Servers Alive Version 3.3

Administrator's Guide

Revision Date: September 12, 2002

Woodstone bvba

Contents

Introduction

Welcome to Servers Alive, the award winning monitoring tool from Woodstone bvba. Servers Alive is designed to monitor many different types of servers and services from a centralized location and report their status. It supports many generalized tests applicable to servers of all types, along with specialized tests for certain types of services. When it detects that a server or service has become unavailable it is capable of reporting this condition in a variety of ways. It can even act to take care of the problem without any human interaction.

Servers Alive is used all over the world by companies in all types of businesses, from computer to legal, military to government. They rely on it to monitor their mission critical servers. Servers Alive is a compact and inexpensive tool, but it packs a lot of punch. It has a feature set that compares favorably with the most popular monitoring packages available, but sells for a fraction of the cost and can monitor up to 1000 servers or services (registered version only).

We're sure you'll enjoy your experience with Servers Alive. As such, we offer the product free to those who only wish to monitor ten or less servers or services. We're confident you'll see the incredible worth you can get out of this amazing product!

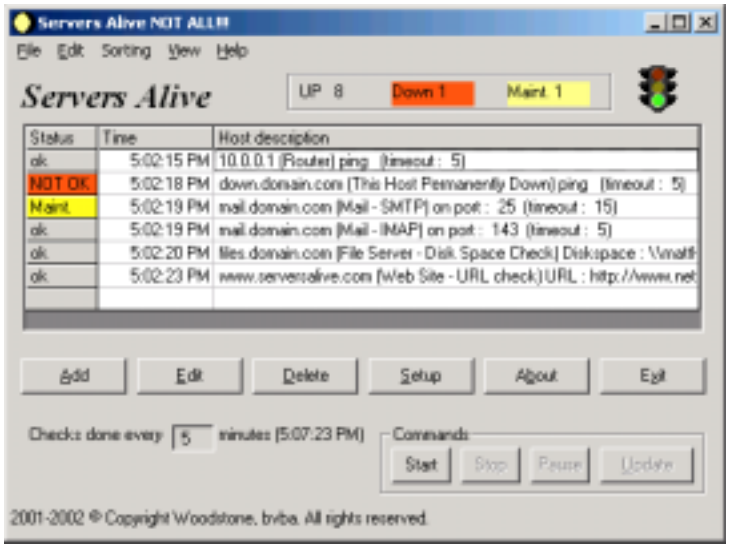
Installation

Servers Alive has the following requirements for installation:

- Windows 2000 (professional or server), NT (workstation or server), ME, 98, or 95. Windows XP is not supported.
- Network Interface Card
- TCP/IP

If you use a double-byte version of Windows (ex. Chinese or Japanese versions) you will need a custom version of Servers Alive. Contact us for details.

Before installing Servers Alive it is best to make sure that Windows has been updated to include the most recent patches provided by Microsoft. This assures the best possible compatibility. If you plan to use Servers Alive to check Oracle or MS SQL databases, you must install the corresponding client software provided by the database manufacturer, as Servers Alive uses the client to perform its checks. If you will be checking any Novell specific servers you must install the Client for Novell Networks provided by Novell. The Novell client provided by Microsoft is not sufficient for the Netware checks.



Servers Alive

Servers Alive is obtained primarily through an Internet download. If you want a CD you have the option of having one shipped to you when you purchase the full version of the software. There is only one version of the software, regardless of whether you will use it for ten or less entries or whether you have purchased a full license. You can download the software from http://www.woodstone.nu/salive.

You can find the download link at that page and may choose from any of the worldwide mirrors.

Once you have downloaded the software package and saved it to a convenient location simply launch the installation program. Note that you cannot install Servers Alive through a Terminal Server session, and when running Servers Alive as a service through Terminal Server you will not see the tray icon. The installation program will ask you for a location where it can install the software, which you may set to any location you want. The install program will extract all program files to the location you specify and create entries for Servers Alive on your Start Menu under the heading **Alive**. Please note that you must be an administrative user on the computer before you can install Servers Alive. Also note that on Windows 2000 you must have the **telephony service** running or the CPU will go to 100% utilization.

Servers Alive can be run as a service if the computer you install it on is running Windows NT or Windows 2000. During installation your OS will be detected, and the service automatically installed if Windows NT or 2000 is detected. To have Servers Alive start automatically on boot up you must go to the **Services** control panel and set the service called **Servers Alive** to automatic startup.

When Servers Alive is installed it also installs a few companion applications that can be used to extend the functionality of Servers Alive. You will find a subdirectory called external which includes some sample external check applications that you can use. The applications that are included in the external directory are created and maintained by Woodstone bvba, but there are other applications, made by other authors and provided free, that you can download from the Woodstone bvba web site. There are also some applications in the main Servers Alive directory that you can use to help you create your own external checks. For more information reference the External Checks section.

Configuration

Before adding any monitored entries to Servers Alive you need to configure its various options and features. Servers Alive has many powerful features that you can use to tweak the monitoring process. It's recommended that these be configured before adding any entries, as you will not be able to use most of the alerting or monitoring features without globally configuring them first.

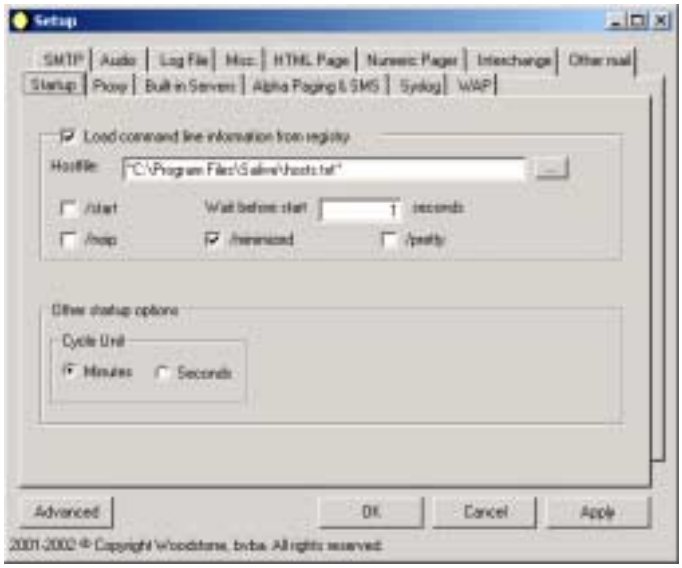
The first thing to do is enter your registration code if you purchased the product. You can do this by selecting the **Register** menu option. This menu option is only visible in the unregistered product. The required **Name**, **Company**, and **Registration Code** should have been provided to you by email when you purchased a full license. If you did not receive a registration code please send an email to support@woodstone.nu.

Next you should open up the configuration menu. Do this by pushing the button at the bottom of the screen labeled **Setup**. There are many tabs in the Setup portion that allow you to configure how Servers Alive goes about monitoring and alerting you. We will go through each tab individually.

Startup

The startup tab controls how Servers Alive gets its list of monitored services, and what it does with them initially. If you plan to have Servers Alive startup automatically and read in a saved list of monitored services (required for operation as a service) check the **Load command line information from registry** check box. Servers Alive will store in the registry the various startup options and the name of the file containing information on what hosts to check.

You can use **Hostfile** to specify where the saved file containing check information is located. This file hasn't been created yet if you are reading through this documentation for the first time, so you will have to come back to this later, after you have created your list of entries.



Startup

Start tells servers alive to automatically start checking when it is launched. The **Wait before start** box allows you to make Servers Alive pause before checking. This is useful if you are running Servers Alive as a service when the computer boots up, but need it to wait for all local programs to finish launching before starting its check cycle.

By default the first time Servers Alive checks a host it will resolve the name into an IP address. Each of the following times Servers Alive checks your host it will use the IP address it has stored in memory. In some cases (people using some dynamic IP services) servers will periodically change addresses. In order to force Servers Alive not to keep the IP addresses in memory you must specify the **noip** parameter.

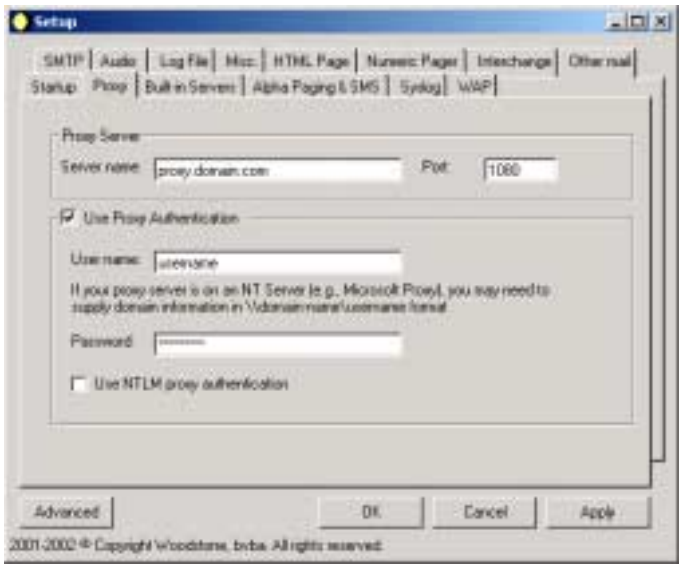
Minimized starts Servers Alive minimized (whether it is launched manually or as a service), and **Pretty** shows only the pretty names in the main interface. Pretty names are labels that you assign to your monitored items for easy recall.

Finally, at the bottom you can decide whether Servers Alive will use minutes or seconds as its **Cycle Unit**. This time unit determines how long Servers Alive will wait between check cycles, which is set on the **Misc** tab.

Proxy

Depending on your setup, you may require Servers Alive to do some or all URL type checks through a proxy for security purposes. You can force this behavior by specifying a server and port in the proxy section. You may enter either the domain name or IP address of the server. Just entering information in this section of setup does not force all URL checks to go through the proxy. You must still enable the use of proxy on specific entries.

Some proxy servers can't be accessed if you are not authenticated by the proxy server. Servers Alive can do **BASIC** authentication or **NTLM** authentication (Challenge response). To enable NTLM proxy authentication you check the **Use NTLM proxy authentication box** at the bottom.

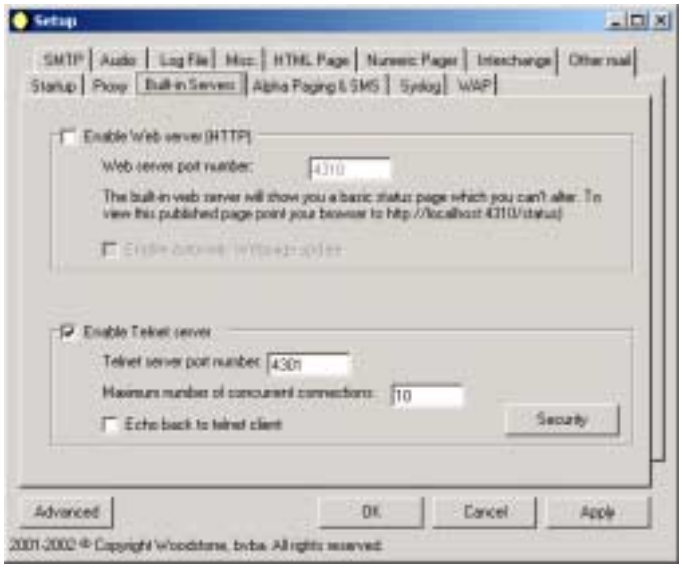


Proxy

Built-in Servers

Servers Alive has two built-in management servers, a web server and a telnet server. You can use these to remotely determine the status of all checked items, and issue some basic management commands.

