group. To delete role assignments, use the **Delete** buttons and menu item.

To create a custom role, use the **Add** button in the **Roles** part of the **Access Control** view. A dialog will be opened where you can specify a name for the role to be created and a set of privileges to be granted to users in this role `Pic 2`.
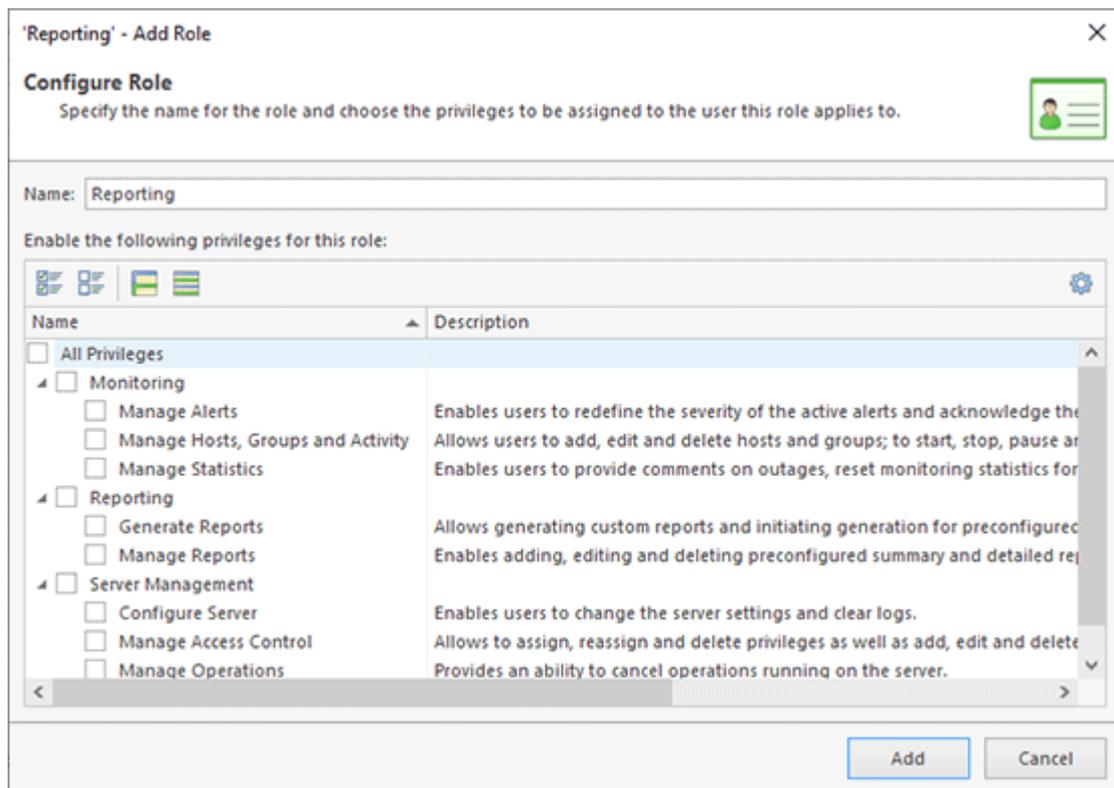
Pic 2. Creating a user-defined role

You can use the **Edit** button and menu item to change the role in the future. As during creation, it is possible to specify the role name and a set of privileges. To delete specific user-defined roles - if they are no longer required - use the **Delete** button and menu item. If the role is assigned to principals, you are prompted to decide during the deletion process whether you would like to delete the assignment altogether or reassign another role to those principals.

Chapter 16: Optimizing System Performance

Ping Monitor is designed to monitor a large number of hosts simultaneously, but the monitoring performance depends on multiple factors. The main factors are the number of monitored hosts, the monitoring settings and the hardware of the machine where the Ping Monitor server runs. When starting the program for the first time, you may indicate the estimated number of hosts to be monitored, so that the program can automatically configure the appropriate monitoring settings.

By installing the Ping Monitor server on a modern computer that satisfies hardware requirements listed below, it is possible to monitor 8,000+ hosts. The program has a technical limit of 32,000 hosts that can be monitored by one server. The practical limit depends on the used hardware configuration. You can use the following recommendations to configure hardware on the Ping Monitor server.

