



Service Protector User's Manual

Version 10.5

1.	Introduction	2
2.	Key Features & Benefits	4
3.	System Requirements	5
4.	Using Service Protector	6
4.1.	The Main Window	6
4.2.	The Menu	8
4.3.	The Toolbar	10
4.4.	The Task Tray Icon	11
4.5.	Adding a Protector	13
4.5.1.	The General Tab	14
4.5.2.	The Monitor Tab	16
4.5.3.	The Email Tab	18
4.5.4.	The Extras Tab	22
4.6.	Editing Protector Settings	24
4.7.	Starting a Protector	26
4.8.	Stopping a Protector	26
4.9.	Removing a Protector	26
4.10.	Reporting on a Service's Activities	27
4.11.	Exporting a Protector to a File (XML)	28
4.12.	Exporting all Protectors to a Directory	28
4.13.	Importing a Protector from a File (XML)	28
4.14.	Adding a Copy of a Protector	29
5.	Licensing & Registration	30
6.	Troubleshooting and Reporting Problems	32
7.	Appendix I: The Sanity Check Feature	33
7.1.	Check that a drive is mapped	34
7.2.	Check that a file was recently updated	36
7.3.	Check that a network server is accepting connections	38
7.4.	Check that a web server is responding properly	40
7.5.	Check that an application is running	42
7.6.	Check that your service has open network connections	44
7.7.	Check for one or more adverse Windows events	46
7.8.	Check your service with a custom program/script	48
7.8.1.	Special Command Line Variables	50
8.	Appendix II: Working from the Command Line	51
8.1.	Importing a Protector	51
8.2.	Exporting a Protector	51
8.3.	Starting & Stopping a Protector	52

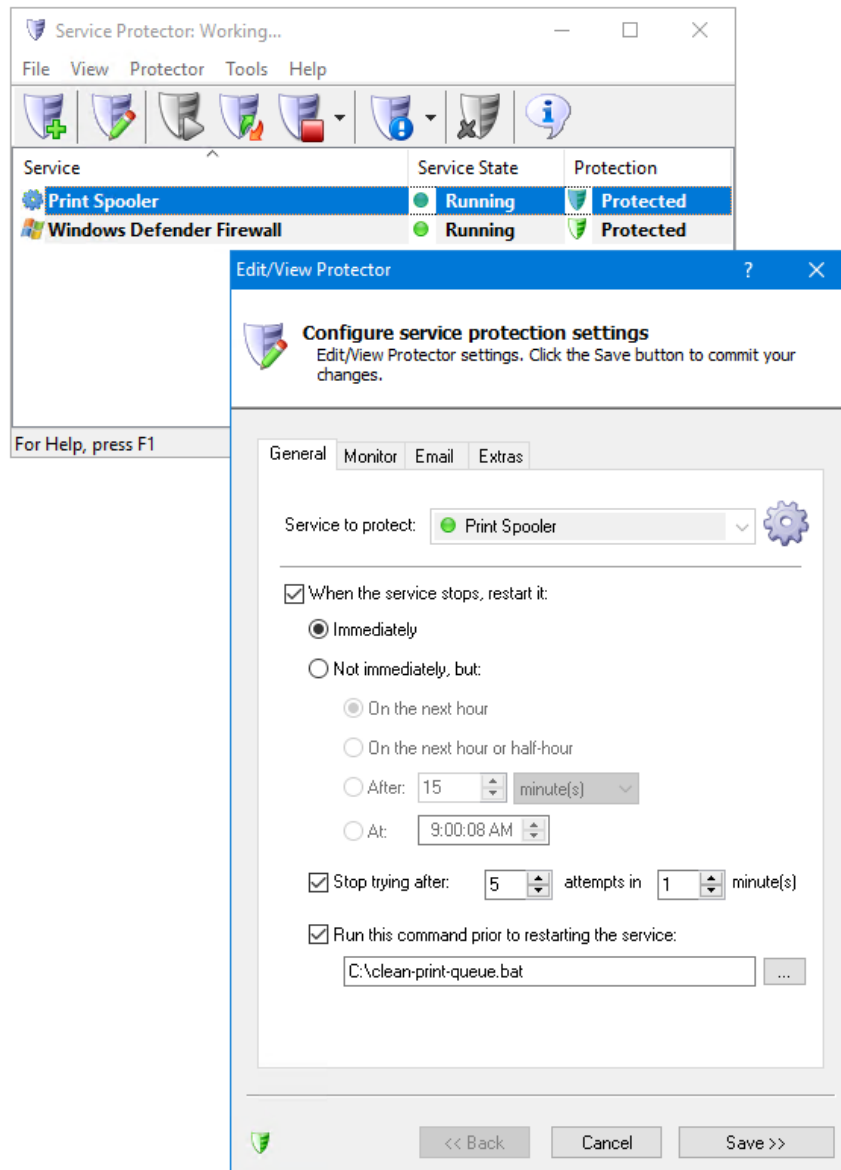
1. Introduction

Service Protector monitors your mission-critical Windows Services and keeps them running 24/7.

This manual describes how to use the Service Protector Graphical User Interface (GUI), which is responsible for adding and editing your service's protection settings. Note that once you have configured and started your service, the GUI is not necessary to monitor your running service.

Find out more about Service Protector at its web site:

<https://www.CoreTechnologies.com/products/ServiceProtector>



2. Key Features & Benefits

- Monitors your service and restarts it whenever it fails
- Able to manage virtually any service with minimal configuration
- The intuitive GUI makes it easy to protect your service, but no GUI is necessary once your service protection has been configured.
- Able to detect and restart services that hang, hog the CPU or consume too much memory.
- Able to restart your service (or reboot the computer) at a scheduled time
- e-mails you with details of crashes, restarts and other problems
- Supports the integration of your own custom "sanity check" utilities, executed regularly to test if your service is functioning normally or not
- Automatically dismisses common "Application error" dialog boxes that prevent crashed services from fully exiting
- Automatically dismisses Debug dialog boxes and logs the dialog box text for subsequent review by developers -- thus facilitating the deployment of services in "Debug mode"
- Reports all activities to the Windows Event Log
- Works in all virtual environments (VMware, Virtual PC, etc.)
- Very efficient; demands minimal CPU & memory resources
- No programming required!

But perhaps most important of all, Service Protector was designed and implemented by senior software engineers with over 25 years of real-world experience developing robust, mission-critical applications. Our software is of the highest quality, and we stand by it without reservation.

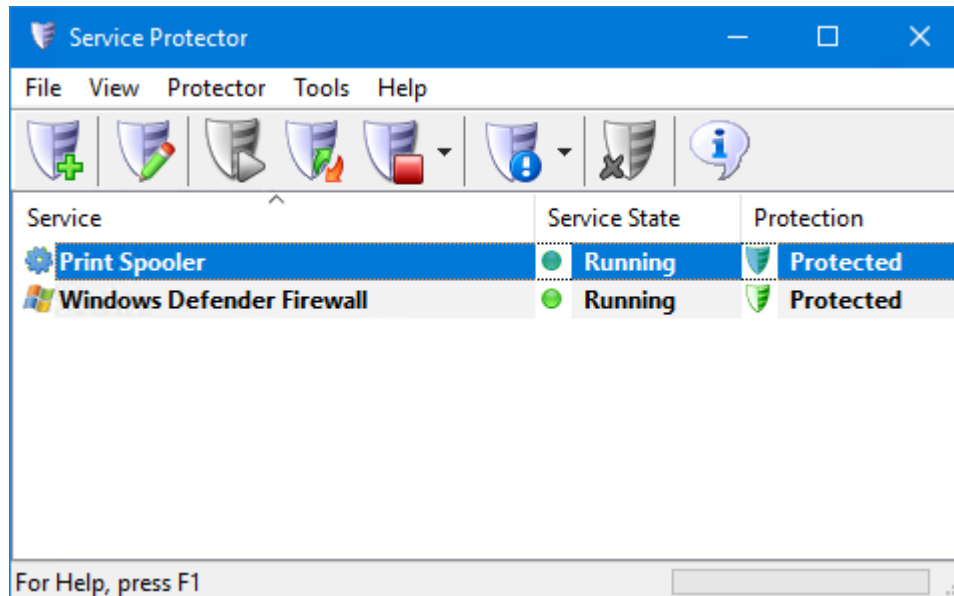
3. System Requirements

- Windows 11/10 or Windows Server 2025/2022/2019/2016 (x86 and x64 versions).
- 20 MB free hard drive space for installation files.

The Service Protector components that monitor your service are designed to be extremely frugal with machine resources. They almost always consume less than 1% of the CPU, less than 25 MB of RAM, and don't fall victim to the "Memory Growth" characteristic of many applications today.

4. Using Service Protector

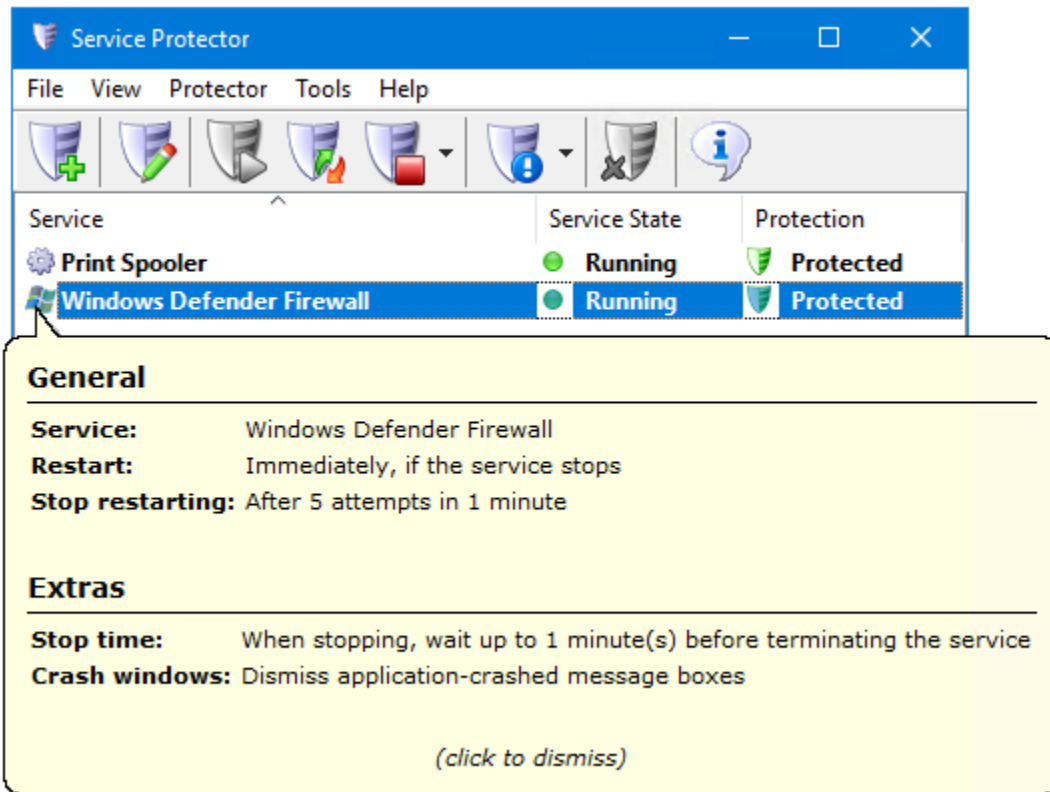
4.1. *The Main Window*



When started, Service Protector displays a list of the services it is protecting. The list will be empty when Service Protector is run for the first time. The above screenshot shows two services being protected, one per line. See [section 4.5](#) for adding a service to be protected.

Each entry in the list is called a **Protector**. A Protector protects a single service, that is, each service being protected is managed by a Protector.

Hovering over the first column in the list (the service's name) will pop up a convenient tooltip summarizing the Protector's settings:



Note that clicking on that icon/image will cause the tooltip to remain on screen instead of quickly going away.

4.2. The Menu

Service Protector's menu contains the following entries:

File

Exit	Exit Service Protector
-------------	------------------------

View

Toolbar	Toggle viewing of the button toolbar
Status Bar	Toggle viewing of the status bar
Large Icons	View the list of Protectors as large icons
Small Icons	View the list of Protectors as small icons
List	View the list of Protectors as a list of icons
Details	View the list of Protectors as a report with columns
Always On Top	Keep Service Protector on top of other windows
Hide When Minimized	Hide Service Protector when the minimize button is clicked
Refresh	Re-load the list of Protectors
Auto-refresh Every 5 seconds	Automatically re-load the list of Protectors every 5 seconds
Auto-refresh Every 10 seconds	Automatically re-load the list of Protectors every 10 seconds
Auto-refresh Every 30 seconds	Automatically re-load the list of Protectors every 30 seconds
Auto-refresh Disabled	Don't automatically re-load the list of Protectors

Protector

Add	Add a new Protector
Add Copy	Add a new Protector, but copy all settings from an existing Protector
Import	Adds a new Protector from a file
Export	Save the selected Protector to a file (in XML)
Export all	Save each Protector to a separate file (in XML)
Edit/View	Edit / View the settings of the selected Protector
Start	Start the selected Protector if it is not running
Stop	Stop the selected Protector if it is running
Restart	Restart the selected Protector if it is running
Start all	Start all Protectors
Stop all active	Stop all Protectors running/active
Restart all active	Restart all Protectors running/active
Remove	Remove the selected Protector. Note – does not remove the service!
Report Activity Today	Generate and launches a HTML report on the service's activities for today
Report Activity Past Week	Generate and launches a HTML report on the service's activities over the past week

Report Activity Past 30 Days	Generate and launches a HTML report on the service's activities over the past 30 days
Protected Service Start	Start the service being protected. Note – does not start the Protector
Protected Service Stop	Stop the service being protected. Note – does not stop the Protector

Tools

Local Security Settings/Policy	Open the application for editing security settings for the current machine
Desktop Security Settings	Open the application for editing desktop security settings for the current machine
Event Viewer	Open the Windows Event Viewer application, for examining the Event Logs
Services	Open the Services Control Panel application
Computer Management	Open the Computer Management Control Panel application
Task Manager	Open the Task Manager
Switch to Session 0	Switches to the isolated Session 0 desktop. Note that this option is only available on versions of Windows where Session 0 is accessible.