If you enable the built-in web server it will publish a standard status page on the port you designate (the default is 4310). The default URL to use is http://hostname:portnumber/status (ex. http://networkchecker:4310/status). This web page cannot be altered beyond a few cosmetic changes. If you need to have a more detailed web page, or desire a different layout, please refer to the HTML Page section below. Note that the options on the HTML Page section do not apply to the built-in web server.



Built-in Servers

If you turn on the **Enable automatic web page update** option the web page will cause the browser to refresh itself every minute for an up to date view of the current checked status of all items. Note that this web page does not include any management options and is not password protected. If you need this sort of functionality you must use a third party web server.

You can use the following registry key to change the automatic update interval of the built-in web server (default is 60 seconds):
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\AutoUpdateHTTPInterval (string)

If you enable the telnet server and specify a port number (the default is 4301) you can interrogate Servers Alive via a telnet client (a client comes with Windows). Via a telnet client you can see a list of all hosts, their status and the last time the status changed. The list is ordered by status. You can also issue some commands that modify the behavior of Servers Alive. The telnet server supports multiple connections.

The telnet server understands the following commands:
RELEASE IP
Internally Servers Alive will convert all host names into IP addresses the first time they are used. This goes for the hosts you check as well as any SMTP servers that you use. If you want to release all of these IP addresses from memory while Servers Alive is running you can do this via the RELEASE IP command on the telnet interface.

START CHECKING
This command does exactly the same as pushing the START button on the main screen of Servers Alive.

STOP CHECKING

This command does exactly the same as pushing the STOP button on the main screen of Servers Alive.

SYST
Shows the build number of Servers Alive.

STATUS
Shows a list of all hosts and their current status.

STATUS DOWN
Shows a list of all hosts in a down state.

STATUS MAINTENANCE
Shows a list of all hosts in a maintenance state.

QUIT
Disconnects your telnet client from the telnet interface of Servers Alive.

HELP
Shows some very basic help on various telnet commands.

UPDATE
This command does exactly the same as pushing the UPDATE button on the main screen of Servers Alive.

MAINTENANCE x
Puts host **x** into maintenance mode. To get the number of the host issue a STATUS command and you will see the number of all hosts.

MAINTENANCE ALL
Puts all hosts into maintenance mode.

ACTIVE x
Puts host **x** into active mode. To get the number of the host, issue a STATUS command and you will see the number of all hosts.

ACTIVE ALL
Activates all hosts.

LOAD *filename*
This option does exactly the same as doing a FILE -> OPEN from the GUI.

RESET PAGER
This clears all pager queues.

RESET DOWN COUNTERS

This resets all down counters for all hosts.

RESET STATISTICS
This resets the statistics of all hosts.

SET ALL SOUND TO NONE
Sets all sound entries to none.

SET ALL SOUND TO DEFAULT
Set all sound entries to default (typically used when you add a sound card to your machine after you have configured Servers Alive).

SET ALL PRIMSMTPMESSAGE TO *xyz*
Sets all primary SMTP messages to *xyz*.

SET ALL ALTSMTPMESSAGE TO *xyz*
Sets all alternate SMTP messages to *xyz*.

ENABLE TEAM=<name of team>
Enables the named team.

DISABLE TEAM=<name of team>
Disables the named team.

By default telnet echo is not turned on. This means that what you type may not be visible on the screen as you type it, depending on the client you use and how it is configured. If you would prefer to turn character echoing on just check the **Echo back to telnet client** box.

You can provide some security to the built-in telnet server so that only approved personnel can issue administrative commands. You do this by clicking on the button labeled **Security**.

In the telnet access restrictions box your first option for securing the telnet server is to allow only certain IP addresses to connect. You can choose from two basic modes. Everyone is either granted or denied access by default, and then you add exceptions to the rule. If you choose to use this type of security you will most likely want to deny everyone access by default and then add in certain exceptions (by IP) for known good addresses. To add an IP address range specify an appropriate subnet mask.

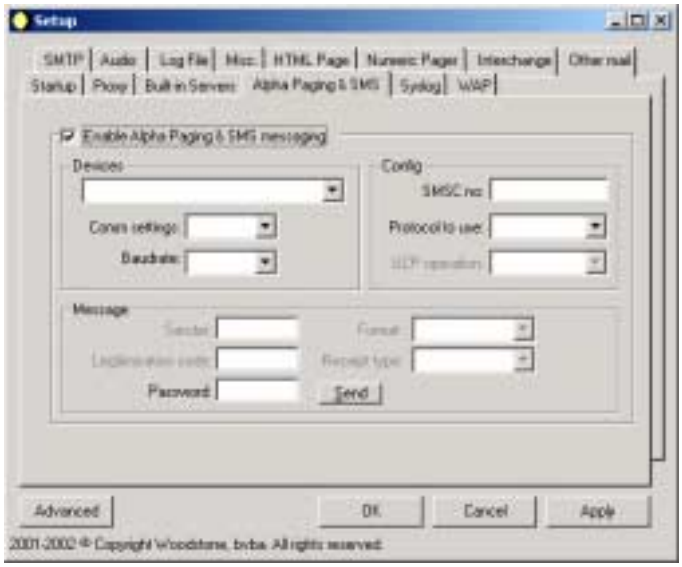
To add exception addresses click on the **add** button and supply the required information. To remove an entry select it and click on **remove**. You may also edit an entry that you have already added by selecting it and clicking on **edit**.

The other telnet security option you can use is password authentication. To turn this on choose **Password protected** and supply a username and password in the appropriate boxes. You can have two logins if you choose, one that has full control and one that can only retrieve the status of checked hosts. If you use this type of authentication keep in mind that the telnet protocol does not make use of any encryption. Any username and password you use will go out over the network in clear text, and may be intercepted. Plan accordingly. Note that you can use both types of security simultaneously.

Alpha Paging & SMS

One of the most common methods of alerting is alphanumeric paging. You can send small alerts to your alphanumeric pager detailing exactly what has gone down, often with collaborating information. To do this you must provide a modem device that will allow you to send alphanumeric pages. The actual paged device/number will be added on a host-by-host basis.

To turn on this feature check the **Enable Alpha Paging & SMS messaging** box. Next you have to configure the device that Servers Alive will use to send the message. Use the list under **Devices** to choose a modem. This drop down box will show any modems you have previously installed in Windows. If you have not installed a modem yet leave Servers Alive and install one first (via the modem applet in the control panel), then come back.



Alpha Paging & SMS

Once you have selected an appropriate modem you must supply the communication settings in the **Comm settings** box. Your paging/SMS provider must supply these settings, along with the protocol and SMSC. Please contact them for this information. There is an informal list that is maintained by Woodstone bvba with the various settings reported by users of Servers Alive for

providers around the world. You can find this list at http://www.woodstone.nu/salive/pagersettings.asp. Woodstone bvba takes no responsibility for the accuracy of the supplied information, but it may help you. In general, either *7E1* or *8N1* are good defaults to try.

The final option to choose is your **Baud rate**. Choose a setting that is appropriate for your service provider.

When you have finished entering your **Comm settings**, move over to the **Config** section. The first thing you need to know is the phone number of your provider's modem, or **SMSC**. You must also select the protocol used by your provider. This will be either TAP or UCP. If your provider uses UCP then there will also be another portion that you must specify, called a **UCP operation**. Again, you can look at the list at the above address for these pieces of information, but the information may not be listed for your provider or up-to-date. Please contact your provider for the correct information.

Finally you must present authentication information in the **Message** section. This is required by your provider in order to send a message. There are five pieces of information in this section, and, once again, you should get this information from your provider. In most cases the **Sender** box should be left blank, the **Format** is usually *ALPHA NUMERIC*, and the **Receipt type** will most likely be *GSM*. You may or may not need the **Legitimization code** and **Authentication code**.

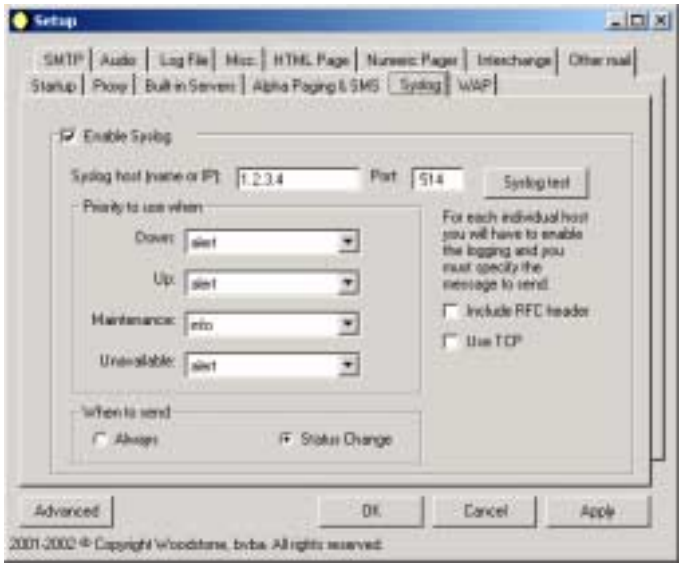
When you have entered the requisite information, hit the **Apply** button and then the **Send** button to test the information. If you have entered everything correctly you will receive a test page.

Note that in some rare cases the SMS message must be sent twice before it gets through. To enable this feature you must add/edit the following registry entry:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\Paging\DoubleMessage (dword) 1 or 0

Syslog

Syslog is a standard method of centralizing various logs. You can use a syslog server to store your Servers Alive logs in a remote location for later perusal or long-term storage. If you want to use syslog, there are various freeware syslog servers on the Internet, and since it is an established standard Servers Alive will work with any of them. For a Windows based syslog server we recommend Kiwi Syslog Daemon, available from http://www.kiwisyslog.com/.

You can enable syslog storage on the **Syslog** tab. You must provide an IP address and port for your particular syslog server. The port will be *514* unless you are using a non-default port number on your syslog server. When you have entered the server and port press **Apply** and then hit the **Syslog test** button. You will then be able to check the logs on your syslog server to verify that it is correctly logging events from Servers Alive.



Syslog

You can add RFC compliancy from within the syslog setup. This RFC compliant header adds some info to the message (date stamp of send - who did the send - name of process that does the send). It's also possible to send syslog message via TCP to the remote syslog server. Most of the time this is done on port 1468.

You can specify which particular events should be logged. You can also change the priority for the down, up, maintenance, and unavailable conditions. There are various levels to choose from, so pick whatever is most appropriate for your situation.

Finally, at the bottom, in the **When to send** section, you should choose whether to log an event on every check cycle, or whether to only log status changes.

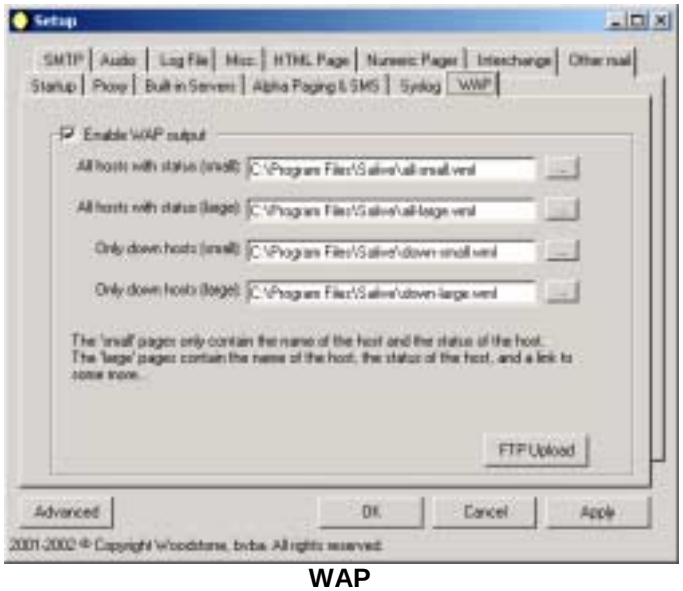
Please note that you must enable syslog logging for each particular host that you want to log. It is not turned on for every host by default. It is best to determine if you want to use this service before adding many hosts so that you can turn it on as needed as you add hosts.