Hardware Requirements

Processor

- A single-core processor on the server allows monitoring up to 1000 hosts.

- Using a multi-core processor each core allows monitoring 4000 hosts. For example, using a 2-core processor, you can monitor 8000 hosts.

Memory

Depending on the amount of RAM installed, you will be able to monitor up to:

- 500 hosts per 1 GB if you have no more than 4 GB of RAM

- 1000 hosts per 1 GB if you have more than 4 GB, but no more than 8 GB of RAM

- 2000 hosts per 1 GB if you have more than 8 GB of RAM

For example, to monitor 2000 hosts the server requires at least 4 GB of memory. To monitor 8000 hosts the server needs at least 8 GB of memory installed.

Disk Usage Estimation

The program uses a database to store the collected data. Using the default settings, the program stores data in the file-based SQLite database. If you plan to monitor more than 1000 hosts during a long time, it's recommended to use a SQL Server database to improve the data storage performance. You can switch the database type on the **Program Database** page of the program preferences.

The program stores hosts statistics, raw ping reply data and all registered events for each host. With the default monitoring settings, it takes about **2.5 MB per host per month** (0.2 MB for storing statistics and 2.3 MB for storing raw ping reply data), so make sure you have enough free space to store this data. The SQLite database is stored on the file system of the server, so make sure the hard drive space is sufficient to store the collected data.

To optimize the disk usage over time, the program may delete old data for each host automatically. You can configure the program to automatically clean up old data on the **Monitoring Statistics** page of the program preferences.

> To save the disk space, the program skips storing the raw ping reply data by default if you monitor over 5000 hosts. You can configure the program to store raw ping reply data on the **Monitoring Statistics** page of the program preferences. Make sure you have sufficient free space available to store the data.

Tuning the Monitoring Settings

The program pings every monitored host regularly at a configured time interval, as explained in the **How the Program Works** chapter. If you monitor thousands of hosts at short intervals, it can cause a large CPU and network workload on the server. To prevent that, the program sets appropriate monitoring intervals at the first start of the program depending on the estimated number of hosts. You can change those settings later on the **Monitoring Settings** page of the program preferences.

> If you plan to monitor a very big number of hosts, you need to avoid using short intervals to prevent a high system workload. The server tunes the intervals automatically depending on the current system workload and increases them, if required, to guarantee the monitoring system responsiveness. The server changes the intervals to the nominal values automatically when the system workload goes down. It's recommended to use 10-sec. monitoring intervals if you plan to monitor over 500 hosts and 30-sec. intervals if you plan to monitor over 1000 hosts, otherwise the server may change them automatically to prevent a high system workload.

Other Performance Optimization Recommendations

When you monitor a large number of hosts (i.e. over 1000 hosts), the program GUI client can use the system CPU and memory quite intensively. In this case, it's recommended to run the Ping Monitor server and GUI client on different machines to reduce the system workload. Parallel GUI client connections also influence the server performance, so you have to reduce the number of parallel connections to the server if it runs out of resources.