Help

User's manual (PDF)	Open this user's manual
Registration	Display the registration dialog, for purchasing and registering Service Protector (not available once registered)
Service Protector Home Page (Web)	Open the Service Protector home page in your browser. Your computer will need to be connected to the Internet for this to work.
How to Protect Popular Services (Web)	Open the tutorials web page in your browser. Your computer will need to be connected to the Internet for this to work.
Provide your feedback (Web)	Open the feedback web page in your browser. Please let us know what you think of Service Protector! Your computer will need to be connected to the Internet for this to work.
Check for Updates	Visit the program's web site and check if a new version is available
About Service Protector	Display program information

4.3. *The Toolbar*

For convenience, the most common functionality can be accessed from the toolbar. The buttons are as follows:



Add a Protector



Edit/View the selected Protector's settings



Start the selected Protector



Restart the selected Protector



Stop the selected Protector



Report on the selected Protector (in your web browser)



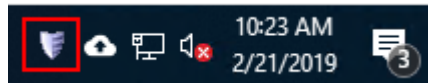
Remove the selected Protector



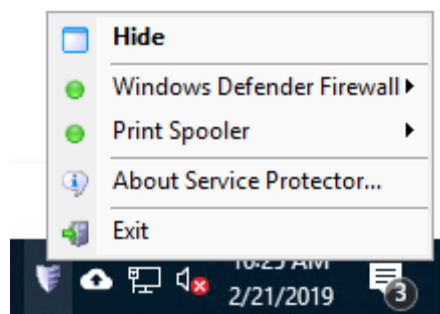
Display program information

4.4. The Task Tray Icon

When running, Service Protector will display its tray icon in the notification area of the Windows taskbar (pictured in the red rectangle):

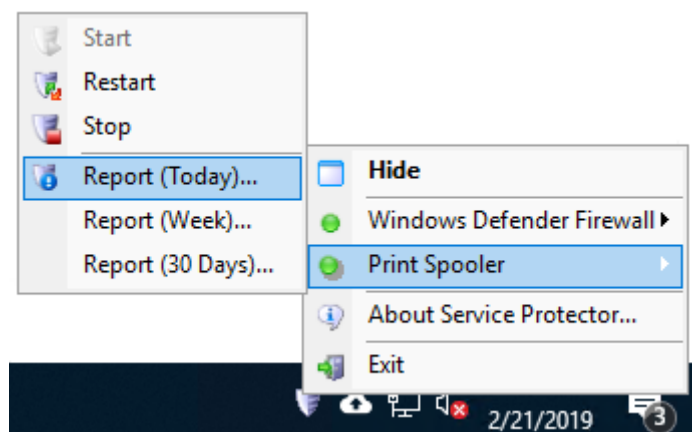


Several operations can be performed from this tray icon. Double-clicking the icon will hide or show the Service Protector main window. A right-click displays the menu:



Hide (or Show)	Hide (or Show) the Service Protector main window
<Protector1>	Display a sub-menu for controlling <Protector1>
<Protector2>, etc.	Display a sub-menu for controlling <Protector2>
About	Display program information
Exit	Exit Service Protector

A Protector can be started, restarted, stopped, or reported on from its sub-menu:



Start	Start the selected application if it is not running
Stop	Stop the selected application if it is running
Report (today)	Generate and launches a HTML report on the application's activities for today
Report (week)	Generate and launches a HTML report on the application's activities over the past week
Report (Past 30 Days)	Generate and launches a HTML report on the service's activities over the past 30 days

4.5. *Adding a Protector*

To monitor and protect a service, click on the “Add” toolbar button or select “Add” from the “Protector” menu. This will summon the “Add Protector” dialog, which consists of four tabs: General, Monitor, Email, and Extras.

Please see our web site for a short demonstration video showing how to protect the Print Spooler service:

<https://www.coretechnologies.com/products/ServiceProtector/HowToProtectVideo/>

4.5.1. The General Tab

The basic settings can be specified on the General tab:

The screenshot shows the 'Add Protector' dialog box with the 'General' tab selected. The title bar says 'Add Protector' with a question mark and a close button. Below the title bar is a shield icon with a green plus sign and the text 'Configure service protection settings' and 'Add a new Protector. Click the Save button record your settings.' The dialog has four tabs: 'General', 'Monitor', 'Email', and 'Extras'. The 'General' tab is active. It contains a 'Service to protect:' dropdown menu with 'Print Spooler' selected and a gear icon to its right. Below this is a section for 'When the service stops, restart it:' with a checked checkbox. Under this checkbox are four radio button options: 'Immediately' (selected), 'Not immediately, but:', 'On the next hour', 'On the next hour or half-hour', 'After: 15 minute(s)', and 'At: 10:29:50 AM'. Below these is a checked checkbox for 'Stop trying after: 5 attempts in 1 minute(s)'. Below that is a checked checkbox for 'Run this command prior to restarting the service:' with a text box containing 'C:\clean-printer-queue.bat' and a browse button (...). At the bottom of the tab is a checked checkbox for 'Start monitoring & protecting your service immediately'. At the bottom of the dialog are three buttons: '<< Back', 'Cancel', and 'Save >>'.

Service to protect: Select the service that you would like to protect.

When the service stops, restart it: Check to have Service Protector restart the service whenever it stops running. If not checked, Service Protector will never resuscitate your service if it stops.

Restart it immediately: Check to have Service Protector immediately restart the service whenever it stops running. Most users will want this option – to ensure that their service is always running, 24x7.

Restart it on the next hour: Choose this option to have your service restarted on the next hour whenever it stops running. For example, if it stops at 4:23 am, it would be restarted at 5 am. This option can be useful for services that are run once an hour on the hour.

Restart it on the next hour or half-hour: Choose this option to have your service restarted on the next hour or half-hour. For example, if it stops at 4:23 am, it would be restarted at 4:30 am. This option can be useful for services that should be run every 30 minutes.

Restart it after: Choose this option to have your service restarted after waiting a fixed amount of time (which you must specify in seconds, minutes, hours, or days). For example, if set to 15 minutes and the service stops at 4:23 am, Service Protector would run it again at 4:38 am.

Restart it at: Choose this option to have your service restarted at a specific time. This may be useful for service that must be run once a day, at a fixed time.

Stop trying after: Activate this option to prevent your service from being constantly restarted if it is failing to start properly. Specify the maximum number of attempts to tolerate over a given time frame in minutes.

Run this command prior to restarting the service: Specify a batch file (or application) to be run if there is cleanup work to be done before Service Protector restarts your service. Note that Service Protector will wait for the batch file/application to finish before restarting your service.

Start monitoring & protecting your service immediately: Check this option to have protection started once you click the “Save >>” button. If not, protection will not be launched until you start it explicitly (or reboot your computer).

4.5.2. The Monitor Tab

The Monitor tab groups many of the settings that describe how Service Protector is to monitor and manage the service:

The screenshot shows the 'Add Protector' dialog box with the 'Monitor' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar is a section titled 'Configure service protection settings' with a shield icon and a plus sign. Below this is a subtitle: 'Add a new Protector. Click the Save button record your settings.' The dialog has four tabs: 'General', 'Monitor', 'Email', and 'Extras'. The 'Monitor' tab is active. It contains a section titled 'Monitor the service and stop it:' with several checkboxes and input fields. The checkboxes are: 'Whenever its memory usage exceeds:', 'Whenever it hogs the CPU[s] for more than:', '% CPU threshold:', 'Average over all CPU's (instead of only one)', 'Whenever it "hangs" for longer than:', 'Whenever it fails a periodic sanity check', 'Whenever the computer resumes from sleep/hibernation', and 'At the following times:'. The input fields are: '512 MB', '5 minute(s)', '95', '2 minute(s)', and a list box containing 'Every Sunday @ 3 AM (reboot)'. There are buttons for 'Add...', 'Edit...', and 'Remove' next to the list box. At the bottom of the dialog are buttons for '<< Back', 'Cancel', and 'Save >>'. A note at the bottom left says: 'Note: After the service is stopped, the actions specified on the "General" tab will be performed.'

Monitor the service and stop it:

- ☒ Whenever its memory usage exceeds: 512 MB
- ☒ Whenever it hogs the CPU[s] for more than: 5 minute(s)
- % CPU threshold: 95
- ☐ Average over all CPU's (instead of only one)
- ☒ Whenever it "hangs" for longer than: 2 minute(s)
- ☒ Whenever it fails a periodic sanity check Set... ✓
- ☒ Whenever the computer resumes from sleep/hibernation
- ☒ At the following times:
 - Every Sunday @ 3 AM (reboot)
 - Add...
 - Edit...
 - Remove

Note: After the service is stopped, the actions specified on the "General" tab will be performed.

<< Back Cancel Save >>

Monitor the service and stop it whenever its memory usage exceeds: Check to have Service Protector monitor the service's memory use (as seen in the Windows Task Manager) and stop it when it exceeds the threshold value supplied in Megabytes (MB). Note that Service Protector will check the service

repeatedly over a 30 second time period and only take action if the memory threshold is consistently exceeded.

Monitor the service and stop it whenever it hogs the CPU for more than:

Check to have Service Protector stop the service if it uses too much of the CPU for longer than the specified time in minutes. The service is designated a “CPU hog” if it consumes more than the specified percent of a single CPU (as seen in the Windows Task Manager) over the given duration.

Average over all CPUs (instead of only one): A process consuming a single CPU is classified as a hog. If your service will scale to use all processes, (and use more than a single CPU on average), check this option to avoid false alarms.

Monitor the service and stop it whenever it “hangs”: Check to have Service Protector automatically stop the service whenever Windows classifies it as “Not responding” (as seen in the Windows Task Manager). Enter the time (in minutes) that you wish to wait before restarting a service that remains non-responsive. Activating this option will also allow Service Protector to detect “zombie” processes, which show up as running in the Task Manager but do not actively respond to the operating system.

Monitor the service and stop it whenever it fails a periodic sanity check:

Sometimes, even though your service says it’s running, it is not actually doing its work. For those tricky situations, you may be able to employ advanced failure detection (i.e. a “sanity check”) to identify those scenarios and have Service Protector automatically recycle your service.

You can configure a sanity check from the Monitor tab. Please see [Appendix I](#) for a full discussion of the sanity check feature.

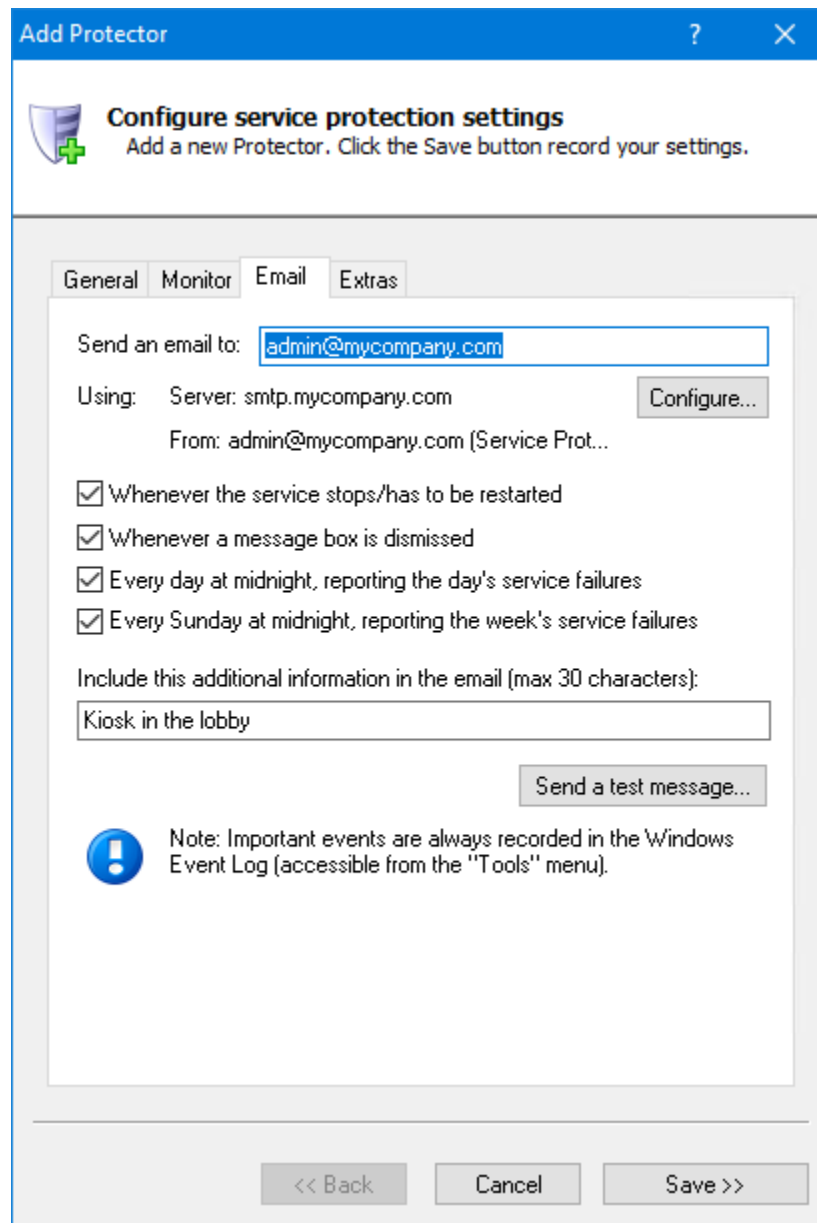
Monitor the service and stop it whenever the computer resumes from sleep/hibernation:

Check to have Service Protector stop the service when the PC comes out of a low-power state. This is useful for services that can’t handle the “time lapses” or interruptions associated with powering down.