By default the syslog messages sent by Servers Alive includes the process name "Servers Alive". This can be removed by adding/editing the following registry entry:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\SYSLog\WithoutProcess (dword)
Value of 1

WAP

Servers Alive is the first monitoring platform to support alerting via WAP (wireless access protocol) pages. If you have a cellular device capable of viewing WAP pages this can be a wonderful method of spot-checking your servers while on the road!

WAP alerting uses the concept of WML cards, which are like linked HTML pages, to allow you to choose the way you view Servers Alive's current status. There are four different page types that can be used. You can view a large or small page with either all hosts or just the hosts currently marked as down. A **large** page has an initial view showing the names of the hosts and their status, with a link to show their exact check description. Alternately you can use a **small** page that shows only the host names and their status. To enable one of the pages you type in a full file path, including file name, or you may hit the button on the right side of each location box and browse to the correct location.



WAP

Servers Alive can also upload these WML files to your web server using the FTP protocol. You can configure this via the **FTP UPLOAD** button. You will have to provide the needed FTP upload info, being the name of the FTP server, the username, the password and the remote directory. The general mode of operation for FTP uploads is to use the FTP PORT command, which asks the server to connect to the client (Servers Alive) and then accept data. This method may not work, however, for those behind a firewall. In this case you may optionally

choose to use **PASV** transfer, which allows the client to handle the connection setup for sending data to the FTP server. In either case Servers Alive will use the file names you specified in the various boxes for the file names on the ftp server.

Servers Alive does NOT provide any WAP access through its built-in web server. It only generates WML files that can be viewed via a WML enabled browser, typically a WAP enabled phone, through a third-party web server.

If you want to publish WML files via your own web server don't forget to add the needed MIME type to your web server. Some WML browsers need those to be able to show the downloaded WML files.

You will need:
Associated extension: WML
Content type (MIME): text/vnd.wap.wml

If you are using a large host file the *ALL - LARGE* WML file could become very big. On some WML browsers the size of a deck is limited. This is the compiled size of a deck, and since there is no direct link between the size of the source WML file and the size of the compiled WML file, it is very difficult to put a size limit within Servers Alive for the source WML file. Even worse, not all browsers have the same limit (apparently some don't have a limit).

Therefore we have decided that we are not going to put a limit within Servers Alive on the size of the WML file. If you encounter size problems with the all - large file within your browser we suggest that you use the *DOWN - ALL* WML file. In future version of Servers Alive you will have more control over what host should be in which WML file.

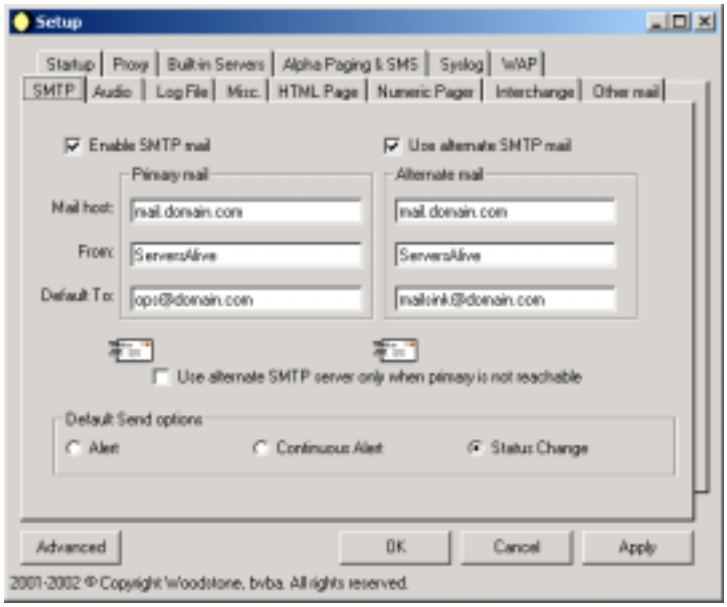
If you want to store your WAP page on a remote server that requires authentication you can use the following registry entries to supply the authentication information. The server listed here should be the same as the server listed in the GUI for WAP file storage.
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\WAP\Username (string)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\WAP\Password (string)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\WAP\Server (string)

The upload of WAP pages may give a "Busy executing command" error when several files have to be uploaded. By default Servers Alive will wait 100ms after the upload in order to give the socket the time to do a correct reset. If this is too much or to little time you can change the value via the registry:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\WAP\FTPSleepTime (dword) Max is 5000 (ms).

SMTP

Mail alerting is one of the most common types of alerting used. Servers Alive supports two different methods of sending mail: **SMTP** and **Other Mail**. You will most likely want to use the **SMTP** tab unless your mail server does not support SMTP or you have special mailing needs, in which case you should examine the **Other Mail** options.

The **mail host** can be filled in as a NetBIOS name, DNS name or IP address. (Ex. HERMES, mail.domain.com, or 123.45.67.89).



SMTP

The **From** field can be just a name or a fully qualified domain name (Ex. Servers Alive or serversalive@company.com). What you fill in will depend on the way your SMTP server is configured, but most SMTP servers want a FROM name that looks like a valid email address (something like salive@domain.com). If you have any trouble, please check with your mail server administrator for the proper setup.

The **To** field will always be a full email address (Ex. person@company.com)
If the message must be sent to several email addresses then separate them with a comma (ex. user1@company.com,user2@company.com).

The **Envelope** icon will send a test message to the specified user(s). Remember to push the APPLY button first, otherwise Servers Alive will use the old values for the test mail. The icon on the left tests the **primary mail** settings, while the icon on the right tests the **alternate mail** settings.

If the **Enable SMTP mail** is checked Servers Alive will send an SMTP mail with the list of all non-up services (except for the Status Change option where the UP

hosts will be included too if they just changed their status) hosts. If the **Use alternate SMTP mail** option is also enabled the mail will be sent to both SMTP recipients (the address can be on different servers).

The **Send options** are the defaults that will be used for each new host you create.

Alert: a mailing is sent when a host goes down (only one mail even if a hosts stays down for several check-cycles). The mail will include the list of all down hosts.
Continuous Alert: a mailing is sent as long as at least one host is down. If a host stays down for 25 check cycles you will get 25 mails with the list of down hosts.
Status Change: a mailing is sent when a host changes status. (Ex. from up to down, from down to up).

If you enable the **Use alternate smtp server only when primary not reachable** option, the alternate will only be used when the primary is unreachable. If you don't check this option, the mail will be sent via both smtp servers (if they are enabled).

Servers Alive will use your LAN (network) connection to send the mail to your SMTP server. Servers Alive can also do this via DUN (Dial Up Networking). This can be configured via the advanced setup.

Before sending a mail, Servers Alive will ping the SMTP server to see if it is responding. You can use the following SMTP\PingTimeout parameter to determine the amount of time Servers Alive should wait for a response (max. 32 sec). You can disable the mail server pinging entirely in Advanced setup.
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\SMTP\pingtimeout (dword)

There is another parameter called SMTP\Timeout that controls how long Servers Alive will wait for the SMTP server to respond. The default is 15 seconds, and the maximum is 60 seconds.
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\SMTP\timeout (dword)

If SMTP/ResolveAtStart equals 1 then Servers Alive will attempt to resolve the SMTP (and alternate SMTP) server name to its IP address when Servers Alive starts and use that from then on.
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\SMTP\ResolveAtStart (dword) 1 or 0

This key is used for any additional email footer additions. You can use **{saversion}** in the string to show the version of Servers Alive being used. This registry key is considered obsolete, and has been replaced by the PrimaryFooter key described further down in this section.
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\SMTP\CustomFooterMessage (string)

If ExcludeDateTimeInMail is 1, the generated SMTP mailings will NOT include the last line (Mail generated by ... date/time).
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\ExcludeDateTimeInMail (dword) 1 or 0

You can specify an alternate port (not 25) for the primary and alternate SMTP server by modifying the following keys:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\SMTP\PrimarySMTPPort (string)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\SMTP\AlternateSMTPPort (string)

You can use the following keys to add custom headers to any SMTP mail Servers Alive sends:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\SMTP\PrimaryXHeader (string)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\SMTP\AlternateXHeader (string)

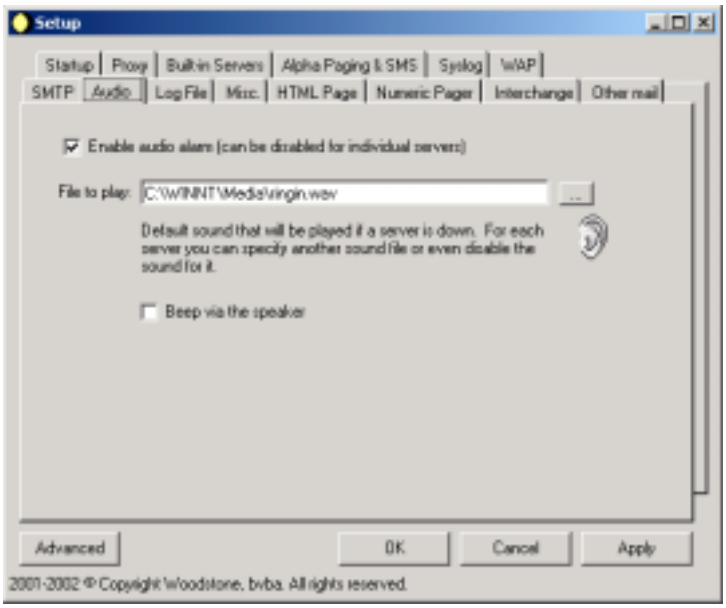
You can use the following keys to add custom footers to any SMTP mail Servers Alive sends:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\SMTP\PrimaryFooter (string)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\SMTP\AlternateFooter (string)

You can use the following variables in the PrimaryFooter entry:

{time}	hh:mm:ss format
{date}	
{stime}	hh:mm format
{saversion}	Servers Alive version number
{0d}	Carriage return character
{0a}	New line character

Audio

If you want Servers Alive to warn you of a failure with a sound click the **Enable audio alarm** and select the correct **file** to play. If there is no WAV capable device available you will not be able to check the **Enable audio alarm** checkbox. You can, however, still use some *sounds* as alarms by enabling the **beep via speaker** option. The filename you enter is the default that Servers Alive will use. You can change this on a per host basis.