Chapter 17: Notification Center

The **Notification Center** is used to notify users about possible configuration problems, available program updates, etc. As soon as notifications arrive, you are able to see a balloon icon in the status bar together with the number of available notifications. When you click on this element, the notifications are displayed in a flyout window on the right of the main program window Pic 1.
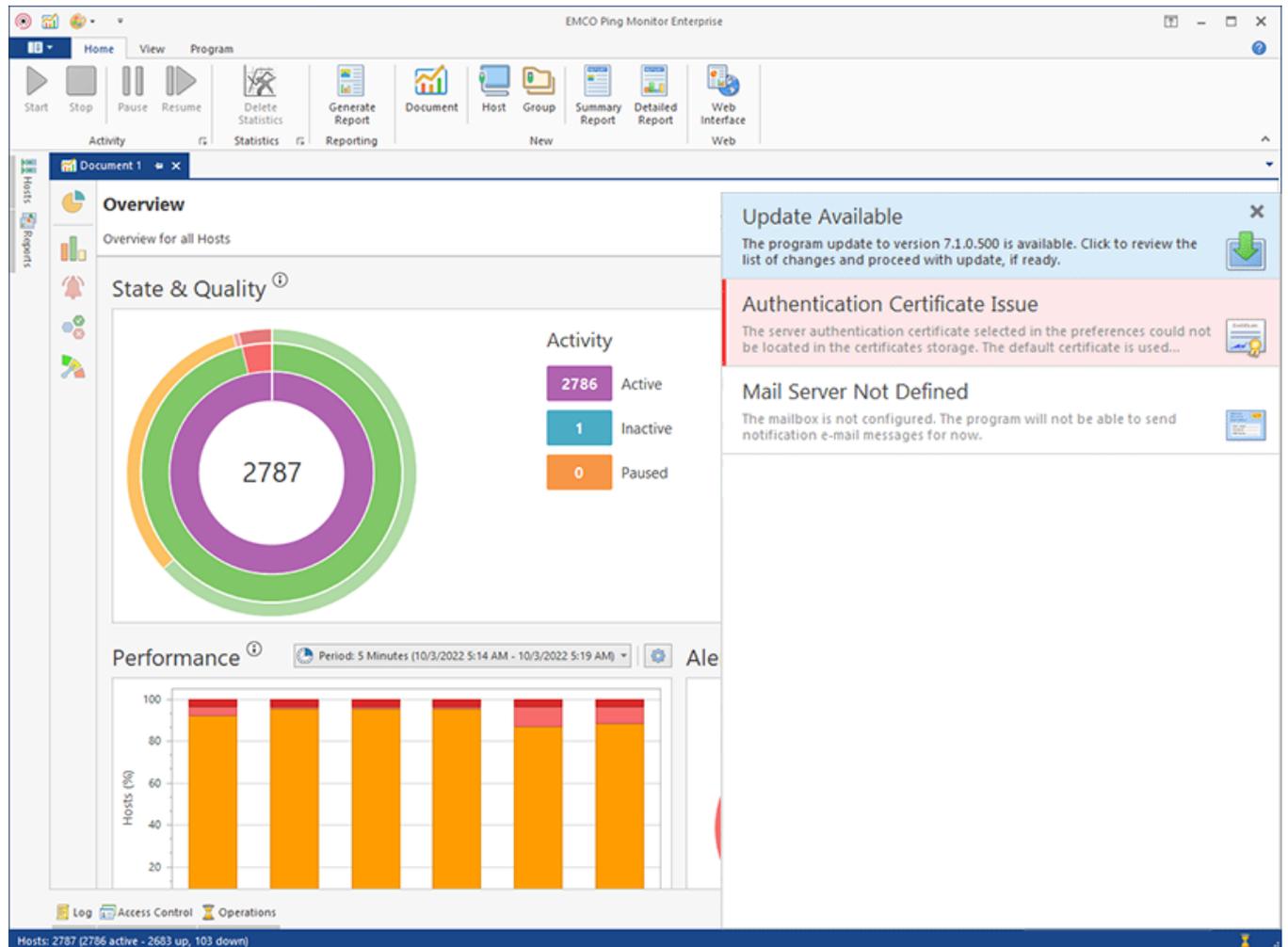
Pic 1. Displayed notifications

When you click on the notification, you are proposed to perform the action requested by the notification. For example, in case of the configuration issue, the preferences dialog is displayed on the appropriate page, allowing you to fix the issue, and in case of the available update, the update wizard is displayed.

If the notification is about any kind of a critical issue, it is highlighted red and it is not possible to ignore it. For other notifications, you can close each and every one using the cross button in the right top corner of the notification row. As the notification is closed, it won't be displayed again until the condition for displaying it is reached once again.

Chapter 18: Requirements

Please carefully read and follow all requirements, listed here, or you may not be able to successfully use the product. You can contact our support if you experience a problem during the product use.

System Requirements

Computer running Ping Monitor must meet the following requirements:

Minimum Hardware Requirements

- Intel Core iX Processor or equivalent
- 4 GB of RAM
- 2 GB of free disk space

Recommended Hardware Requirements

- 6th Gen Intel Core iX Processor or equivalent
- 8 GB of RAM
- 10 GB of free disk space

Supported Platforms (x86/x64)

- Windows 11, 10, 8.1, 8, 7 (with SP1 or later)
- Windows Server 2022, 2019, 2016, 2012 R2, 2012, 2008 R2 (with SP1 or later)

Requirements

- Administrative rights on the local computer
- Microsoft .NET Framework 4.5.2 or above
- TCP ports opened: 48019, 48020

Chapter 19: Edition Upgrade

The program has multiple editions with different features, so you can select the one that suits your needs.