Monitor the service and stop at the following times: Check to stop the service (or reboot the machine) at one or more specific times. Use the buttons to the right to add, change or remove the times to stop the service. Note that the service will be restarted as per the schedule indicated on the General tab.

4.5.3. The Email Tab

The Email tab describes the email alert settings:



The screenshot shows the 'Add Protector' dialog box with the 'Email' tab selected. The dialog has a blue title bar with a question mark and a close button. Below the title bar, there is a shield icon with a green plus sign and the text 'Configure service protection settings' and 'Add a new Protector. Click the Save button record your settings.' The dialog has four tabs: 'General', 'Monitor', 'Email', and 'Extras'. The 'Email' tab is active. It contains a text box for 'Send an email to:' with the value 'admin@mycompany.com'. Below this, there is a 'Using:' section with 'Server: smtp.mycompany.com' and a 'Configure...' button. The 'From:' field is 'admin@mycompany.com (Service Prot...'. There are four checkboxes, all of which are checked: 'Whenever the service stops/has to be restarted', 'Whenever a message box is dismissed', 'Every day at midnight, reporting the day's service failures', and 'Every Sunday at midnight, reporting the week's service failures'. Below these is a text box for 'Include this additional information in the email (max 30 characters):' with the value 'Kiosk in the lobby'. There is a 'Send a test message...' button. At the bottom, there is a note with an exclamation mark icon: 'Note: Important events are always recorded in the Windows Event Log (accessible from the "Tools" menu)'. At the very bottom of the dialog are three buttons: '<< Back', 'Cancel', and 'Save >>'.

To: The target email address(es). Separate multiple addresses with a space or comma (,).

Whenever the service stops/has to be restarted: Check to send an email when the service being monitored stops prematurely/crashes.

Whenever a message box is dismissed: Check to send an email whenever Service Protector dismisses a message box on behalf of the service being monitored. The full text of the message box will be included in the email.

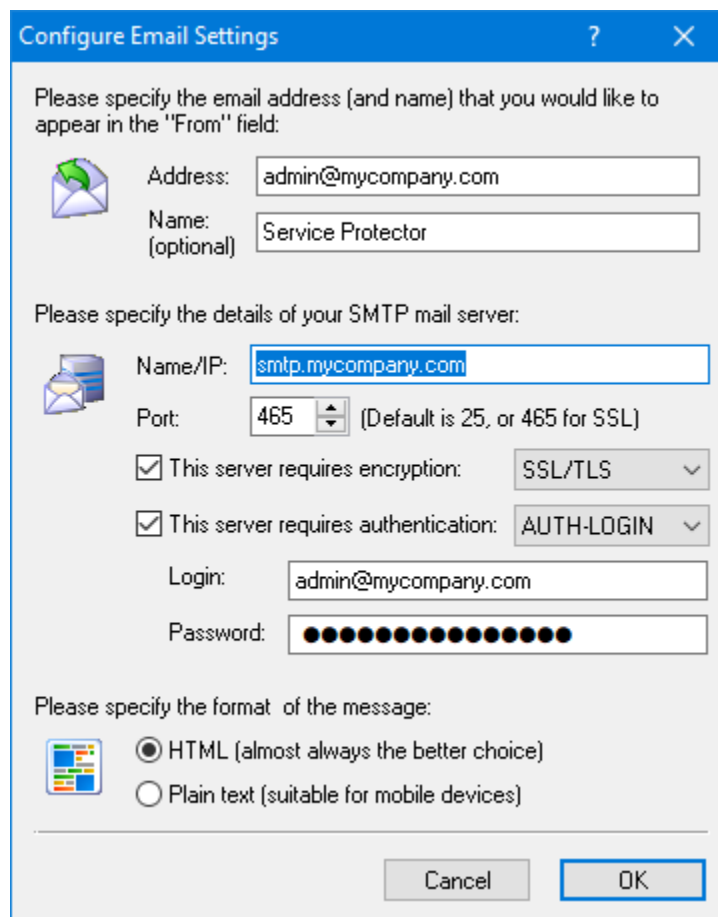
Every day at midnight, reporting the service's activities: Check to send a nightly email detailing the service's activities over the previous day. A sample report is shown in [section 4.12](#).

Every Sunday at midnight, reporting the service's activities: Check to send a weekly email detailing the service's activities over the previous week. A sample report is shown in [section 4.12](#).

Include this additional information in the email: Optionally specify some text that will be included in each email message sent. The text will appear in the body, in a line labeled "Additional". If you expect many emails from various similar installations you are encouraged to enter an identifier of some kind here -- one that will help you to identify the source of each message you receive. Please specify at most 30 characters.

Send a test message: Clicking this button will generate a test email to the given target address(es) using the settings specified.

Configure: Clicking this button will summon the "Configure Email Settings" dialog, where details on the mail server (and more) can be specified:



Configure Email Settings

Please specify the email address (and name) that you would like to appear in the "From" field:

Address: admin@mycompany.com

Name: (optional) Service Protector

Please specify the details of your SMTP mail server:

Name/IP: smtp.mycompany.com

Port: 465 (Default is 25, or 465 for SSL)

☒ This server requires encryption: SSL/TLS

☒ This server requires authentication: AUTH-LOGIN

Login: admin@mycompany.com

Password: [Masked]

Please specify the format of the message:

☒ HTML (almost always the better choice)

☐ Plain text (suitable for mobile devices)

Cancel OK

Address: The email address that will be displayed in the "From" field of the email messages sent by Service Protector.

Name: The name that will be displayed in the "From" field of the email messages sent by Service Protector. This value is optional.

Name/IP: Enter the name (or IP address) of your mail server. The server must be able to accept and route standard SMTP traffic. Please consult a system administrator if in doubt.

Port: The numeric port on which the mail server is available. Note that the default is 25 for regular SMTP servers and 465 for servers using SSL – please specify one if these if in doubt.

This server requires encryption: Check this box if the mail server uses SSL, TLS or STARTTLS. Select the appropriate protocol from the accompanying dropdown.

This server requires authentication: Check if the server requires authentication, and select the authentication method. The choices are CRAM-MD5, AUTH-LOGIN, AUTH-PLAIN, and AUTH-NTLM. A login and a password will be required for all but AUTH-NTLM.

Login: The user name/login for the mail server.

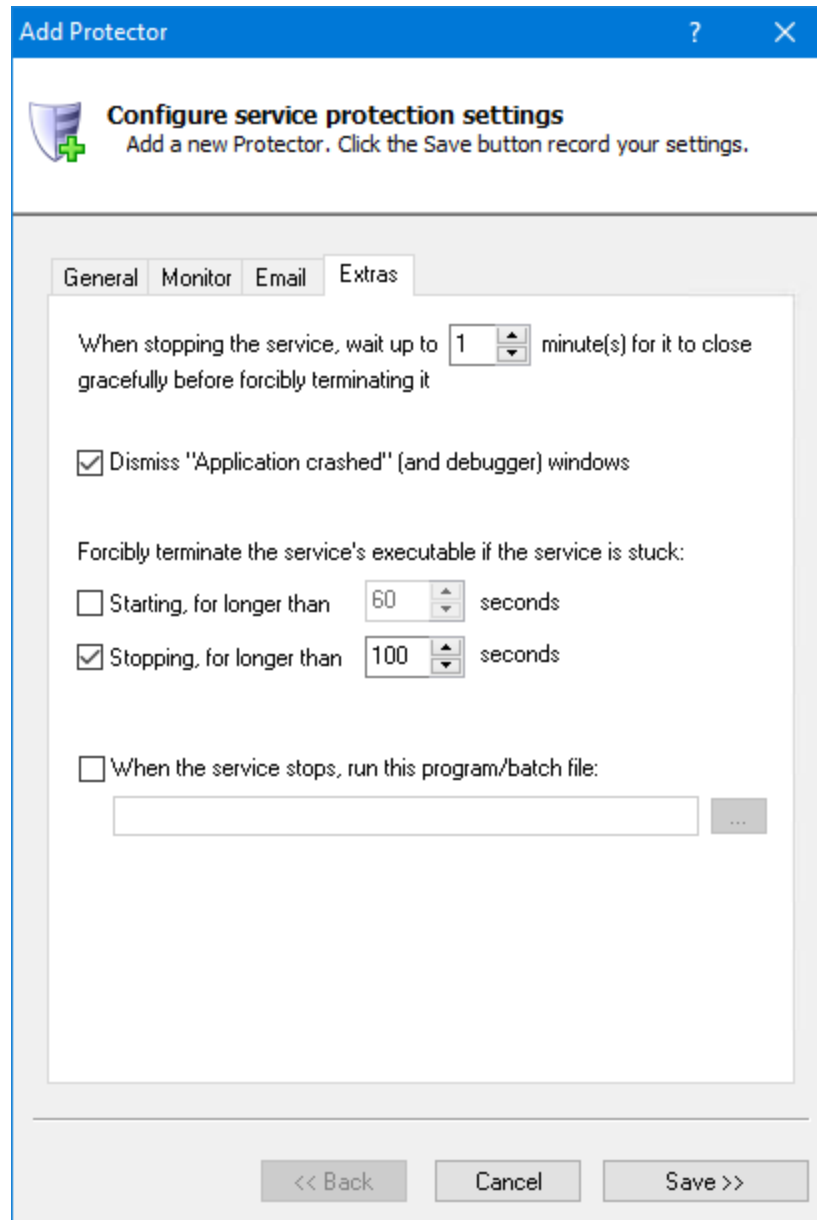
Password: The password for the mail server.

HTML Format: Select this option to have your emails composed in rich HTML format (the default).

Plain Text Format: Select this option to have Service Protector send email in simple text, with no markup. This is an appropriate choice for mobile devices which can not effectively render HTML.

4.5.4. The Extras Tab

This tab contains a few “extra” settings:



The screenshot shows the 'Add Protector' dialog box with the 'Extras' tab selected. The dialog has a blue title bar with a question mark and a close button. Below the title bar is a section with a shield icon and the text 'Configure service protection settings' and 'Add a new Protector. Click the Save button record your settings.' The 'Extras' tab is active, showing several settings: 'When stopping the service, wait up to 1 minute(s) for it to close gracefully before forcibly terminating it' (with a spinner box set to 1); a checked checkbox 'Dismiss "Application crashed" (and debugger) windows'; a section 'Forcibly terminate the service's executable if the service is stuck:' with two options: 'Starting, for longer than 60 seconds' (unchecked) and 'Stopping, for longer than 100 seconds' (checked); and an unchecked checkbox 'When the service stops, run this program/batch file:' with an empty text box and a browse button (...). At the bottom are three buttons: '<< Back', 'Cancel', and 'Save >>'.

When stopping the service, wait for it to close gracefully before terminating it: By default, Service Protector will wait for 1 minute for the service to stop gracefully before it terminates the underlying process. You should increase the time here if it can take longer for your service to shutdown properly.

Dismiss/cancel “Application crashed” (and debugger) windows: Check to have Service Protector automatically dismiss/cancel message boxes that the service being monitored (or Windows) may pop up while running. This handles the dreaded Application Error dialog, which informs of a crash but still leaves the process running in a vegetative state. This option is particularly useful for developers running their services in debug mode as the standard debug/assert dialogs are handled (and their full textual content captured in the Windows Event Log and email).

Forcibly terminate the service’s executable if the service is stuck Starting: If your service can get stuck forever in the Starting state, check this box to have Service Protector terminate it after waiting a while. Specify the amount of time to wait.