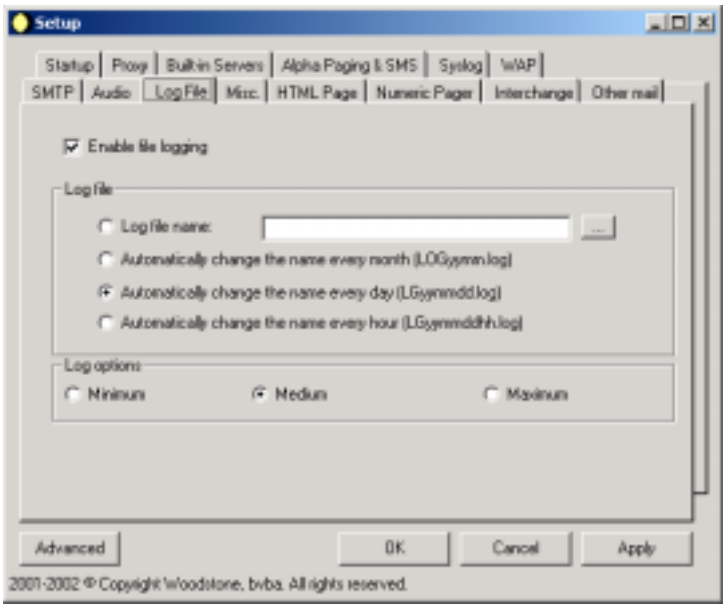
Audio

Servers Alive can now also play a sound when starting or stopping and as a proof that it is still alive. Therefore you must add/edit the following registry keys:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\KeepAlive\StartSound (string)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\KeepAlive\StopSound (string)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\KeepAlive\KeepAliveSound (srting)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\KeepAlive\KeepAliveSoundMinutes (dword)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\KeepAlive\KeepAlivewithSound (dword) 1 to enable

Log File

If you **enable file logging** Servers Alive will log all that it is doing into a log file. What will be logged can be changed with the **Log options**. If you want Servers Alive to log events into a fixed log file select the log file name option and fill in the name of the file to which the logging should be done (all new logging will be appended at the end of the file).

If you would prefer to have Servers Alive rotate your logs you can use the other logging options. If you want a file per month, select the **Automatically change the name every month** option. For a file per day, select the **Automatically change the name every day** option. For a file per hour, select the **Automatically change the name every hour** option. For these options the file will be kept in the same directory as Servers Alive.



Log File

Servers Alive will by default save the log file (all except the fixed name log) in the same directory as Servers Alive. This can be changed by adding/editing the following registry entry:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\Log\Path (string)

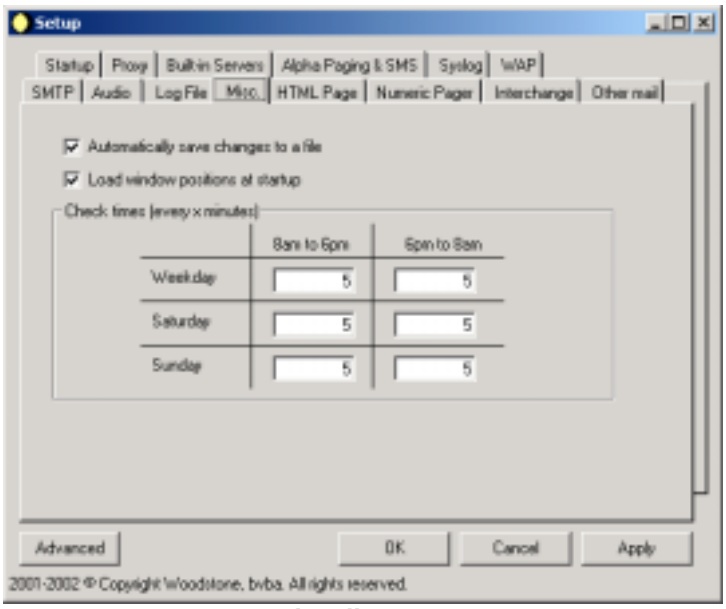
When performing a URL check with a "contains" clause, Servers Alive will save 150 bytes (by default) of the retrieved web page in the log file. You can however change how much is saved by changed by adding/editing the following registry entry:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\Log\HTTPBytesinLog (string) a value of -1 means the full web page (use this with care since your log file will grow very fast), a value of 0 will default back to 150 bytes.

If you want to safe guard the Servers Alive logs against missing data due to power failures or critical OS errors, you can request that Servers Alive close the log file after each write with the following registry entry:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\Log\CloseEachTime (dword)
Value 1 will force Servers Alive to close the log file after each write (not the default)

Miscellaneous

If the **Automatically save changes to a file** option is enabled all changes made to the current hosts configuration will be saved automatically. If it is enabled and you start a new set of hosts, you will be prompted for a filename when you quit Servers Alive.

If **Load window positions at startup** is enabled, Servers Alive will restore the last position on screen it had and also restore itself to the last known size it had on screen.



Miscellaneous

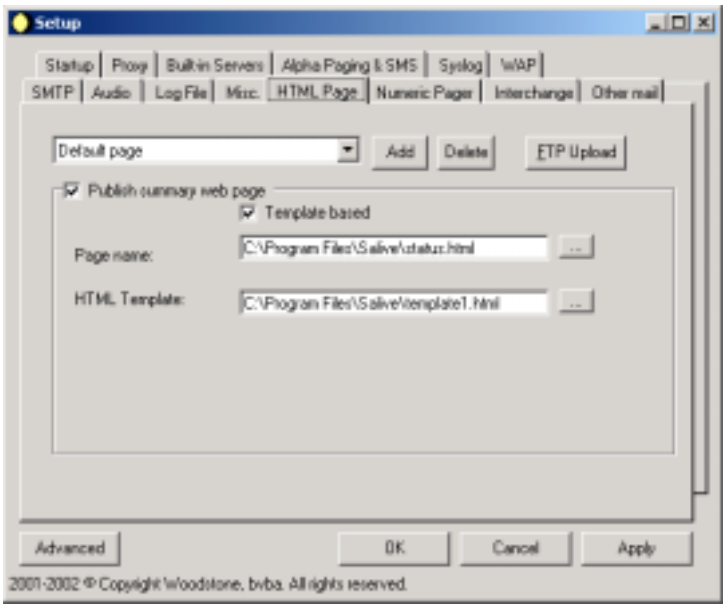
The **Check times** grid tells Servers Alive when to begin a check cycle on your list of hosts. If the value is 0 (zero) than no checking will be done in that time period. Saturday 6pm to 8am means from Saturday 6pm to Sunday 8am. The same logic holds for all others.

By default the morning starts at 8h (8AM) and the evening starts at 18h (6PM). You can change this by adding/editing the following registry entries:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\StartUp\MorningStart (dword)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\StartUp\EveningStart (dword)
Times are given in 24h format. 6pm would be 18.

HTML Page

When the **publish summary web page** option is enabled, Servers Alive will create one or more HTML pages after every check cycle. Each of these pages must be configured with a **display name**. This display name will be used when adding/editing a host entry and when you select which HTML page the host will be seen on. You must also specify the **page name**. The name must also include the directory in which the file will be created.

You can customize the web page by specifying a custom HTML **Header** page and HTML **Footer** page. You must also specify both the name and directory for these two files. Don't forget that they go in a pair! When creating the page, Servers Alive will copy the header, add the Servers Alive grid to it, and append the footer at the end.



HTML Page

By specifying the **look**, you can also customize the contents of the grid created by Servers Alive.

Technical: the grid will contain name, port number and pretty name.
Manager: the grid will contain the pretty name (and not the name and port number)

The grid always includes the current status and the time/date it detected that status. To publish this page on the internet/intranet you need a third-party web server.

Servers Alive can upload the page to your web server via FTP. Click on **FTP Upload** to enter the required info (hostname, username, password, remote directory and filename).

If the page must be on a remote machine and you need to get authenticated by this remote machine in order to get the rights to write on the remote machine's disk you can specify the username and password to use. To do this you must add/edit the following registry keys:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\Username (string)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\Password string)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\Server (string)

The upload of HTML pages may give a "Busy executing command" error when several files have to be uploaded. By default Servers Alive will wait 100ms after the upload in order to give the socket the time to do a correct reset. If this is too much or to little time you can change the value via the registry:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\FTPSleepTime (dword) Max is 5000 (ms).

For each of the different statuses that Servers Alive can display in the HTML pages, you can change the font type by adding/editing the following registry keys:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\UpFontStart
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\UpFontStop
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\DownFontStart
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\DownFontStop
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\MaintenanceFontStart
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\MaintenanceFontStop
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\UnavailableFontStart
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\UnavailableFontStop
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\UncheckedFontStart
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\UncheckedFontStop

Servers Alive will show the last check time just before or just after the table with the hosts. This can be configured by adding/editing the following registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\PlaceOfCheckTime (dword)
0 is below the table, 1 is above the table

You change the default size of the columns by adding/editing the following registry values:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\HostColumn (string)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\StatusColumn (string)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\SmallStatusColumn (string)
Example: "100" or "35%" or "AUTO"

To change the background color of the table of the generated HTML page you must add/edit the following registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\TableBackground (string)
Example: "#FF0000" or "Red"

By default Servers Alive generates *<TABLE BORDER="1">* as beginning of the table with the entry's statuses. Using the above table background property this already gives you the option to do *<TABLE BGCOLOR="tablebackground">*. By adding/editing the following registry value you are now able to do *<TABLE BGCOLOR="tablebackground" tableproperties>*
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\TableProperties (string)

If you want to see the number of times a host has been down since the last log filename change in the saved HTML file you must add/edit the following registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\Includedownstatus (dword)
with a value of 1

Servers Alive can replace the words UP - DOWN - ... in the HTML page by icons. To do this you must add/edit the following registry values:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\UpIcon (string)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\DownIcon (string)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\MaintenanceIcon (string)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\UncheckedIcon (string)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\UnavailableIcon (string)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\IncludeIcons (dword) when 1 the icons will be substituted for the normal words.

All the above registry settings can be used differently for all the pages that Servers Alive must generate. The default page uses
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\ as the root for its registry keys. A web page with a display name of WebServers uses

HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\WebServers\ as the root for its registry keys.

HTML Templates

If you choose to have Servers Alive generate an HTML page that is **template based** you have access to tools that allow you a higher degree of control over the final product. To use a template, you must first tell Servers Alive what the end result **Page name** will be, and then select the **HTML Template** to use. Servers Alive will read through the template after each cycle and use it to generate the end result page.

Basically a template has three parts, and supports a set of custom HTML tags that Servers Alive will replace on the fly with the associated information. The three parts are the header, core, and footer.

The header part is everything before the **<sa_report>** tag. The header is only interpreted once per page generation. Everything between **<sa_report>** and **</sa_report>** is interpreted for every host that must be on the page. The footer part is the part after **</sa_report>** and will also be interpreted only once. You can add an optional parameter to sa_report called **sort** that determines how the hosts will be sorted. To sort by status you would use **<SA_REPORT SORT=STATUS>**. To sort by the type of check you would use **<SA_REPORT SORT=CHECK>**. The default sort is that set in the GUI.

The interpretation of the header and footer part, will convert these tags to their current value:

- **<sa_currentlongtime>** - 1:32:07 PM
- **<sa_currentshorttime>** - 13:32
- **<sa_currentlongdate>** - Day, Month Date, Year (Monday, May 1, 2002)
- **<sa_currentshortdate>** - Day/Month/Year (5/1/2002)
- **<sa_version>** - ex. 2.1.952
- **<sa_cycles>** - Number of cycles since Servers Alive started
- **<sa_cyclestart>** - Date/time when the cycle started
- **<sa_cyclestop>** - Date/time when the cycle stopped

Note that **sa_currentlongtime**, **sa_currentshorttime**, **sa_currentlongdate** and **sa_currentshortdate** use the format that is defined within the international settings of the control panel of the Servers Alive computer.