Edition Upgrade	**Edition Upgrade** The **Edition Upgrade** provides you with an ability of benefiting from update to a more comprehensive edition of Ping Monitor with a help of the **Edition Upgrade Wizard** that will help you choose an appropriate edition and purchase a license for using it.

The **Edition Upgrade Wizard** `Pic 1` was designed to make the upgrade process easier. This wizard can be reached by clicking an appropriate hyper link in the **About** dialog or by using the **Edition Upgrade** button from the **Program** Ribbon page.
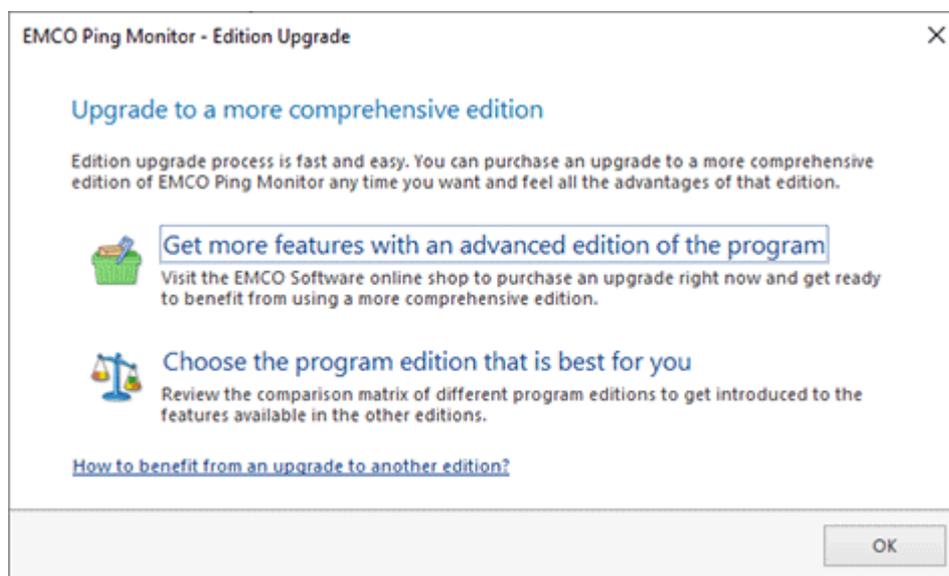