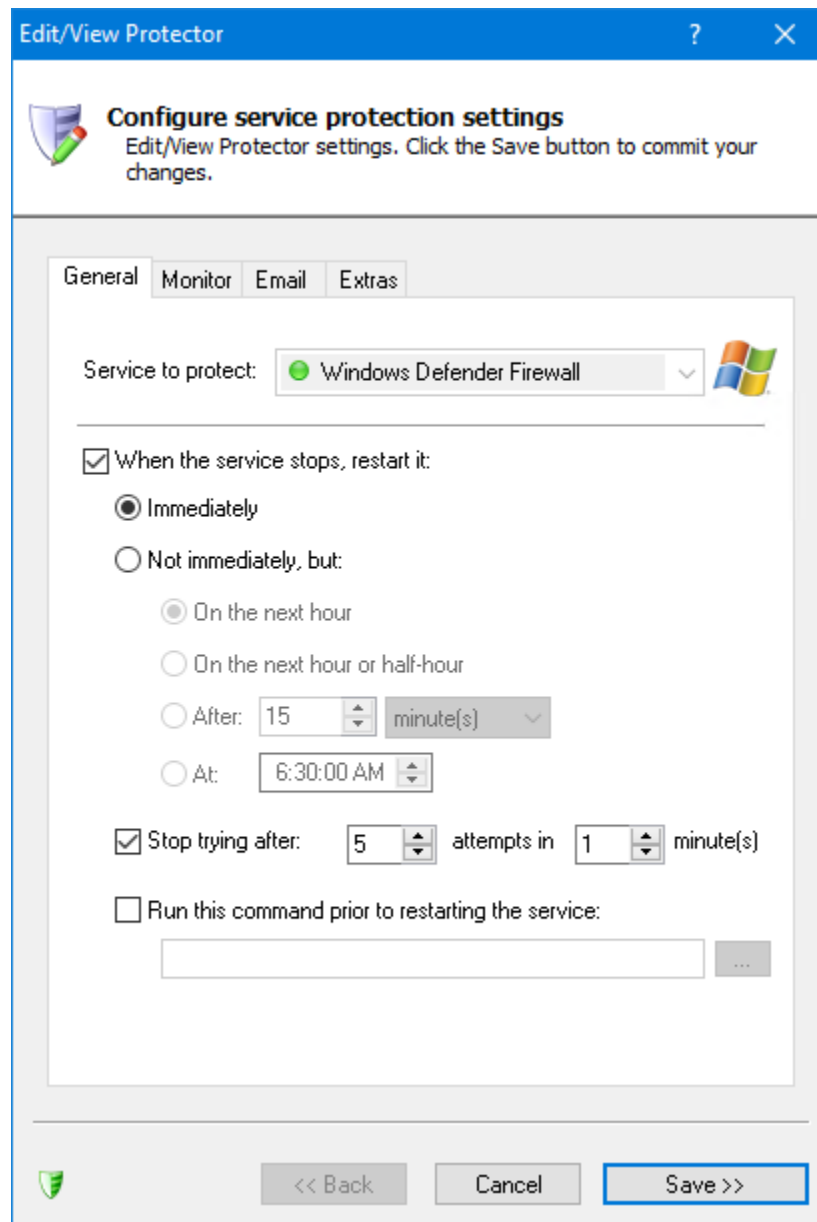
Forcibly terminate the service’s executable if the service is stuck Stopping: If your service can get stuck forever in the Stopping state, check this box to have Service Protector terminate it after waiting a while. Specify the amount of time to wait.

When the service stops, run this program/batch file: Check to specify a program that will be run whenever Service Protector has detected that the service has stopped. Note that this program will be invoked under all circumstances, independently of how the service stops (normally or abnormally), and that Service Protector will wait for it to complete (except sometimes when the protection is being stopped).

Once all required information has been specified to your satisfaction, click the “Save >>” button to add your new Protector.

4.6. Editing Protector Settings

Edit a Protector's settings by either double-clicking on its entry, or highlighting its entry and choosing "Edit/View" from the "Protector" menu. This will bring up the "Edit/View Protector" dialog:



The "Edit/View Protector" dialog is identical to the "Add Protector" dialog described in [section 4.5](#), with the only difference being that the service being

protected cannot be changed. Please see [section 4.5](#) for a description of the “Add Protector” dialog.

Click on the “Save >>” or “Save & Restart >>” button to commit your changes. Note that if your Protector is running, it will be briefly stopped while changes are saved, and then restarted in a few seconds. *The service being protected will not be stopped.*

4.7. *Starting a Protector*

Start a Protector by highlighting its entry in the list and clicking the “Start” toolbar button, or by selecting “Start” from the “Protector” menu. This functionality will not be available if the selected Protector is already active/running.

4.8. *Stopping a Protector*

Stop a Protector by highlighting its entry in the list and clicking the “Stop” toolbar button, or by selecting “Stop” from the “Protector” menu. This functionality will not be available if the selected Protector is not active/running.

4.9. *Removing a Protector*

Remove a Protector by highlighting its entry in the list and clicking the “Remove” toolbar button, or by selecting “Remove” from the “Protector” menu. You will be asked to confirm the removal. Note that a Protector cannot be removed while it is active/running.

4.10. Reporting on a Service's Activities

As it monitors your service, Service Protector writes relevant information to the "Application" section of the Windows Event Log, including:

- CPU statistics (average / peak)
- Memory statistics (average / peak)
- Service restart events
- Threshold exceeded events (CPU & memory), etc.

Service Protector will summarize this activity in a single web page if you select "Report Activity" from the "Protector" menu and choose whether to see today's or the past week's activity. The report will be opened in your web browser and can be saved in HTML format from the browser. A sample report is below.

**Service Protector Agent Report for "Web Server"**

Date & Time: Thursday, March 25, 2010 12:00:32 AM (Eastern Standard Time)
Computer: kiosk-pc / 192.83.201.153
Additional: XP VM

Summary

	Wednesday 3/24/2010
Number of times run	43
Number of restarts	40
Memory: Average / Peak	3.5 / 49.0 MB
CPU: Average / Peak	4 / 99 %
Time running	23.4 hours
Availability	98 %

Note: Today's statistics may not include all information if the service is currently running.

Details
Wednesday 3/24/2010

Time	Description
10:34:59 PM	The service has been restarted (run #7).
10:34:55 PM	Service Statistics: 2010/03/24 19:57:35 - 2010/03/24 22:34:50 (2.6 hours) CPU (Avg / Max): 0% / 2% Memory (Avg / Max): 3.4MB / 7.0MB
10:34:55 PM	Service Protector Agent has detected that the service has stopped.
10:34:45 PM	A message box entitled "Microsoft Visual C++ Runtime Library" has been dismissed. The message box contained the following text: Runtime Error! Program: C:\Apps\SPSimulator\ServiceProtectorSimulator.exe This application has requested the Runtime to terminate it in an unusual way. Please contact the application's support team for more information.
07:57:30 PM	The service has been restarted (run #6).
07:57:26 PM	Service Statistics: 2010/03/24 19:10:05 - 2010/03/24 19:57:24 (47.3 minutes) CPU (Avg / Max): 6% / 99% Memory (Avg / Max): 3.4MB / 3.5MB
07:57:25 PM	The service has been using on average 97% of the CPU(s) for longer than 2 minutes. It will be terminated.

4.11. *Exporting a Protector to a File (XML)*

Service Protector allows you to export your Protector's settings to a XML file by either:

- (1) selecting "Export..." from the "Protector" menu and subsequently specifying an XML file to be created, or
- (2) dragging-and-dropping from the list of Protectors to Windows Explorer (or the desktop, etc.) to create a new XML file in the specified location.

The XML file created can be taken to another machine and imported there to re-create the Protector on that machine.

4.12. *Exporting all Protectors to a Directory*

All Protectors can be exported at once by selecting "Export all..." from the "Protector" menu. You will be prompted for a directory, and an XML file will be created there for each Protector.

Each file name created will resemble:

"<service-name>_ serviceprotector.xml"

For example, if you have a service called "Firewall", then the exported file will be named "Firewall_ serviceprotector.xml".

The XML files created can be taken to another machine and imported there to re-create the Protectors on that machine.

4.13. *Importing a Protector from a File (XML)*

Service Protector allows you to import a previously exported XML file by either:

- (1) selecting "Import..." from the "Protector" menu and selecting the XML file, or
- (2) dragging-and-dropping from Windows Explorer (or the desktop, etc.) to the list of Protectors in Service Protector.

Importing a file will summon the "Add Protector" window (described in [section 4.5](#)) where you can confirm settings and supply passwords if necessary prior to actually creating the Protector.

4.14. *Adding a Copy of a Protector*

To make a copy of a Protector, select it in the list and choose “Add Copy...” from the “Protector” menu. This will launch the “Add Protector” window (described in [section 4.5](#)) with all settings copied from the selected Protector. You will have to choose the service to protect before saving.

5. Licensing & Registration

Service Protector is free to evaluate for the first 30 days. After the trial period a license must be purchased to continue usage.

Prior to licensing, Service Protector will:

- 1) Show a “Registration” dialog when it is started. Follow the instructions there to purchase a license and register the application.
- 2) Emit registration reminders whenever an email is sent from the program or when a message is added to the event log.

If you find the program useful, we encourage you to license it. The small licensing fee charged will fund continued development of Service Protector and will entitle you to expedited support from Core Technologies Consulting LLC, the author of the software.

Please see:

<https://www.CoreTechnologies.com/products/ServiceProtector>

for the latest licensing and registration information. The software can be purchased there as well (Visa / MasterCard / PayPal / Amazon accepted).

Pricing is as follows (subject to change – please check our website above for the current):

Quantity/Description	Price per license (US dollars)
1	\$99.99
2-9	\$89.99 (<i>a 10% discount</i>)
10+	\$79.99 (<i>a 20% discount</i>)
Limited Site <i>Install on up to 50 computers, at a single geographic location.</i>	\$1,999 (<i>50% savings</i>)
Unlimited Site <i>Install on an unlimited number of computers, at a single geographic location.</i>	\$2,999 (<i>unlimited savings</i>)
Limited Multi-Site <i>Install on up to 100 computers, at multiple geographic locations.</i>	\$2,999 (<i>62% savings</i>)
Unlimited Multi-Site <i>Install on an unlimited number of computers, at multiple geographic locations.</i>	\$3,999 (<i>unlimited savings</i>)
Limited OEM <i>Royalty-free distribution, limited to a maximum of 25 client installations per year.</i>	\$1,999 (<i>unlimited savings</i>)
Unlimited OEM <i>Royalty-free distribution, with unlimited client installations per year.</i>	\$3,999 (<i>unlimited savings</i>)

6. Troubleshooting and Reporting Problems

If you encounter a problem while using Service Protector, please send email to:
support@CoreTechnologies.com

Be sure to include the following information:

- Your Operating System
- The version of Service Protector in use
- Detailed steps for reproducing any software bugs/issues

Feel free to send requests for enhancements to the same address, or fill in our Feedback Form:

<https://www.coretechnologies.com/products/ServiceProtector/customer-feedback>

7. Appendix I: The Sanity Check Feature

Sometimes, even though your service says it's running, it is not actually doing its work. For those tricky situations, you may be able to employ advanced failure detection (i.e. a "sanity check") to help Service Protector expose and automatically recycle your service.

You can activate a sanity check from the [Monitor tab](#). Start by checking the **Whenever it fails a periodic sanity check** box:

Add Protector ? X

Configure service protection settings
Add a new Protector. Click the Save button record your settings.

General **Monitor** Email Extras

Monitor the service and stop it:

- ☐ Whenever its memory usage exceeds: 512 MB
- ☐ Whenever it hogs the CPU(s) for more than: 5 minute(s)
% CPU threshold: 95
☐ Average over all CPUs (instead of only one)
- ☐ Whenever it "hangs" for longer than: 1 minute(s)
- ☒ Whenever it fails a periodic sanity check Set...
- ☐ Whenever the computer resumes from sleep/hibernation
- ☐ At the following times:

Add... Edit... Remove

Note: After the service is stopped, the actions specified on the "General" tab will be performed.