Within the core section (between **<sa_report>** and **</sa_report>**) much more can be done. You can use the following tags in the core section:

- **<sa_hostname>**
- **<sa_prettyname>**
- **<sa_status>**

- **<sa_statuschangedate>**
- **<sa_statuschangetime>**
- **<sa_checkdescription>**
- **<sa_checkresponse>** - same as the %e parameter
- **<sa_hostid>**
- **<sa_uid>**
- **<sa_roundtrip>** - same as the %a parameter
- **<sa_threshold>**
- **<sa_stats_avgrtrip>** - average roundtrip time of all UP cycles
- **<sa_stats_maxrtrip>** - maximum roundtrip time of all UP cycles
- **<sa_stats_minrtrip>** - minimum roundtrip time of all UP cycles
- **<sa_stats_upcycles>** - number of UP cycles
- **<sa_stats_uptime>** - uptime as a percentage
- **<sa_stats_downtime>** - downtime as a percentage
- **<sa_stats_maintenancetime>** - maintenance time as a percentage
- **<sa_stats_nondowntime>** - consecutive uptime
- **<sa_stats_downcycles>** - number of DOWN cycles
- **<sa_stats_maintenancecycles>** - number of MAINTENANCE cycles
- **<sa_stats_totalcycles>** - number of total cycles
- **<saif>**

The most powerful tag is **<SAIF>**. SAIF allows you to include certain HTML code depending on the condition of the current host. SAIF is used as follows:
<SAIF variable IS value AND variable IS value>something</SAIF>
<SAIF variable IS value OR variable IS value>something</SAIF>
<SAIF variable NOT value>something</SAIF>

Note that an SAIF statement must be on one contiguous line. You can have many things inside the SAIF start and stop tags, but they must all be on one line (no line breaks).

The variables you can check are listed here along with their possible values.

- **SA_STATUS** – possible values are UP, DOWN, MAINTENANCE, UNAVAILABLE, and UNCHECKED.
- **SA_CHECK** – possible values are NETWARE, ORACLE, SQL, URL, DISKSPACE, PROCESS, SERVICE, PING, IPXPING, UDP, SNMP, WINSOCK, and EXTERNAL.
- **SA_HOSTNAME** – hostname of the entry.
- **SA_HOSTID** – ID assigned to entry.
- **SA_UID** – Unique ID assigned automatically to the entry by Servers Alive.

Examples:
<SAIF SA_STATUS IS DOWN>help us please it's down</SAIF>

<SAIF SA_STATUS IS DOWN AND SA_CHECK IS SQL>The SQL database is down, again.</SAIF>

<SAIF SA_CHECK IS ORACLE OR SA_CHECK IS SQL>A database.</SAIF>

<SAIF SA_CHECK IS URL OR SA_CHECK IS SERVICE OR SA_CHECK IS DISKSPACE AND SA_STATUS IS DOWN>Big alert. Houston we have a problem</SAIF>

<SAIF SA_HOSTNAME IS www.domain.com AND SA_STATUS IS DOWN>Might wanna update the resume, pal.</SAIF>

Note: the evaluation is ALWAYS done from left to right and case doesn't matter. Also, you can include quotes around the values, but they are not necessary.

If you would like additional information, and a starter template to work with you can download a zip archive with helpful information from: http://www.woodstone.nu/salive/doc/template.zip

If you choose to use the **sort=check** option in the **sa_report** tag you can specify a custom priority for the various check types. You edit the following registry entry and supply a string that lists the order of importance for all checks.
HKEY_LOCALMACHINE\SOFTWARE\DBU Consulting\Servers Alive\HTMLPage\CheckTypeSortOrder (string)

Ex. Default is WIPXSRDUQONME
(Winsock TCP (W) - Winsock UDP (I) - PING (P) - IPX Ping (X) - NT Service (S) - NT process (R) - Disk space (D) - URL (U) - SQL server (Q) - Oracle (O) - Netware (N) - SNMP (M) - External (E))

Example Template:

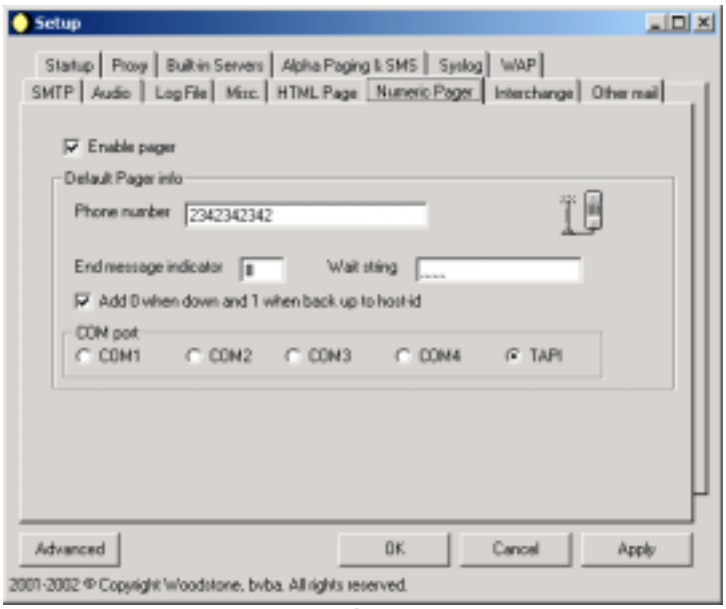
```
<!--This is the header section.-->
<BODY>

<!--Here the current date and time variables are used-->
<H4>Last check done on <sa_currentlongdate>   <sa_currentlongtime>

<!—Add in a comment that notes that Servers Alive generated the page.-->
<!-- Generator Servers Alive version <sa_version> via template.....->
<p>

<TABLE WIDTH="762" cellpadding="4">
<TR><TD WIDTH="32" align="center"><FONT face="verdana" size="2"><B>Up?</TD>
<TD width="20" align="center"><FONT face="verdana" size="2"><B>ID</TD>
<TD width="130" align="center"><FONT face="verdana" size="2"><B>Host</TD>
<TD width="280" align="center"><FONT face="verdana" size="2"><B>Host Check</TD>
<TD width="80" align="center"><FONT face="verdana" size="2"><B>Parameter</TD>
<TD width="70" align="center"><FONT face="verdana" size="2"><B>Actual</TD>
<TD width="145" align="center"><FONT face="verdana" size="2"><B>Time of Last
Status Change</TD>
</FONT>
</TR>

<!--The core section begins here.  It will be repeated for every host on the
page.-->
```

```
<sa_report sort=status>

<!--Use SAIF to change the color depending on whether the host is up or down.-->
<tr bgcolor="<saif sa_status is down>ff0f00</saif><saif sa_status is
up>dbdcaf</saif>">

<TD BGCOLOR="#ffffff">
<!--Use SAIF to display the correct icon (not supplied with Servers Alive)
 depending on the host condition.-->
<SAIF SA_STATUS IS UP><img src="images/running.jpg"></SAIF>
<SAIF SA_STATUS IS DOWN><img src="images/stop.gif"></SAIF>
</TD>

<TD WIDTH=20 BGCOLOR="#8fbc8f">
<!--Display Host ID with SA_HOSTID.-->
<CENTER><FONT SIZE=2><sa_hostid></FONT></CENTER>
</TD>

<TD WIDTH="145">
<!--Display Pretty Name with SA_PRETTYNAME.-->
<FONT FACE=verdana SIZE=1><sa_prettyname></FONT>
</TD>

<TD WIDTH="280">
<!--Display the type of check with SA_CHECKDESCRIPTION.-->
<FONT FACE=verdana SIZE=1><sa_hostname> (<sa_checkdescription>)</FONT>
</TD>

<TD WIDTH="80">
<!--Display check parameters iwth SA_THRESHOLD.-->
<FONT FACE=verdana SIZE=1><CENTER><sa_threshold></CENTER></FONT>
</TD>

<TD WIDTH="70">
<!--Display the response time/data with SA_CHECKRESPONSE.-->
<FONT FACE=verdana SIZE=1><CENTER><sa_checkresponse></CENTER></FONT>
</TD>

<TD WIDTH="175" valign="center" align="center">
<!--Display the time of the last status change with SA_STATUSCHANGETIME and
SA_STATUSCHANGEDATE.-->
<FONT FACE=verdana SIZE=1><sa_statuschangetime>, <sa_statuschangedate></FONT>
</TD>
</TR>

<!--End of the core section.-->
</sa_report>

<!--Beginning of footer.-->
</TABLE>

<BR>

<!--Display when the last check cycle occurred using SA_CURRENTLONGDATE
and SA_CURRENTLONGTIME.-->
<H4>Last check done on <sa_currentlongdate>   <sa_currentlongtime>
</BODY>
```

Numeric Pager

If you check the **enable pager** option Servers Alive can send you alerts via an attached modem to a numeric pager. In order to send you the alert, you must specify the **Phone number** of your numeric pager. You must also specify the **COM port** (in most cases **TAPI** will work best) to which your modem is attached. Remember that you will also have to enable paging on a host-by-host basis. By default you will not be paged for any hosts when a DOWN condition is

detected. Note that since numeric paging is not based on a standard protocol it is not considered as reliable as alphanumeric paging.



Numeric Pager

In most cases, after dialing the phone number of your pager, Servers Alive will have to wait several seconds before sending out the numeric information. This **wait** time can be entered as some number of commas (every "**,**" represents approximately 2 seconds). Also, after a numeric message has been entered, you need to specify an end-of-message indicator. This must be entered in the **End message indicator** box. Generally paging providers use # as the indicator.

You can test the pager by clicking on the **pager-icon**. Remember to push the apply button first, otherwise Servers Alive will use the old settings.

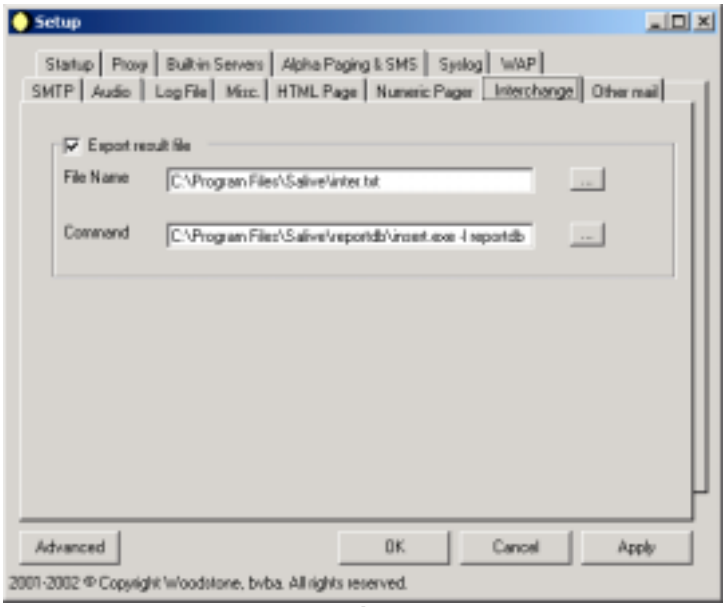
You can flag the **Add 0 when down and 1 when back up to host-id** option to receive extended information on your page. Servers Alive will add a -0 for a down-host to the host ID and a -1 for an up-host to the host ID. Since numeric paging is not based on any standard protocol this may be unreliable.

The message that you will get on your pager will show you a number. This number is the Host ID, which you can change when creating/editing a host.
If you enabled the **Add 0 when down and 1 when back up to host-id** option, Servers Alive will send a "-" (dash) between the host ID and the 0/1 (down/up).
You can change this if you add/edit the following registry value:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\Pager\Separatorstring (string)

Interchange

If you enable the **Export result file** option, Servers Alive will create an export file after each check cycle that contains the status of all hosts. You need to specify the filename (including the full path) to which the export file should be written. The file will be re-created on each check cycle, so you must gather the data after each cycle.

To do this you can specify a command that Servers Alive will execute after each creation of the export file. This is typically used to put the check information from the interchange file into a database for reporting purposes.



Interchange

Format of the interchange file:
UID, status, date (yyyymmdd), time (hhmmss), response time

Status can be:
1 – down
2 – possible down
3 – unavailable
4 – maintenance
5 – up
6 – unchecked
7 – possible unavailable

If instead of the UID (which is a unique ID that Servers Alive gives to each host entry and can't be changed) you want to see the host ID you should add the following registry value:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\Interchange\UseID
(string) with a value of 1

As a sample of what can be done with the interchange file a utility called ICF2DBF is included in the same directory as Servers Alive. This utility can be used from within Servers Alive to add the content of the interchange file to a Dbase III+ file. More info on this ICF2DBF utility can be found in the README.ICF file, that is also available in the same directory as Servers Alive.