Pic 1. The Edition Upgrade Wizard

With a help of the **Edition Upgrade Wizard**, you can purchase an upgrade to more comprehensive edition of Ping Monitor with a single click on the **Get more features with an advanced edition of the program** option or introduce yourself to the features available in the other edition of the program using the **Choose the program edition that is best for you** option. This option will open a feature list web page that shows you the detailed comparison matrix of the features available in different Ping Monitor editions so that you can review all the features of each edition before choosing the one that best fits your needs.
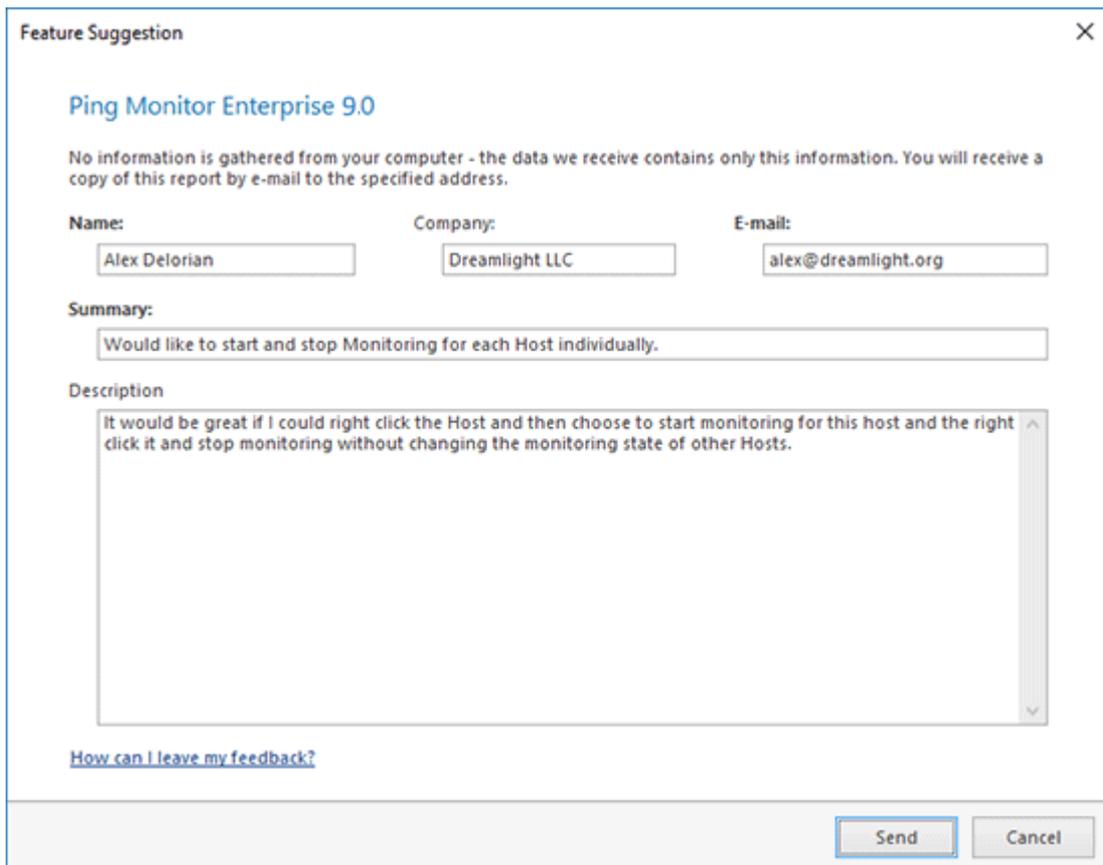
Chapter 20: How can I leave my Feedback?

EMCO Software always takes care of its customers, and your opinion means a lot to us. For this reason, our programs have built-in features for your feedback. You can suggest a feature you want to see in new program versions or report a technical problem you have faced using the program. Specifying your contact information on the feedback forms ensures that you will be informed of any changes with regard to the reported issue, our plans for implementing the suggested feature or fixing the reported bug. Those actions can be found in the **Feedback** Ribbon group of the Program page.
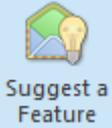
Suggest a Feature	**Suggest a Feature** The **Suggest a Feature** button from the **Feedback** Ribbon group should be used to suggest a functionality you would like to see in the next versions of Ping Monitor.

Ping Monitor comes with a wide range of features, but if you feel some functionality is missing, you can always suggest a new feature to us that you want to see in the program. To suggest a new feature, you should press the **Suggest a Feature** button from the **Feedback** Ribbon group. After pressing this button, you will see the **Feature Suggestion** dialog `Pic 1` on the screen where you are offered to enter your contact information and describe your suggestion.


Pic 1. The feature suggestion form

Press **Send** when you are done with filling out the form to send your suggestion.

Report a Problem

The **Report a Problem** button should be used to report a problem you have faced while working with Ping Monitor.