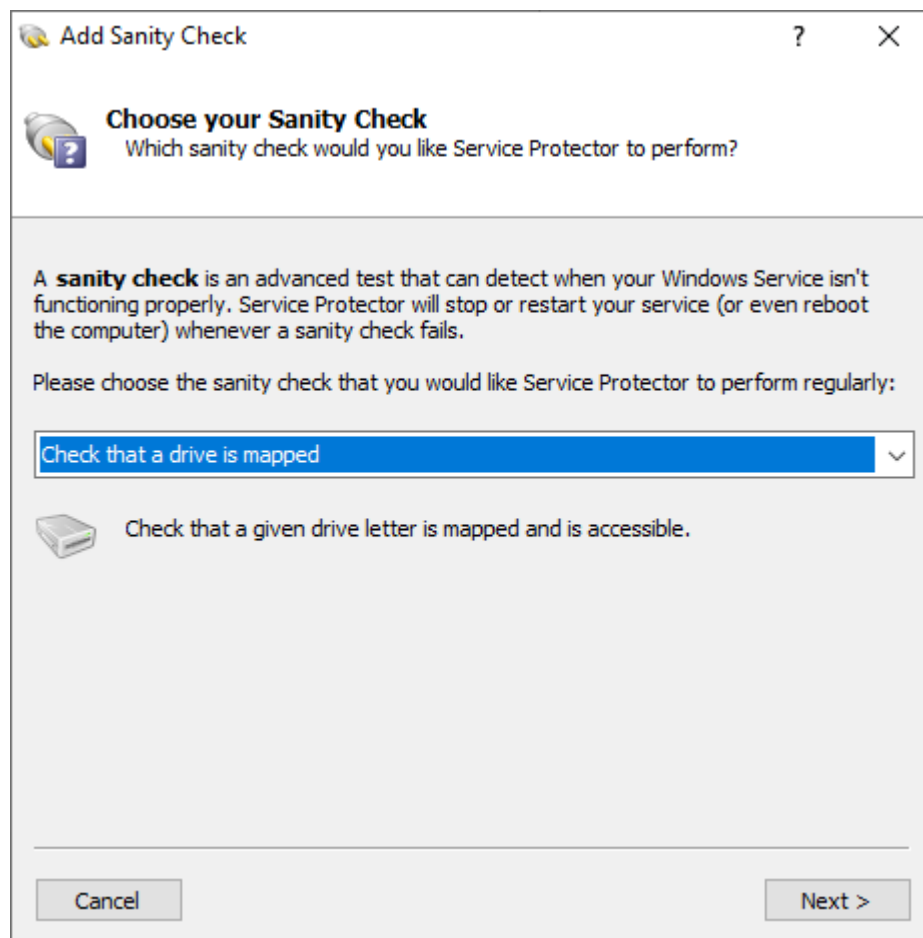
<< Back Cancel **Save >>**

Next, click the **Set** button to summon the Sanity Check Wizard, which will guide you step by step through the configuration process.

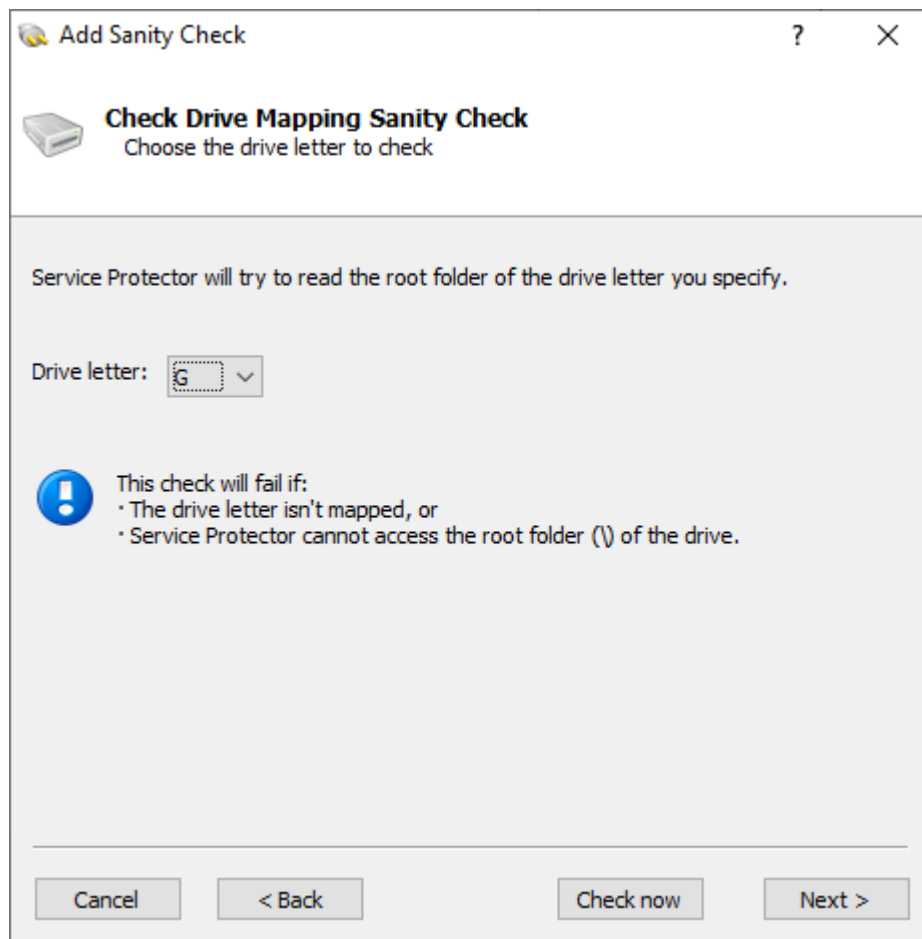
The following sanity checks are available.

7.1. *Check that a drive is mapped*

Does your service rely on a specific drive to do its work? Or does it map a drive letter for other programs? If so, this sanity check may be helpful because it restarts your service whenever it detects that a given drive isn't available.

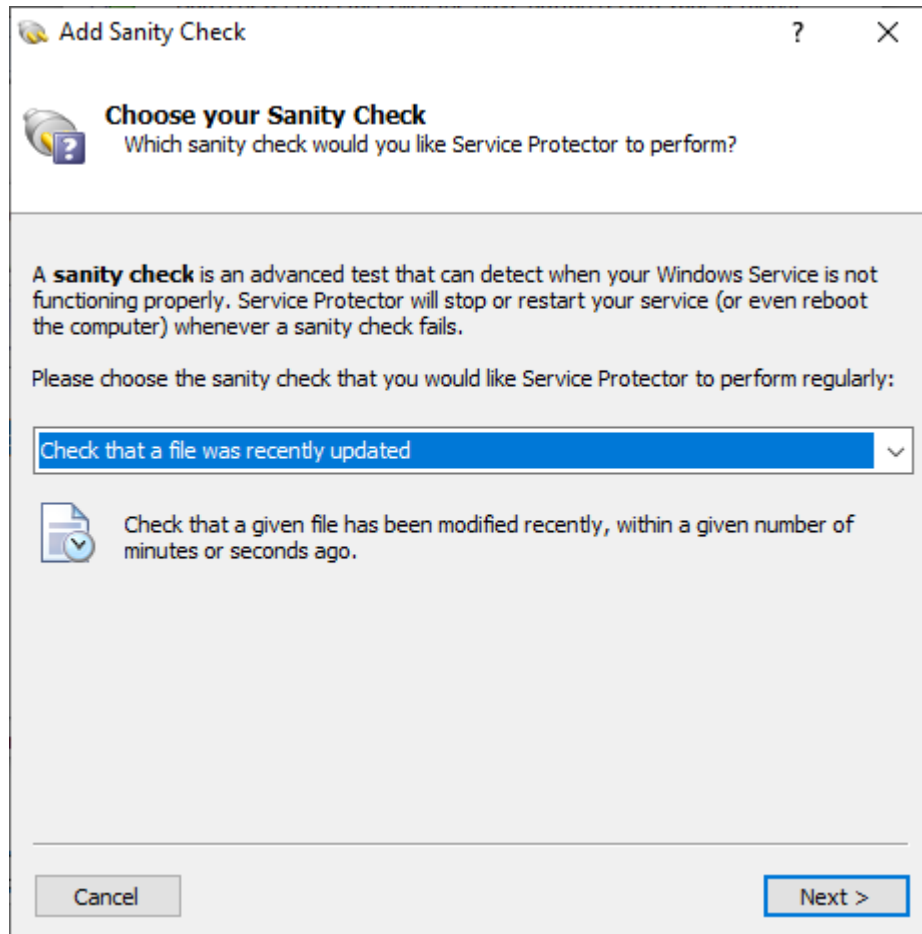


You must specify the drive letter to be checked:

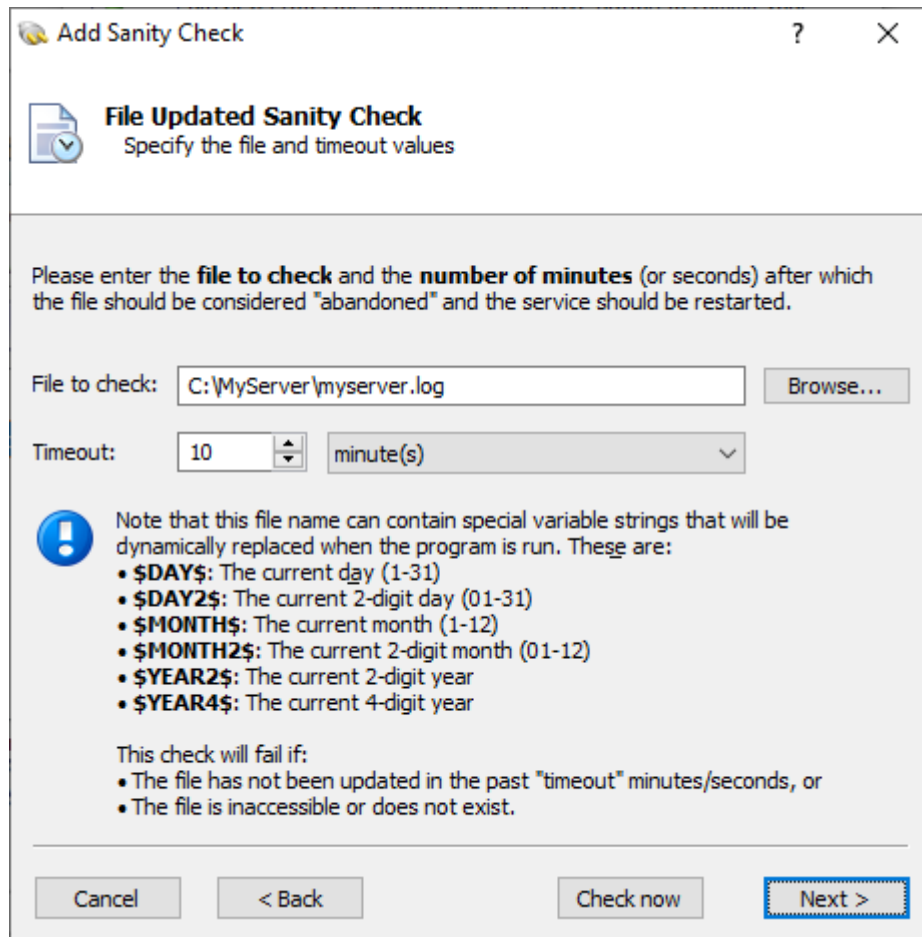


7.2. *Check that a file was recently updated*

This sanity check may be helpful if your service should be considered failed if it stops writing to a file.



You must specify the full path to the file to be checked and the time after which the file should be considered “stale”:



The screenshot shows a Windows-style dialog box titled "Add Sanity Check". It has a question mark icon and a close button (X) in the top right corner. Below the title bar, there is a tab labeled "File Updated Sanity Check" with a document icon and a downward arrow. Underneath the tab, it says "Specify the file and timeout values".

The main area of the dialog contains the following text: "Please enter the **file to check** and the **number of minutes** (or seconds) after which the file should be considered "abandoned" and the service should be restarted."

There are two input fields: "File to check:" with a text box containing "C:\MyServer\myserver.log" and a "Browse..." button to its right; and "Timeout:" with a spinner box set to "10" and a dropdown menu currently showing "minute(s)".

Below the input fields, there is a blue information icon followed by a note: "Note that this file name can contain special variable strings that will be dynamically replaced when the program is run. These are:"

- **\$DAY\$**: The current day (1-31)
- **\$DAY2\$**: The current 2-digit day (01-31)
- **\$MONTH\$**: The current month (1-12)
- **\$MONTH2\$**: The current 2-digit month (01-12)
- **\$YEAR2\$**: The current 2-digit year
- **\$YEAR4\$**: The current 4-digit year

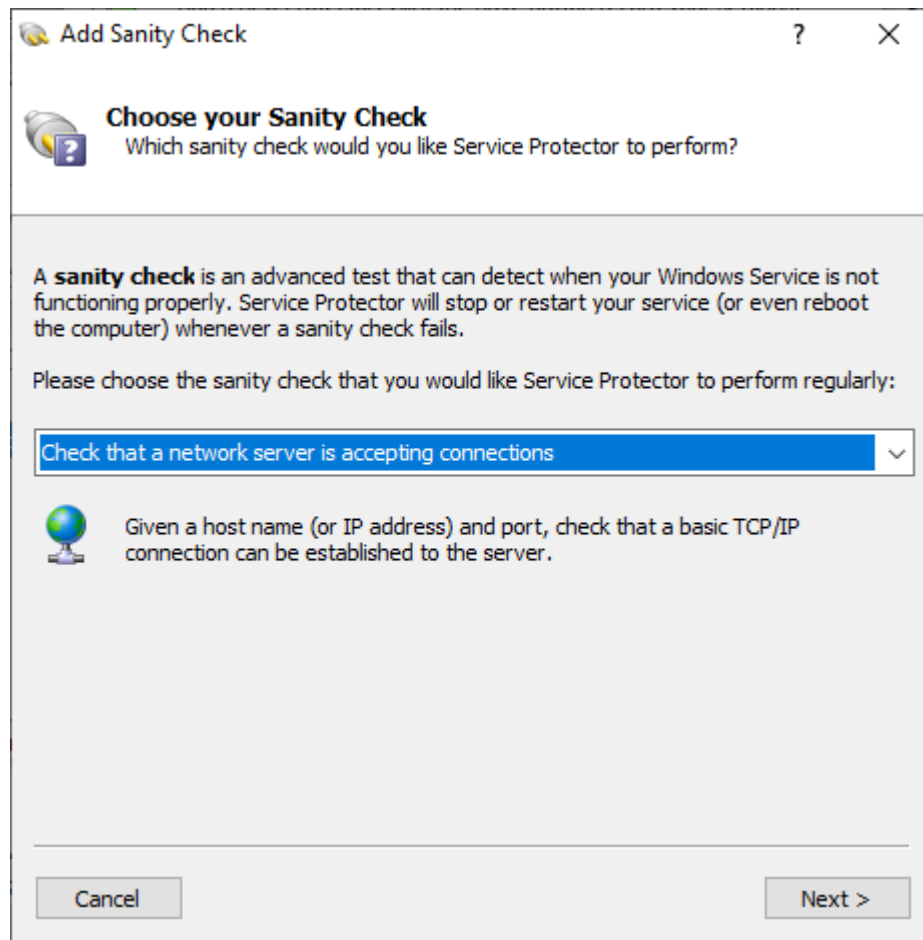
Below the list, it says "This check will fail if:"

- The file has not been updated in the past "timeout" minutes/seconds, or
- The file is inaccessible or does not exist.