NOTE: This sample application only works with the default interchange file format.

You can add several fields to the interchange file using the following registry value:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\Interchange\Fields (string)

You can change the default field separator using the following registry value:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\Interchange\Separator (string)
You can use "<tab>" to indicate a tab character.

To know what value to give to the "fields" registry entry you will have to do some calculation. Each possible field has a value. To arrive at the correct value to put in the registry you add the values for each field you desire. Below you find a table with the fields and values as well as an example of calculating the total field value.

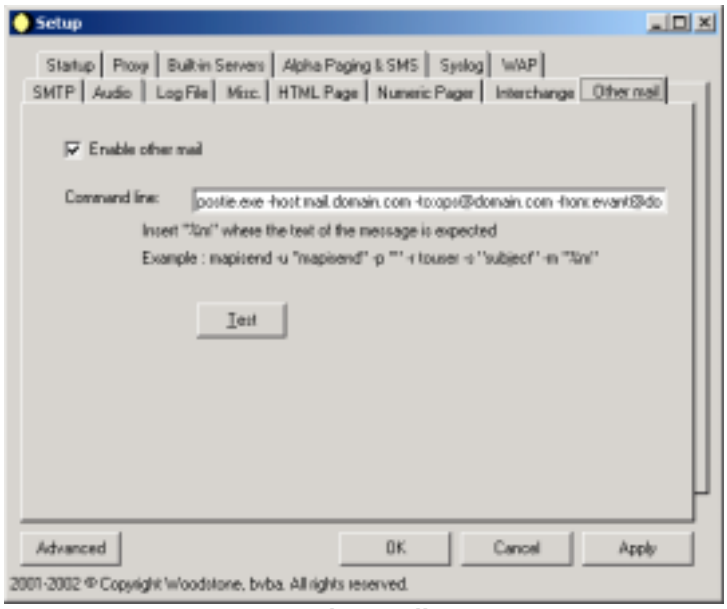
Field	Value
%h (hostname)	1
%p (pretty name)	2
%c (string containing check info, like in the dependency setup screen)	4
%e (extra info)	8
%a (additional info -> contains a timing value)	16
Number of cycles since Servers Alive started	32

Sample: Let's say you want to add the prettyname (%p) and the checking info string (%c) to the interchange file.

Pretty name (%p) = 2 and checking info string (%c) = 4. Therefore, the value of Fields (in the registry) must be 6 (2+4).

Other Mail

Servers Alive can natively send mail via an SMTP server. If you are not using an SMTP server Servers Alive can still send mail using your mail server if you have a command line mailer for your mail system. If you **Enable other mail**, Servers Alive will send mail using the command line mailer you specify.



Other Mail

In the **command line** you enter the command that Servers Alive will issue when sending mail via your command line mailer. Within the command line the %m will be replaced with the actual message that Servers Alive generates. If you push the **Test** button Servers Alive will send you a message using this command line. Remember to push the Apply button first; otherwise Servers Alive will use the old (or empty) values.

Servers Alive will use the send options of the SMTP mail to decide when to send a mail. Servers Alive will use the **defaultprimarymessage** registry key as template for the message (%m) that will be used in the **other mail** mailings. The default primary message registry key can be found at:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\SMTP\DefaultPrimaryMessage (string)

You can modify the message that Servers Alive sends by adding/editing the following registry value:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\OtherMail\OtherMessage (string)

Within this "othermessage" value you can use the following variables:

- %h for the host name
- %p for the pretty name
- %s for the status
- %t for the last check time
- %d for the date
- %u for the unique ID of the host
- %c for the complete host/check description
- %e for extra info (for a URL checking this could contain 404 Not Found as the error message)
- %a for additional info (for a ping check this will the round trip time)
- %i for hosted (used for numeric paging)

- {0d} for chr(13) – carriage return
- {0a} for chr(10) – line feed

If you want to force the case of the message to uppercase or lowercase only you will need to add/edit this registry key.
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\Othermail\ForceCase (string) U or L

Advanced

At the bottom of the normal setup dialog box is a button labeled **Advanced**. Advanced setup contains a few options for special tweaks dealing with SMTP, ESMTP, checking and DUN. The four tabs will be discussed individually.

SMTP

Servers Alive can send you an email every x minutes to prove it is still running. The mail will be sent using the default settings of the primary SMTP server. When Servers Alive starts/stops checking it can also send a email. Again using the settings of the primary SMTP server. Before sending email to an SMTP server, Servers Alive will ping the server and only send email to the server if it gets a response. If your server is not responding to pings (because a router or firewall filters out the ICMP packages) the email will not be sent. You can disable this ping-before-send feature to get around this. All email sent by Servers Alive is by default sent as *URGENT* email (being high priority). This can be changed for both primary and alternate email. Use the **SMTP** tab of **Advanced** setup to select these options.

Advanced SMTP Options

By default the keep-alive mailings are sent to the default primary mailto parameter. This can be altered via this key.
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\SMTP\KeepAliveTo (string)

Checking

When Servers Alive does a winsock check, it will (for all port/protocols that have a * displayed by them in the entry setup) check the return string for a correct (RFC compliant) response to indicate an UP condition. This can be disabled if your server/host is using non-standard responses.

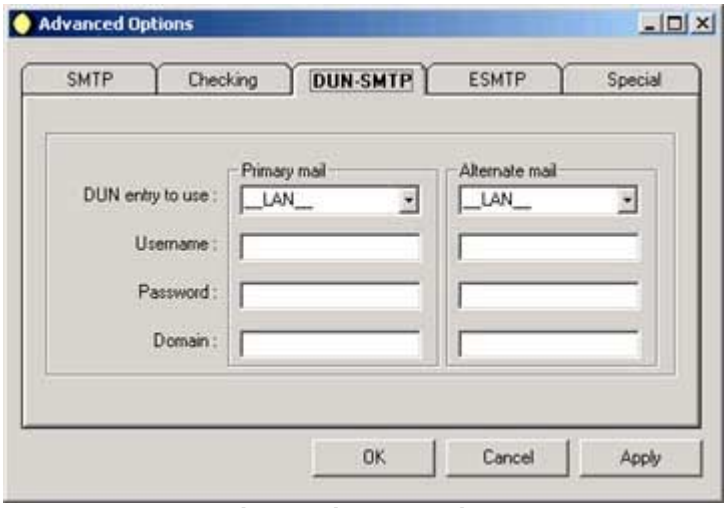
By default the ping packet size is 32 bytes. In some rare situations you may need to change this package size. An example for this would be wireless LAN connections.

When you stop the checking from the GUI Servers Alive can automatically restart the check (basically push the START button for you) after x number of minutes. This is helpful if you typically stop the check cycle to handle outages, and don't want to forget to re-enable it.

Advanced Checking Options

DUN-SMTP

When Servers Alive sends SMTP mail it will do this using your normal LAN connection (__LAN__). You can, however, force Servers Alive to dial into a remote network before sending mail to an SMTP server. To turn on this functionality you will first have to configure the correct DUN (dialup networking) settings in windows. Once you have done that you will be able to select them using the appropriate drop down boxes on the **DUN-SMTP** tab. If you need to provide a username, password, and domain to establish the connection you can enter them in the appropriate text boxes.

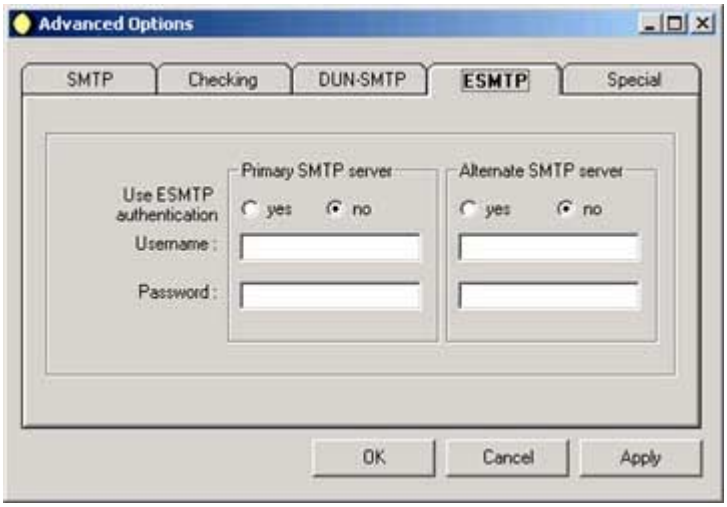


Advanced DUN Options

ESMTP

Many organizations do not allow standard SMTP connections for outgoing mail, as they can tend to be used by outside spammers to send unsolicited mail. Most have an option to use ESMTP, which forces a person to log in to the SMTP mail server before allowing that person to send any mail. If your company uses ESMTP you will need to supply a username and password combination for your primary and/or secondary mail settings to allow Servers Alive to send mail.

To use this simply select **yes** under the appropriate mail settings, and then type in the username and password combination.



Advanced ESMTP Options

Special

You can use the **Special** tab to edit your list of public holidays. These public holidays can be treated as a Sunday, rather than whatever day they actually fall on, when Servers Alive determines whom to alert. You turn that feature on when defining a person, as described below in the **Team Alerting** section.

The list of holidays should be in dd-mm-yyyy format, and should be separated by commas.

Adding and Editing Entries

Once Servers Alive has been configured properly you are ready to begin adding or editing entries. When adding or editing an entry you are presented with a host configuration dialog that allows you to specify what host should be checked, and what should be checked on that host. You can add new entries by clicking on the **Add** button at the bottom of the screen. You can edit entries by either selecting an entry and clicking the **Edit** button or double clicking on an entry (when not in a check cycle).

Server

Server name or IP(X) address should contain the name of the server or its IP address. If a name is entered it can be a NetBIOS name (server) or its fully qualified domain name (server.domain.com). Internally Servers Alive will attempt to resolve this name to its IP address on its first check cycle and then use that address from then on. If it has trouble resolving a name you may need to specify the host by IP address. For an IPX ping you will have to enter the IPX address of the server. If you enter an IPX address, enter the network address then a ":" and then the node address (example 352FBA2B:000000000001).

The **Pretty name** is only used for display purposes (in the GUI, Telnet client, email, HTTP/HTML output, etc.). You should enter a descriptive name that will instantly identify the machine and check to you when you receive it in a page or email.

The **Host ID** is the number used to identify the host when paging and in the interchange format. You don't need to enter anything in this field, as it will be automatically generated for you when you create the entry. You can change the Host ID to be more meaningful for you, however.

If a host does not respond within the **Timeout**, it is flagged as being DOWN. On slow links (WAN) this value should almost always be set to more than 5 seconds. In order to get the correct values for your network you will have to do some testing. The maximum value is 300 seconds; except for the ping check type where the maximum value is 32 seconds.

Second Knock: If a host is seen as down during a check cycle, and the second knock is enabled, it will be rechecked at the end of the check cycle to verify that it is down. This feature will come in handy if you are dealing with slow links or machines with slow responses.

Include this host in the check cycle: If a host will be down due to maintenance you can exclude it temporarily from the list of hosts that will be checked. The HTML report will show the host as being in MAINTENANCE. The fastest way to do this is via the GUI. You can select the entry, right-click on it, and then choose **maintenance** from the menu that appears. You can also put a host into maintenance mode via the telnet server.