Ping Monitor is easy to use and very stable. Nevertheless, if you have faced any difficulty or problem while working with it, you can send us a problem report. To send such a report, you should press the **Report a Problem** button from the **Feedback** Ribbon group. When this button is pressed, the **Problem Report** dialog `Pic 2` will appear on the screen where you are offered to enter your contact information and describe your problem.
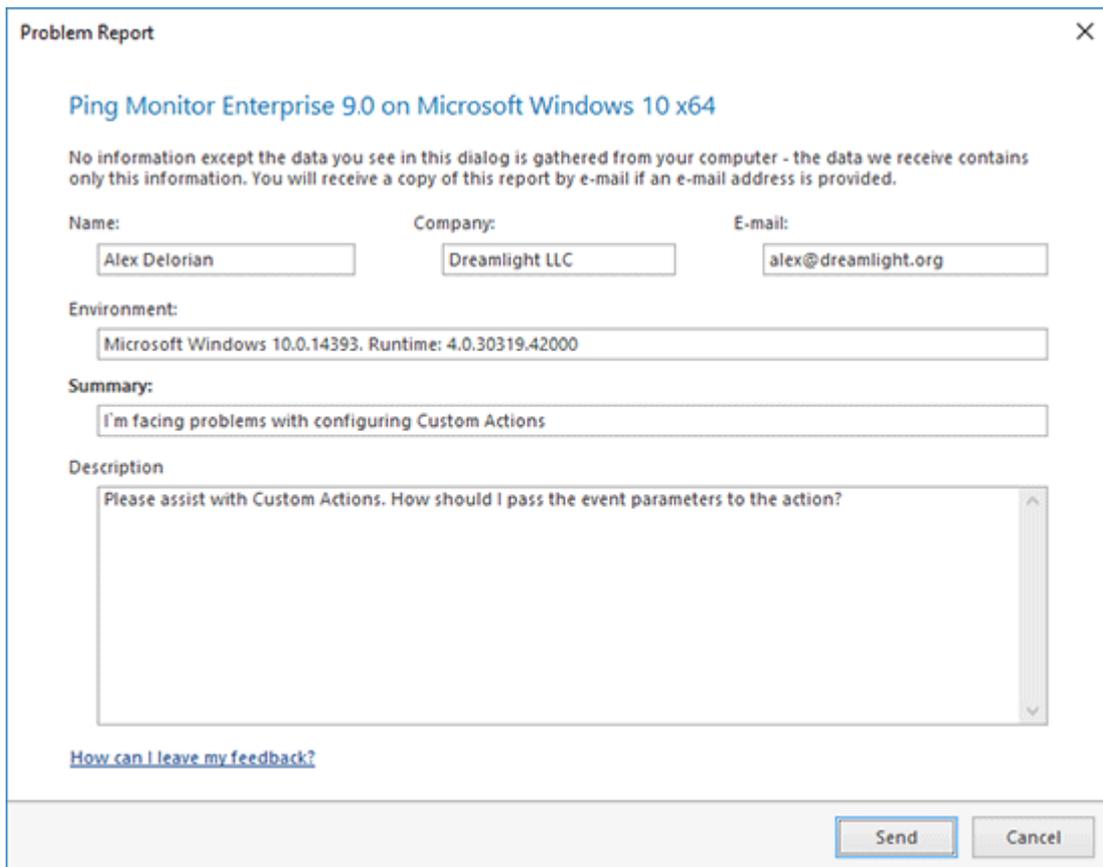
Pic 2. The problem report form

In the **Environment** field, you can provide us with a description of the specific environment used while working with the program. Press **Send** when you are done with filling out the form to send your report.

Do not hesitate to contact EMCO Software - we are always glad to receive your feedback and are doing our best to satisfy our customers' preferences.

Chapter 21: About EMCO Software

EMCO creates mission-critical software to manage network computers remotely and automate network administration.

Our company was founded in 2001 in Reykjavik, Iceland. Managing Windows networks as network administrators, we could not find tools that would help us automate our routine network administration tasks, so we decided to create such tools for fellow administrators and ourselves.

Today we offer innovative software that help IT specialists and network administrators to automate their Windows network management tasks. Our software tools are focused on remote management of Windows computers across networks and allow administrators to perform routine tasks on all managed computers with a few mouse clicks. We automate software audit and deployment, power management, hosts monitoring and other computer administration tasks.

Learn more: https://emcosoftware.com.

Our Customers

Being suitable for managing networks of any size, our products cater to the needs of 25,000+ customers in 85 countries around the globe. They are Fortune 100 corporations and small businesses, as well as governments, military institutions, universities, public schools, libraries and charities.

Our customers rely on EMCO products for managing their mission-critical network infrastructure. Using our products, network administrators monitor, audit, deploy and manage 3,000,000+ network devices every day.

Chapter 22: Contact Information

We would be glad to help you with any questions and problems you might have. Use the contact information below.

Contact Sales	Contact Support
Our sales team is standing by to answer your questions about purchasing or licensing EMCO products. Submit a request, send us an e-mail or call us: Contact Sales.	Our support team is here to help you with any technical product-related issues you may have. We provide free technical support for all our products, including freeware. Submit a request or send us an e-mail: Contact Support.