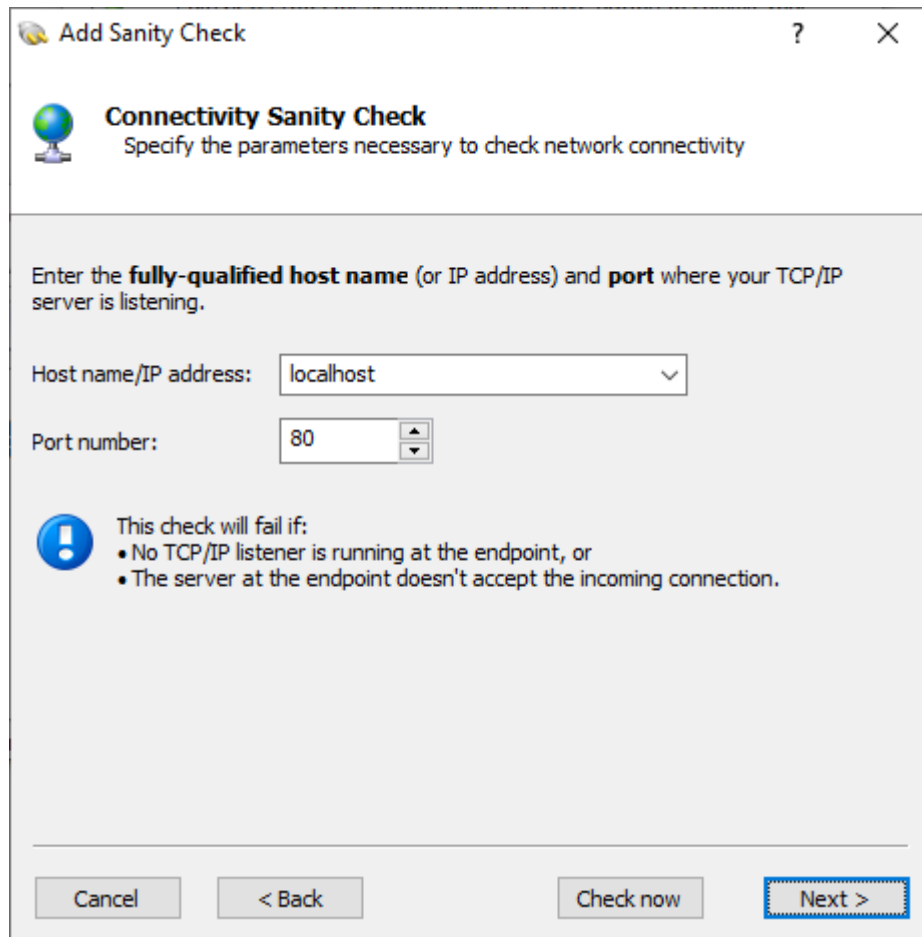
At the bottom of the dialog, there are four buttons: "Cancel", "< Back", "Check now", and "Next >". The "Next >" button is highlighted with a blue dashed border.

7.3. *Check that a network server is accepting connections*

This sanity check will trigger a failure if a given endpoint is not accepting TCP/IP connections. It's good for any server providing an internet service (e.g. FTP, SSH, etc.) to other devices.



You must supply a host name (or IP address) and port number of the endpoint to be checked:



The image shows a Windows-style dialog box titled "Add Sanity Check". It has a question mark icon and a close button (X) in the top right corner. Below the title bar, there is a globe icon and the text "Connectivity Sanity Check" followed by "Specify the parameters necessary to check network connectivity". The main area of the dialog contains instructions: "Enter the **fully-qualified host name** (or IP address) and **port** where your TCP/IP server is listening." Below this, there are two input fields: "Host name/IP address:" with a dropdown menu showing "localhost", and "Port number:" with a spinner box showing "80". Below the input fields, there is a blue warning icon and the text "This check will fail if:" followed by a bulleted list: "• No TCP/IP listener is running at the endpoint, or" and "• The server at the endpoint doesn't accept the incoming connection." At the bottom of the dialog, there are four buttons: "Cancel", "< Back", "Check now", and "Next >". The "Next >" button is highlighted with a blue border.

Add Sanity Check

Connectivity Sanity Check
Specify the parameters necessary to check network connectivity

Enter the **fully-qualified host name** (or IP address) and **port** where your TCP/IP server is listening.

Host name/IP address: localhost

Port number: 80

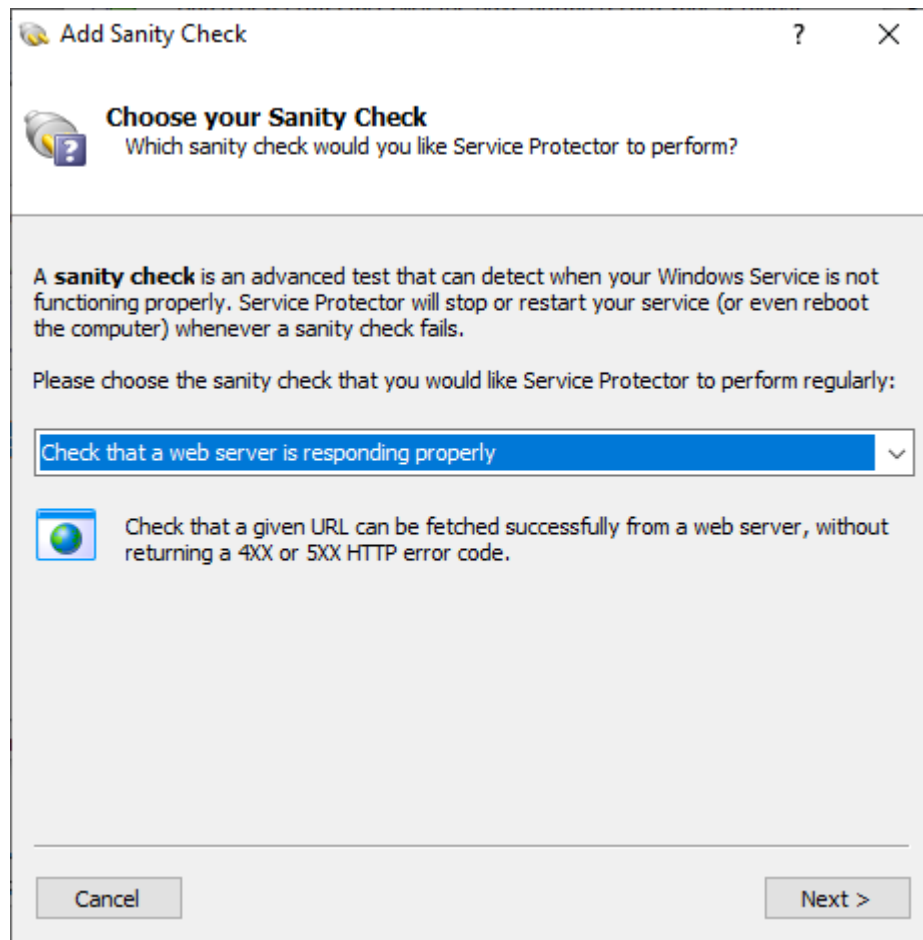
! This check will fail if:

- No TCP/IP listener is running at the endpoint, or
- The server at the endpoint doesn't accept the incoming connection.

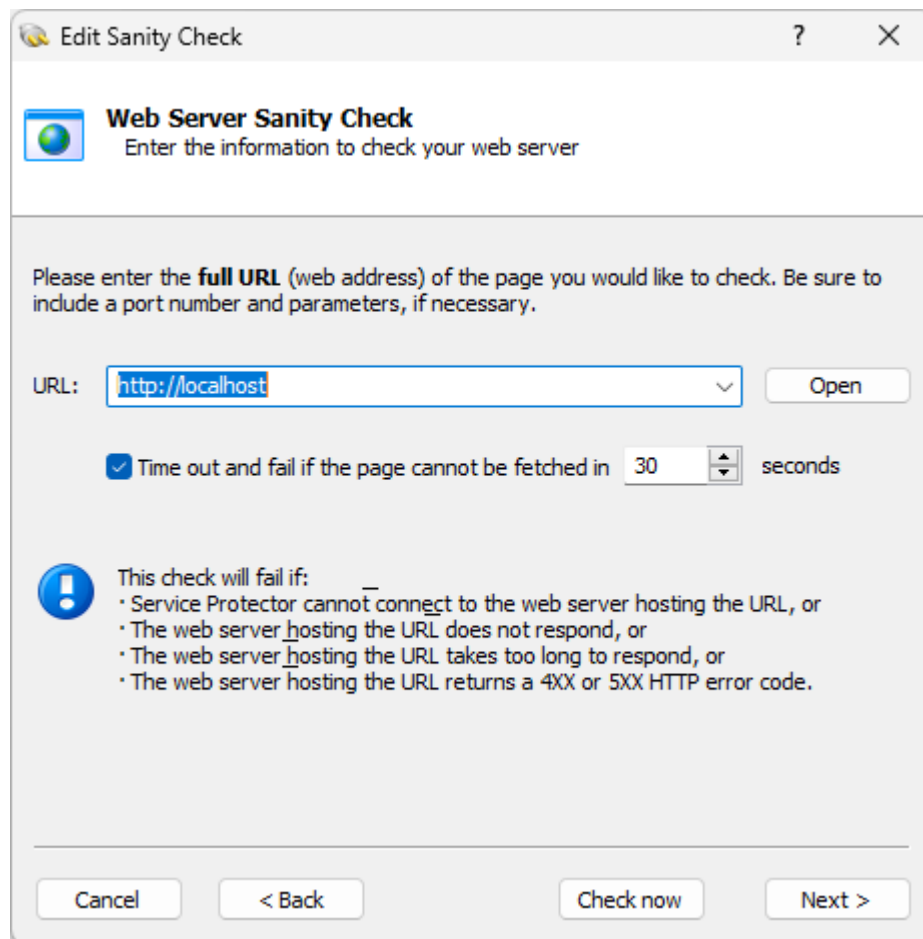
Cancel < Back Check now **Next >**

7.4. *Check that a web server is responding properly*

If your service hosts a web server, this sanity check will help to detect problems serving web pages. The check will fail if your server doesn't respond or returns a 4XX or 5XX HTTP error code.



You must specify the URL that the sanity check will fetch:



The screenshot shows a dialog box titled "Edit Sanity Check" with a question mark icon and a close button. Below the title bar, there is a section titled "Web Server Sanity Check" with a globe icon and the instruction "Enter the information to check your web server". The main area contains a text box for the URL, currently showing "http://localhost", and an "Open" button. Below this is a checkbox labeled "Time out and fail if the page cannot be fetched in" followed by a spinner box set to "30" and the word "seconds". At the bottom, there is a section titled "This check will fail if:" with a list of four conditions: "Service Protector cannot connect to the web server hosting the URL, or", "The web server hosting the URL does not respond, or", "The web server hosting the URL takes too long to respond, or", and "The web server hosting the URL returns a 4XX or 5XX HTTP error code." The dialog box has a "Cancel" button, a "< Back" button, a "Check now" button, and a "Next >" button.

Edit Sanity Check

Web Server Sanity Check
Enter the information to check your web server

Please enter the **full URL** (web address) of the page you would like to check. Be sure to include a port number and parameters, if necessary.