Connect via: By default Servers Alive will connect to the host using the *normal* LAN connection (__LAN__), but Servers Alive can also make a dial-up connection to an *external* network before doing the check. After the check Servers Alive will disconnect from the external network.

This will only be available if DUN (Dial-up Networking) is installed on the machine running Servers Alive. To use this feature effectively Servers Alive must be able to make the connection completely unattended. For that reason, you must have the dialup entry save any necessary passwords.

HTML page: By default all host entries will be seen in the generated HTML file(s). If for some reason you don't want a host in one, (ex. your customers need to know if a server is up but not that there isn't enough disk space), you can exclude the host from the HTML file. You can also select the particular HTML file in which a host will be seen. Up to two pages can be chosen for each host. To create additional HTML files use the HTML Page tab of the SETUP.

Checks

After supplying the needed information for the **Server** tab you will need to select what type of check to use for the entry on the **Checks** tab. There are many different check options to choose from, and an **External** check option that allows you to write your own custom checks, but only one check can be used for each entry. If you want to do multiple checks on a server, you must have separate entries for each check you want. Each check type is discussed below.

For many checks and alerts a username and password are required for successful operation. This information is stored in the entry file you specified in an encrypted form.

Winsock

The winsock checks include any checks that make a basic connection to another computer over TCP/IP. This includes both TCP and UDP connections. TCP checks are used for things such as web and mail servers. UDP checks include things such as Radius servers, DNS servers, and various game servers. Starting in version 3 Servers Alive can also monitor CITRIX Terminal Servers via the UDP tab.

First select the protocol that applies to the check type you want (**TCP** or **UDP**) by selecting the appropriate tab along the bottom of the screen. You will see all the particular protocols that Servers Alive can understand. All protocols marked with an * will be checked using enhanced winsock checking, while the others will use normal winsock checking. While merely verifying that a port is open may be sufficient to monitor a service, you should be aware that it can cause odd logging on whatever server is being checked. Some services (ssh for instance) do not like it when computers connect and then immediately disconnect. For this reason you may see spurious warning in the logs regarding connections from the Servers Alive Server. This is not a problem, but it is something you should keep in mind.

Normal	Servers Alive connects to port x. If this can be done the entry is flagged as up. Servers Alive then disconnects from the port.
Enhanced	Servers Alive connects to port x and waits for returning data from the checked server. If the return is RFC compliant Servers Alive will flag the host as being up. Servers Alive then sends the "quit" command and disconnects from the port.

The enhanced winsock check sends an extra cr/lf pair after the actual connection. This is needed for some checks, such as an IIS SMTP server on the local machine. If you want to disable that use the following registry entry:
HKLM\SOFTWARE\DBU Consulting\Servers Alive\StartUp\NoExtraReturnForWinsock (dword)
Value of 1 disables.

Finally select the specific port/service you want to check. The most common ones have already been defined, along with their default ports, but if you want to check a TCP service that is not on the list or is using a non-standard port you can select the last option, **Other**, and then supply the port number. This is not possible for UDP connections, since there is no standard way to verify a UDP connection.

If you want to check a DNS server you will most likely want to use the UDP check, rather than the TCP check. The TCP check simply verifies that tcp port 53 is open. This can be a problem if there is an intervening firewall, and doesn't actually verify that the DNS server is working correctly. The UDP check will either query the server's status, or request an address resolution. You can find the UDP dns check in the drop down list.

The UDP check will query the DNS server for the address of www.woodstone.nu by default. If you want to have a different query sent you can modify the following registry entries:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\DNS\Host (string)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\DNS\RecordType (string)
RecordType can be A, NS, CNAME, SOA, WKS, PTR, HINFO, MINFO, MX, or TXT

By default the DNS query checks will show an up if the server sends a frame back, regardless of the contents. You can require at least one valid answer with the following entry:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\DNS\CountResponse (string)
Set to 1 for at least 1 answer.

You can also do IPv6 dns queries to servers that are IPv6 enabled. If the server is not enabled you will get an error and a down condition. The default query is for www.6bone.net as an AAAA record type. This can be changed by the following registry entry:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\DNS\Host_IPV6 (string) and HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\DNS\RecordType_IPv6 (string) Both are required.

Servers Alive supports checks for common game servers including Quake1, QuakeWorld Master, Quake 2, Quake 2 Master, Quake 3, Half-Life, Half-Life Master, Tribes, Tribes Master, Tribes 2, Unreal, Unreal Master, Hexen World, and Hexen 2. Note that if you are checking an Unreal server and specify port **x**, the check will actually be done on port **x+1**, since that is the normal communication channel for the server.

Thanks to Carl at www.dnagames.net for providing the information needed to provide the game server checks.

For the Radius checking (on the UDP tab), the default username is SAUser, the password is SAPassword, and the Radius shared-secret is SAShareSecret. These defaults can be changed via the registry (and are global settings).
Values to add/change are:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\Radius\Username (string value)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\Radius\Password (string value)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\Radius\SharedSecret (string value)

The SSH check (winsock port 22) sends a frame to the SSH server to let it know that this connection (although not a full SSH connection) is a friendly connection. The frame that you must send to the server to get this result is SSH version dependant. Set the following key to the appropriate protocol number to use in ssh checks:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\StartUp\SSH_Check_Version (dword) Use 1 or 2.

Ping

Servers Alive can ping a host using an ICMP network frame, which is a very basic way to determine if the computer and the network between the computer and the Servers Alive machine are functional. Servers Alive can also do a ping over the IPX protocol for Novell servers and clients. Servers Alive uses the functionality of the Novell Netware client for that, which you must install separately.

An **IPX ping** uses socket 9086 and the **IPX Diagnostic ping** uses socket 456. The IPX ping and IPX Diagnostic ping will only be enabled if the Novell Netware client is installed and if the hostname is entered as an IPX address. (Ex. 352FBA2B:000000000001)

By default Servers Alive only sends one ICMP frame to the remote host in an IP ping, but you can configure Servers Alive to send several ICMP frames to the remote server and to only flag a host as down when the rate of successful answers is less than x%. You can enable this advanced behavior by going into Setup and clicking on the **Advanced** button. Multi-ping settings are on the **Checking** tab.

This addresses a common problem when pinging a host across a WAN (or the Internet). Many network routers will drop ICMP packets when the networks become congested, since they are diagnostic in nature. These dropped packets may not indicate a failure, however, but rather network congestion.

A ping (IP) can generate the following error codes, which may be found in the log files:

```
IP_SUCCESS = 0
IP_BUF_TOO_SMALL = (11001)
IP_DEST_NET_UNREACHABLE = (11002)
IP_DEST_HOST_UNREACHABLE = (11003)
IP_DEST_PROT_UNREACHABLE = (11004)
IP_DEST_PORT_UNREACHABLE = (11005)
IP_NO_RESOURCES = (11006)
IP_BAD_OPTION = (11007)
IP_HW_ERROR = (11008)
IP_PACKET_TOO_BIG = (11009)
IP_REQ_TIMED_OUT = (11010)
IP_BAD_REQ = (11011)
IP_BAD_ROUTE = (11012)
IP_TTL_EXPIRED_TRANSIT = (11013)
IP_TTL_EXPIRED_REASSEM = (11014)
IP_PARAM_PROBLEM = (11015)
IP_SOURCE_QUENCH = (11016)
IP_OPTION_TOO_BIG = (11017)
IP_BAD_DESTINATION = (11018)
```

Windows (Tab labeled NT)

Servers Alive can do various checks specific to Windows NT and 2000. It can check NT services, process, and performance counters on local and remote machines. Keep in mind that if you are running Servers Alive as a service, and want to check a service, process, or performance counter on a remote machine, you must specify a username and password with sufficient rights to perform the check on the remote machine. You do this using the **username** and **password** boxes at the bottom of the dialog box.

In order for Servers Alive to do the various Windows NT/2000 specific checks it must have access to the remote server's NetBIOS ports. This could be a problem

if there are any intervening firewalls. Please consult with your firewall administrator to get the required access if this is the case.

First select the **NT service**, **NT process**, or **perfmon** radio button. If you select **NT service** then it simply checks to see if the service is running. You can click on the **List the available** services button, assuming you have entered a username and password, to get a listing of all services on the host.

If you select the **NT process** you can click **List the available** to get a list of the running processes on the remote machine. Double click on one to select it and return to the check dialog box. On the right side select the check condition. You can have Servers Alive alert you when there is **less than** or **at least x** number of the specified processes running. This is commonly used to alert when the Dr. Watson process is running (indicating an error).

Note that the process check is known to have a small memory leak. Each check cycle will consume approximately 40 bytes of memory per check. This is a permanent problem and is not subject to remedy at this point.

Servers Alive can only check for Windows NT processes if Servers Alive is running on a machine that runs Windows NT or Windows 2000. NT services can be checked from a Windows 95 or Windows 98 machine if the NT administration tools are installed on the machine and are available to Servers Alive (it will work best if they are installed in the same directory as Servers Alive).

The user performing the service check needs to have at least power-user rights on the machine that is checked. For the process checking you need administrator rights. This means that when Servers Alive runs within the context of user_1, user_1 must have power-user or administrator rights on the machine that is checked.

If user_1 hasn't got sufficient rights you can specify another username (this will in most cases be in the form domain\username) and password of a user with power-user or administrator rights on the machine that is checked.

The perfmon check sometimes fails (or gives weird values) due to timing issues with the performance counters retrieval DLL. By default the timeout is set to 1000ms, you can however change it by creating the following registry entry and giving it a value between 1 and 10000 (milliseconds). Remember it is in ms and the default is already 1000, so you should try it with numbers higher than 1000.
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\StartUp\PerfmonTimings (string)

The various Windows checks may return errors in the log. Some common errors follow:

5	Access denied.
53	The network path was not found.
1219	The credentials supplied conflict with an existing set of credentials.

1312 A specified logon session does not exist. It may already be terminated.
1323 The value provided as the current password is incorrect.
1324 The value provided contains values that are not allowed in passwords.
1325 The value provided does not meet the length, complexity, or history requirement of the domain.
1326 Unknown user name or bad password.
1327 User account restriction.
1328 Account logon time restriction violation.
1329 User not allowed to log on to this computer.
1330 The specified account password has expired.
1331 Account currently disabled.
1332 No mapping between account names and security IDs was done.
1722 The RPC server is unavailable.

Normally Servers Alive will de-authenticate at the end of any check cycle that incorporates authentication. If for some reason this does not succeed it can cause any subsequent checks to fail. To force an authentication disconnect before a check add the following registry entry:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\StartUp\DisconnectBeforeAuthenticationConnection (dword). Value of 1 turns this feature on.

If any error code found within this comma separated list occurs during the authentication phase SA will still see the authentication as being successful. This is not a guarantee that the check as such will pass too.
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\StartUp\AuthenticationErrorIgnoreList

Space

Servers Alive can check if there is enough disk space left on a specific Windows network share. The name of the resource must be given as **\\server\share**.
Servers Alive will send you an alarm when the free space is less then x.
X can be given as:

- 25 meaning 25 Bytes
- 25 kb meaning 25 Kilobytes
- 25 mb meaning 25 Megabytes
- 25 gb meaning 25 Gigabytes
- 25 tb meaning 25 Terabytes

You can also use percentages in your disk checks. If you want an alarm when less than 5% of the disk space is available, then use "**5 %"** in the text box. The space between the number and the percent sign is very important.

The exact byte value of kb/mb/gb/tb can be changed in the registry.
Values to add/change are :
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\diskspace\kb (string value)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\diskspace\mb (string value)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\diskspace\gb (string value)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\diskspace\tb (string value)

The user performing the check needs to have the right to access the share that is checked. This means that when Servers Alive runs within the context of user_1, that user_1 must have access rights on the share that is checked. If user_1 hasn't got this right, you can specify another username (this will in most cases be domain\username) and password of a user that has access rights on the share that is checked.