URL:

☒ Time out and fail if the page cannot be fetched in seconds

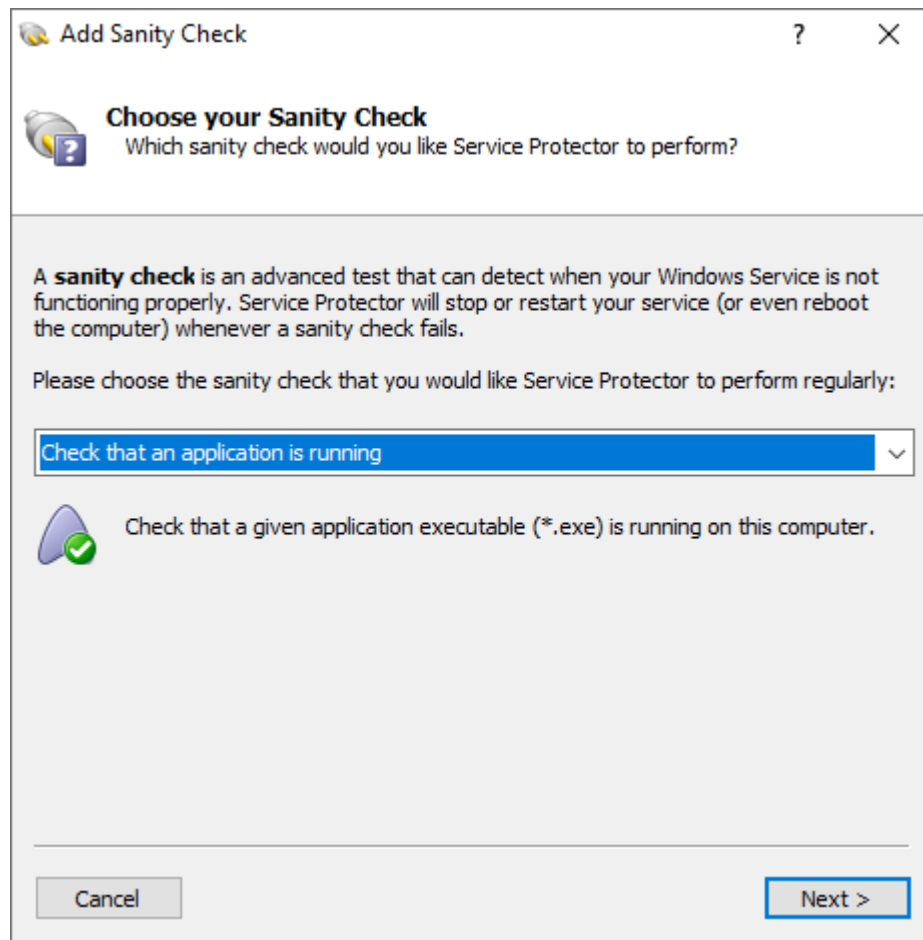
This check will fail if:

- Service Protector cannot connect to the web server hosting the URL, or
- The web server hosting the URL does not respond, or
- The web server hosting the URL takes too long to respond, or
- The web server hosting the URL returns a 4XX or 5XX HTTP error code.

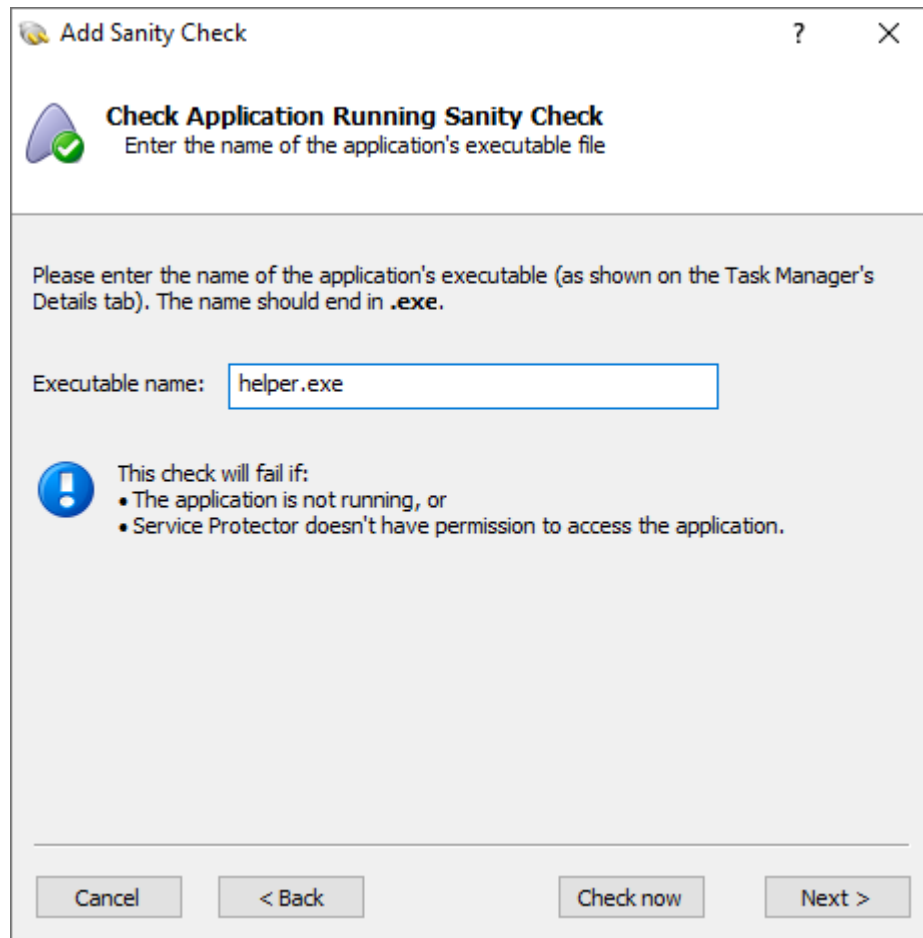
You can also set a timeout value, to indicate how to handle a sluggish web server that takes a long time to respond. By default, the sanity check will fail if the server doesn't respond within 30 seconds.

7.5. *Check that an application is running*


Does your service depend on an important “helper” application to function properly? If so, Service Protector can periodically check if the helper application is running and restart your service if the application isn’t active.



You must specify the name of the helper application’s executable file to enable the check:




Add Sanity Check

 **Check Application Running Sanity Check**
Enter the name of the application's executable file

Please enter the name of the application's executable (as shown on the Task Manager's Details tab). The name should end in **.exe**.

Executable name:

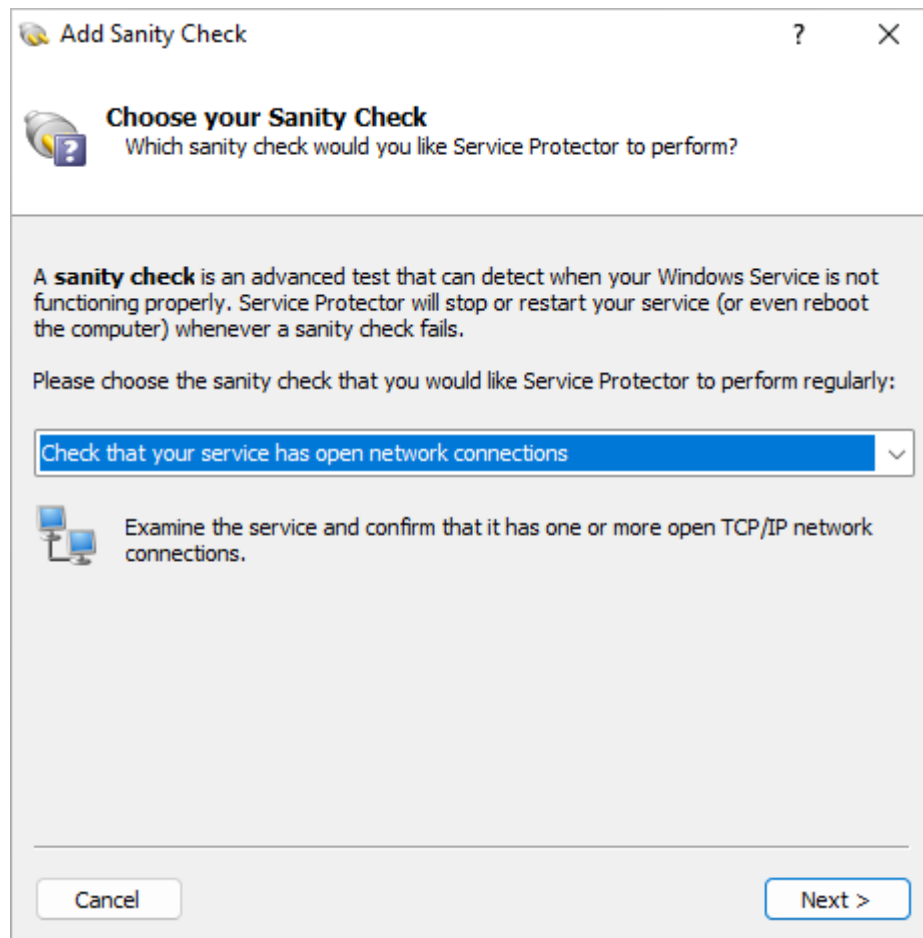
 This check will fail if:

- The application is not running, or
- Service Protector doesn't have permission to access the application.

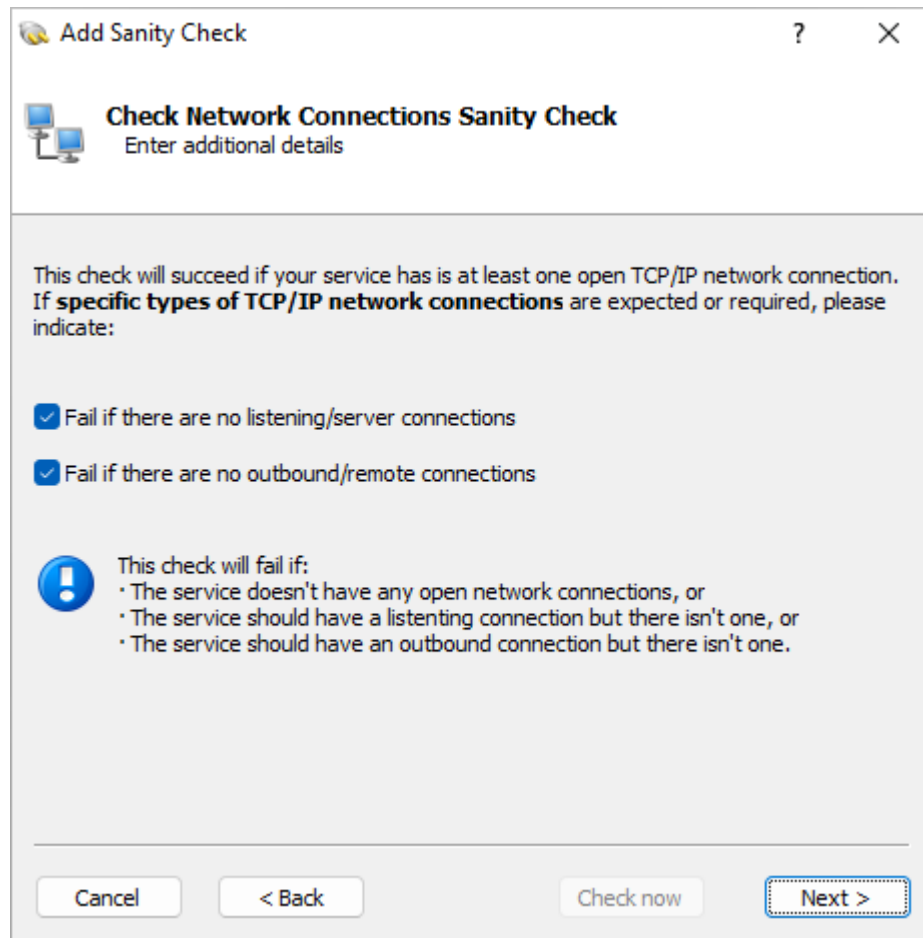
For example, to check that Microsoft Word is running, enter “winword.exe” (no quotes).

7.6. *Check that your service has open network connections*

Is your service a typical server that accepts TCP/IP requests over the network? If so, you may want to configure the network connections sanity check. With that in place, Service Protector will automatically restart your service if it has no inbound or outbound connections.



You get the opportunity to specify what types of network connections (outbound or inbound) to monitor:



The screenshot shows a Windows-style dialog box titled "Add Sanity Check". It has a question mark icon and a close button (X) in the top right corner. Below the title bar, there is a section with a computer icon and the text "Check Network Connections Sanity Check" followed by "Enter additional details". The main area of the dialog contains the following text: "This check will succeed if your service has is at least one open TCP/IP network connection. If **specific types of TCP/IP network connections** are expected or required, please indicate:". Below this text are two checked checkboxes: "Fail if there are no listening/server connections" and "Fail if there are no outbound/remote connections". Further down, there is a blue circular icon with a white exclamation mark, followed by the text "This check will fail if:" and a bulleted list: "• The service doesn't have any open network connections, or", "• The service should have a listening connection but there isn't one, or", and "• The service should have an outbound connection but there isn't one.". At the bottom of the dialog, there are four buttons: "Cancel", "< Back", "Check now", and "Next >". The "Next >" button is highlighted with a dashed border.


Add Sanity Check

Check Network Connections Sanity Check
Enter additional details

This check will succeed if your service has is at least one open TCP/IP network connection. If **specific types of TCP/IP network connections** are expected or required, please indicate:

☒ Fail if there are no listening/server connections

☒ Fail if there are no outbound/remote connections

 This check will fail if:

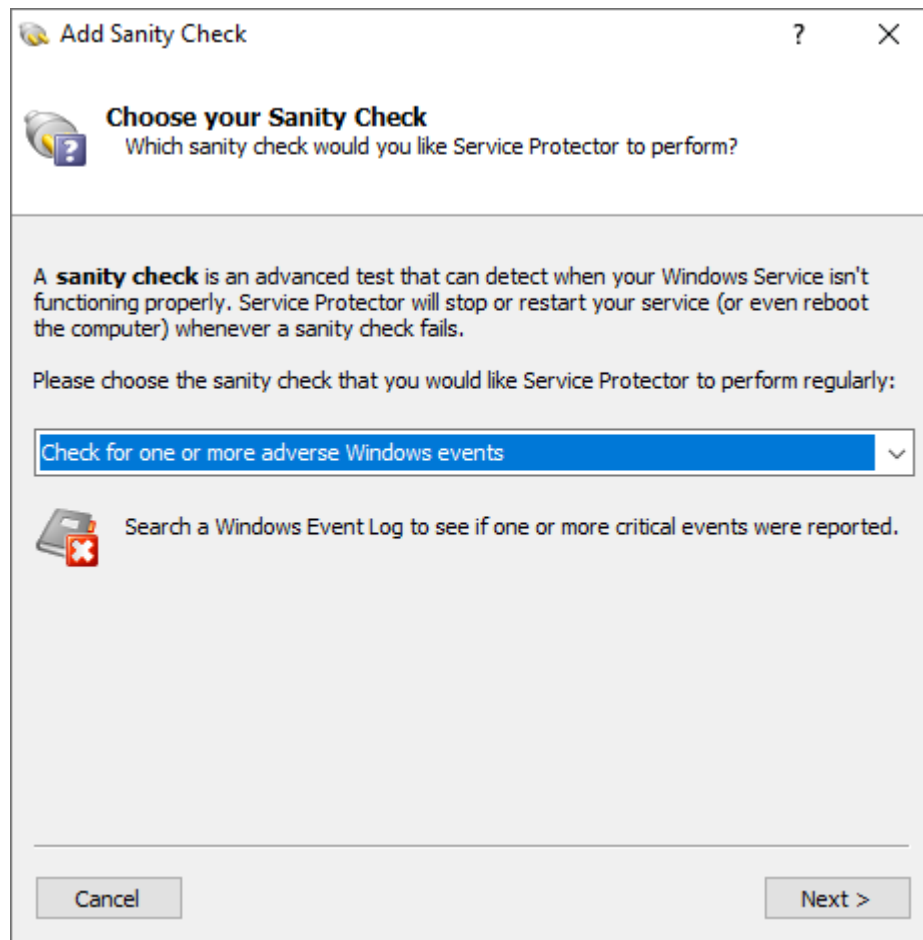
- The service doesn't have any open network connections, or
- The service should have a listening connection but there isn't one, or
- The service should have an outbound connection but there isn't one.

Cancel < Back Check now **Next >**

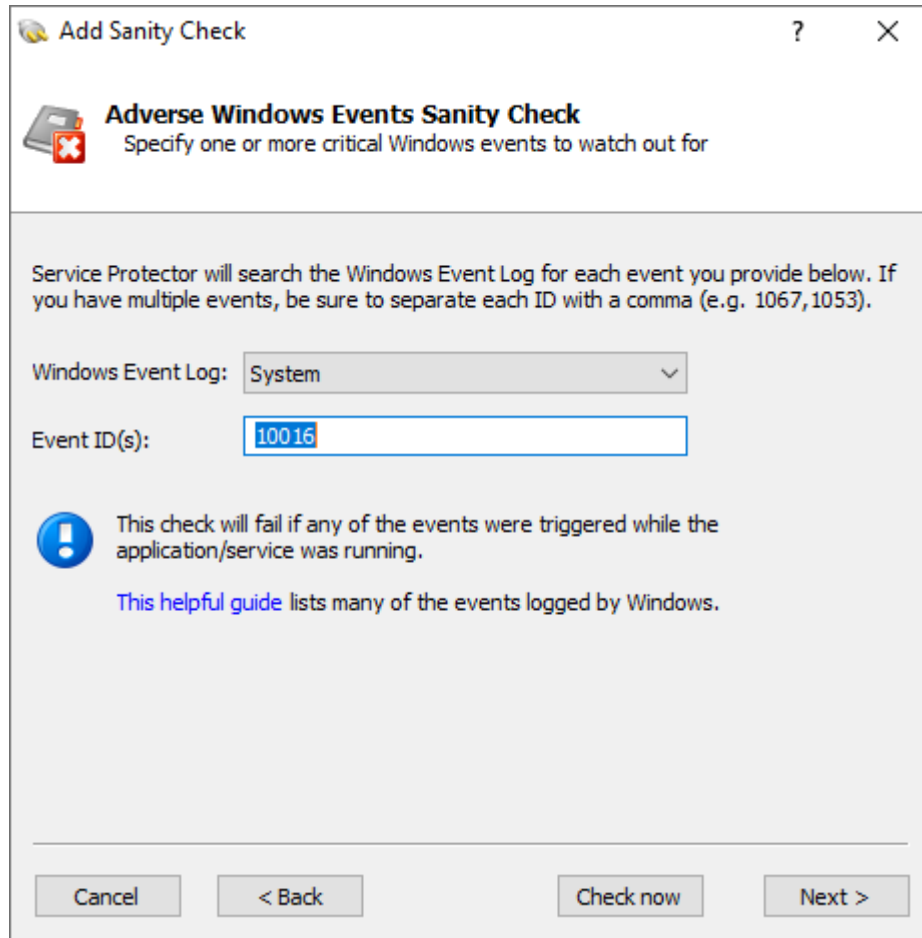
For a simple server, you probably want to check for listening/server connections only.

7.7. *Check for one or more adverse Windows events*

Does your service stop working when a specific event shows up in the [Windows Event Viewer](#)? If so, you should configure this sanity check to watch for that event and restart your service whenever it's reported.



You'll have to choose the Windows Event Log to monitor as well as the events that signal trouble. If there are multiple events, separate the ID's with commas (like 10016,7040,24).



Add Sanity Check

Adverse Windows Events Sanity Check
Specify one or more critical Windows events to watch out for

Service Protector will search the Windows Event Log for each event you provide below. If you have multiple events, be sure to separate each ID with a comma (e.g. 1067,1053).

Windows Event Log: System

Event ID(s): 10016

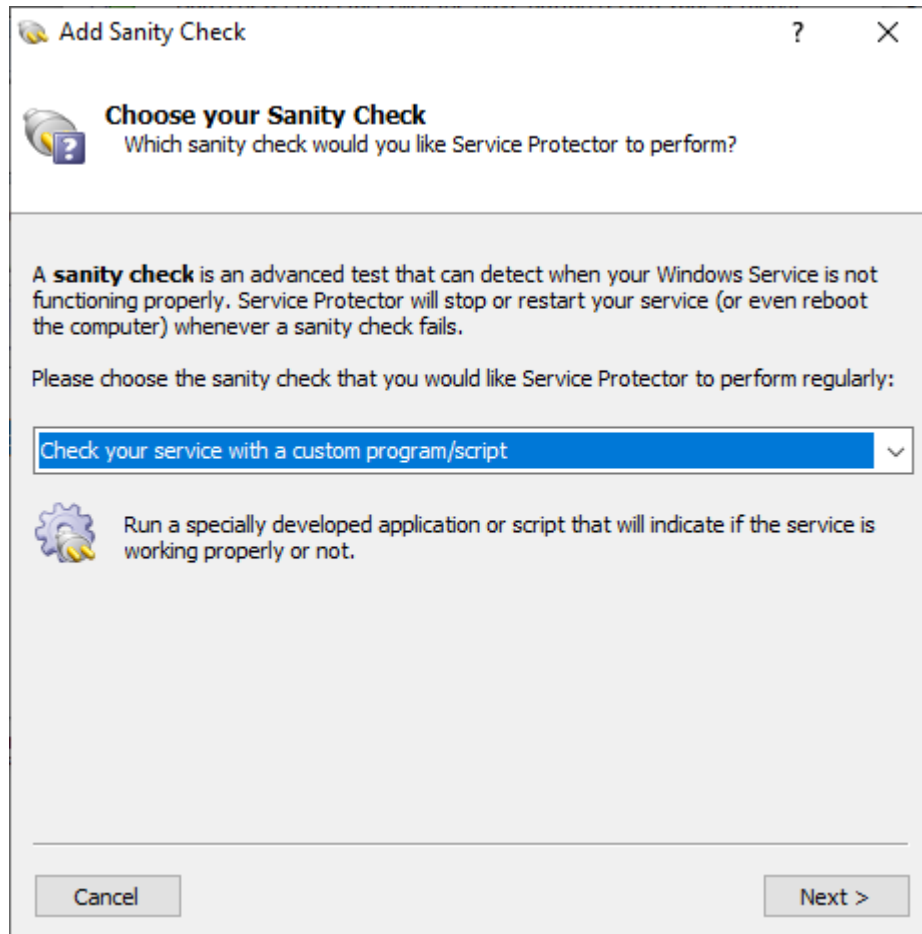
This check will fail if any of the events were triggered while the application/service was running.

[This helpful guide](#) lists many of the events logged by Windows.

Cancel < Back Check now Next >

7.8. *Check your service with a custom program/script*

For the ultimate in extensibility, Service Protector can run your own specially designed program or script to detect if the service is functioning normally.



Specify the full path to your utility and any arguments it needs:


Add Sanity Check

Custom Sanity Check
Specify the command to run to check on your service

Please enter the **application or script to run**. If your application takes arguments, be sure to quote them appropriately.

Application or script:

Arguments (optional):

 The application/script should exit with a return code of:

- 0 if the check succeeds;
- 1 if the check fails and the service should be stopped;
- 10 if the check fails and the computer should be rebooted;
- 100 if the check fails and the service should be stopped and not restarted.

The custom sanity check program should exit with a return code of:

- 0 when the check succeeds;
- 1 when the check fails and the service should be stopped and restarted as you have configured;
- 10 when the check fails and the computer should be rebooted;
- 100 when the check fails and your service should be stopped **and not restarted**;
- any other value when the check fails due to an error independent of the service being monitored (such as an error internal to the utility), or to simply indicate failure without causing a restart.

In the last case, the service is not restarted but a message is written to the event log (and an email is sent if so configured).

Note that if the sanity check utility fails to complete in 120 seconds, the service will be restarted.

The popular “ConnectToSocketSanityCheck” program (with full source code) is available in the “SanityCheck” sub-directory. Given a host and port on the command line, it returns 0 if a socket could be opened, 1 if the socket could not be opened, and -1 if there was an internal error initializing the sockets API. It can be used to check if a TCP/IP application is accepting connections.

7.8.1. Special Command Line Variables

Service Protector is able to pass your custom sanity check program one or more “special” values. Compose your command line with the appropriate string and Service Protector will make the substitution before invoking your program.

Replacement String	Replaced With
<code>\$SERVICEPROTECTOR_PID</code>	The program identifier (PID) of your running service. This can be seen in the Task Manager.
<code>\$SERVICEPROTECTOR_SERVICENAME</code>	The name of the service being protected (the short name).

For example, to have Service Protector pass your sanity check program the service’s program identifier (PID), then your command line might resemble this:

```
C:\myserver\my_check.exe $SERVICE PROTECTOR_PID
```

If your service is running with PID 563, then your Sanity program will be invoked like this:

```
C:\myserver\my_check.exe 563
```

8. Appendix II: Working from the Command Line

Service Protector consists of two main executables. *ServiceProtector.exe* is a conventional GUI application used to manage all Protectors, while *ServiceProtectorAgent.exe* is a command-line program that runs behind the scenes to protect each of your services. This section discusses how to use Service Protector from the DOS command prompt.

*Note: Be sure to run the commands from an elevated DOS prompt. Both *ServiceProtectorAgent.exe* and the NET command (discussed below) require administrative permissions to function properly.*

8.1. Importing a Protector

To import and install a Protector described in an XML file, run:

ServiceProtectorAgent.exe -import <XML-File-Name>

where **<XML-File-Name>** is the full path to an XML file created by exporting a Protector.

A return code of 0 signals success; anything else indicates failure.

8.2. Exporting a Protector

To export all the settings from a given Protector to an XML file, run:

ServiceProtectorAgent.exe -export <Service-Name> <XML-File-Name>

where **<Service-Name>** is the name of the service being protected (Note: not the display name!) as seen in the Windows Services Control Panel application and **<XML-File-Name>** is the full path to the XML file to be created.

A return code of 0 signals success; anything else indicates failure.

Note: If your protector is configured to send email and you have provided an account for your mail server, your password will not appear in the exported XML file. This is for security purposes. Instead, you will see the text "ENTER A PASSWORD". You will have to replace this placeholder value with the real password if you intend to import this file into Service Protector.

8.3. *Starting & Stopping a Protector*

Service Protector creates a Windows Service for each Protector and protection can be stopped and started using the Windows NET command.

To start a Protector, run

NET START "ServiceProtector: <Service-Name>"

where **<Service-Name>** is the name of the service being protected (Note: not the display name!) as seen in the Windows Services Control Panel application. For example, if you are protecting a service named "lanmanworkstation" you could start it by running:

NET START "ServiceProtector: lanmanworkstation"

To stop a Protector, simply use STOP instead of START:

NET STOP "ServiceProtector: <Service-Name>"