By default Servers Alive will choose the next available drive letter to connect with when doing a disk space check. You can, however, force Servers Alive to use a specific one if you choose.
HKLM\SOFTWARE\DBU Consulting\Servers Alive\StartUp\ForcedDriveLetter (string value)

When doing a disk space check the %e parameter contains the actual free space on the share that is checked. If the compare value is given in MB then the %e parameter is also in MB. However, if the compare value is given as a percentage then %e is in bytes. You can now control how %e is returned when checking by a percentage by editing this registry value:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\DiskSpace\PercentageMeasure (string)
possible values: KB MB GB TB (default MB)

URL

Servers Alive can do a URL (Universal Resource Locator) check based on the HTTP (web), HTTPS (secure web), MMS (Microsoft media server), or RTSP (streaming audio) protocol. Servers Alive supports the use of cookies.

A URL should be something like:

- http://www.mydomain.com/sub-dir/page.html
- https://www.mydomain.com/sub-dir/page.html
- rtsp://stream.mydomain.com/sub-dir/streamingaudio.rm
- mms://stream.mydomain.com/sub-dir/stream.asf

For both the HTTP and the HTTPS check Servers Alive can also check if the content of the retrieved page is correct or not. To use this functionality you must use the **should contain** or **shouldn't contain** clause in combination with a word/sentence that should/shouldn't be in the retrieved web page.

In the content check string you can have a portion that is dynamic based on the current date. To do this, add a string that is surrounded by { and } and contains some of the following key words:

dd	day
mm	short month (01)
yy	short year (02)
Mmmm	long month (January)
yyyy	long year (2002)

For instance, “{dd-mm-yy}” would translate to “22-01-02”, and “{dd Mmmm yyyy}” would translate to “22 January 2002”.

For both the HTTP and the HTTPS check Servers Alive can connect to the remote server using a proxy server. This proxy server is defined in the Proxy tab of the setup.

Please note that the only authentication Servers Alive supports for URL checking is basic authentication. The other common method, NTLM, is undocumented and non-standard, so it is not supported.

When Servers Alive does the “contains” check, it does this in a case-sensitive way. This can be changed by adding/editing the following registry value:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\StartUp\URLContentInsensitive (dword)
1 = case insensitive
0 = case sensitive (default)

If you want to specify a different user agent string you can add/edit the following registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\Proxy\UserAgent (string)

The Securityflags key controls how Servers Alive responds to various SSL certificate problems. By default it maintains the maximum secure response to SSL certificate issues and may cause checks to fail. You can change the Securityflags key to vary this response.
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\StartUp\Securityflags (dword)

The following flags are defined (specified in hexadecimal notation). They can be or-ed together to exclude multiple conditions. It is important that the values be entered as hex values.

&H00000001	Ignore time validity status of certificate.
&H00000002	Ignore time validity status of CTL.
&H00000004	Ignore non-nested certificate times.
&H00000010	Allow unknown Certificate Authority.
&H00000020	Ignore wrong certificate usage.
&H00000100	Ignore unknown certificate revocation status.
&H00000200	Ignore unknown CTL signer revocation status.
&H00000400	Ignore unknown Certificate Authority revocation status.
&H00000800	Ignore unknown Root revocation status.
&H00008000	Allow test Root certificate.
&H00004000	Trust test Root certificate.
&H80000000	Ignore non-matching CN (certificate CN not-matching server name).

DB

Microsoft SQL server

Servers Alive can check for the availability of a Microsoft SQL server database. To perform this check, it uses the functionality provided by the Microsoft SQL client, which you must install separately. Servers Alive supports Microsoft SQL 6.5, 7.0 and 2000 clients. The SQL 2000 client will be seen as SQL7.

When you want to check a MS SQL database you must provide the name of the **database**, the **username**, and the **password** that will be used to connect to the database. The SQL server's name is the hostname. If you have both multiple clients installed you can select which client Servers Alive should use.

Oracle server

Servers Alive can also check the availability of an Oracle database. To do this it uses the Oracle OLE object, which is part of the Oracle client. Servers Alive supports Oracle 7, Oracle 8 and Oracle 8i, and Oracle 9i clients. With Oracle 9i you will need to install the "Oracle Windows Interface" included with Oracle. In most cases a full install of the Oracle client is needed. When you want to check an Oracle database you must provide the name of the **database**, the **username**, and the **password** that will be used to connect to the database.

The database name is a name that is defined within the TNSNames.ora file. For more information on how to configure entries in the TNSNames.ora file please consult your Oracle documentation.

Netware

Servers Alive can check several parameters on your Netware server. For these checks it uses the functionality of the Novell Netware client. If this client is not installed the Netware check options will not be available.

Servers Alive can check:

- The number of active connections on the Netware server
- The CPU utilization of the Netware server
- The number of mounted volumes

You can configure Servers Alive to alarm you when the returned number is below (<), above (>), equal to (=), or different from (<>) a base-value.

The Netware checking will only give a valid result when you are currently connected to the Netware server you are checking.

SNMP

Servers Alive can check the status of a device/host via the Simple Network Management Protocol (SNMP). It will check if a certain **OID**:

- is less than
- is greater than
- is equal to
- is different from (<>)
- contains a value
- doesn't contain a value

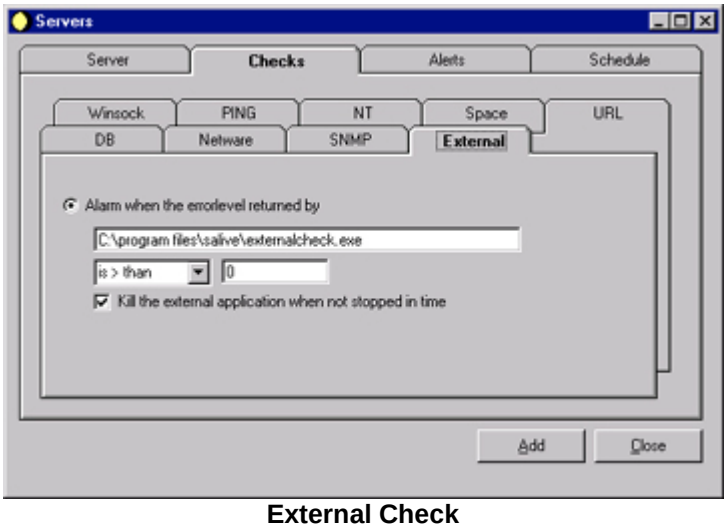
You will have to enter the community string for the SNMP check, for authentication purposes. By default on most SNMP systems this is PUBLIC, but it can be different on your systems.
Servers Alive can, within one check, retry several times to get an answer from the host.

To get a list of valid OIDs for your SNMP enabled devices you should contact the vendor of the device. They should be able to give you a MIB file that contains all the OIDs for the device.

External

Servers Alive has a lot of built-in check types, but Servers Alive can't support all possible check types. To extend the functionality of Servers Alive you can use the **external check** option. With an external check, Servers Alive uses an external application to perform an action and, based on the returned errorlevel, will flag the host entry as being up or down.

If the external application hasn't returned an errorlevel to Servers Alive within the given timeout, Servers Alive will flag the host entry as down. The external application will, however, continue to run. Servers Alive can, in such a situation, kill (shut down) the external application after the timeout has expired. To do this select the **Kill the external application when not stopped in time** option.



External Check

Within the command line that Servers Alive must execute for this external check you can use the following variables:

- %h for the host name
- %p for the pretty name
- %s for the status
- %t for the last check time
- %d for the date
- %u for the unique ID of the host
- %c for the complete host/check description
- %e for extra info (for a URL checking this could contain 404 Not Found as error message)
- %a for additional info (for a ping check this will the round trip time)
- %i for hostid (used for numeric paging)
- {0d} for chr(13) – carriage return
- {0a} for chr(10) – line feed

If you want to test an external check that you wrote without the use of Servers Alive you can use **checkerrorlevel.exe**. This small tool is installed by the Servers Alive setup program in the Servers Alive directory. It will run your application and show you the errorlevel your application returns.

Alerts

Servers Alive supports a rich variety of alerting mechanisms. It supports various email alerting options, numeric and alphanumeric paging, audible alerts, and more. You can even write your own custom alerting software, or use built-in Windows messaging to send popup alerts. Servers Alive is also capable of taking remedial action when it determines that a server is down, by executing scripts of your devising. Finally, it allows you to easily collect alerting events in a central logging server by use of the standard syslog logging mechanism available on Unix and Windows servers (with third-party software). You can select one or more of the following alerts.

Many of the alerts incorporate keywords to describe a server's state. By default it uses the words "up" and "down", but this can be changed via the registry. Under HKLM\SOFTWARE\DBU Consulting\Servers Alive\Status will be a list of single letter keys. Each letter corresponds with a particular check type, as follows:

D – Drive Space
E – External check
F – Perfmon
I – UDP
M – SNMP
N – Netware
O – Oracle
P – Ping
Q – MS-SQL
R – Process
S – Windows Service
U – URL
X – IPX Ping
W – Winsock port (TCP)

Under each of the single letter keys you will find numbered string values. Each one of these represents a particular status keyword, as follows:

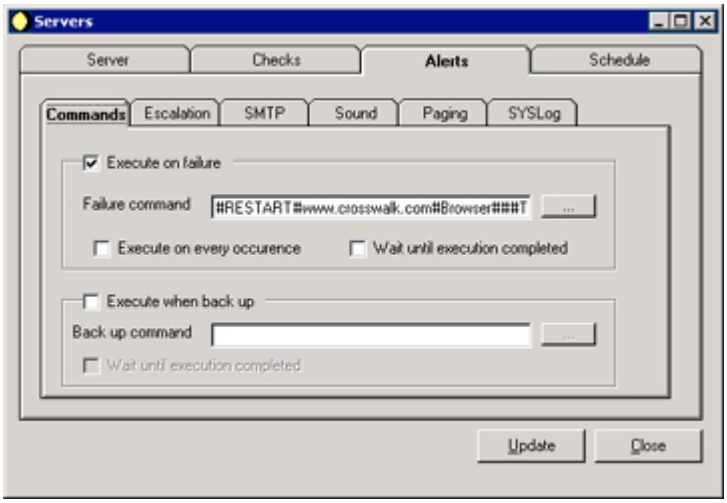
1 – down
2 – possibly down
3 – unavailable
4 – maintenance
5 – up
6 – unchecked
7 – possibly unavailable

If you wanted to have Servers Alive use "-" and "+" instead of "down" and "up" for all pings, you would set the following registry entries:
HKLM\SOFTWARE\DBU Consulting\Servers Alive\Status\P\1 = "-" (string)
HKLM\SOFTWARE\DBU Consulting\Servers Alive\Status\P\5 = "+" (string)

Commands

Use the commands tab to have Servers Alive execute the command of your choice whenever the check status is down. You first check the **Execute on failure** box to enable command execution, and then push the button on the right of the text box. This will launch the command selector window. You can enter three different types of commands:

- A normal command: this can be a BAT or EXE file. You must include the full path to the BAT or EXE.
- Restart of a Windows service, even if you are not checking an NT service. You can specify a user name and password to use to restart this NT service in the boxes provided.
- Reboot a Windows machine. You can specify a user name and password to use to reboot the Windows machine.



Commands

In order to use the **reboot** and **restart service** options Servers Alive must have sufficient rights (in the form of a username and password) and access to the NetBIOS ports of the remote machine. If there is a firewall between Servers Alive and the remote server please contact your firewall administrator for assistance.

Servers Alive will execute this command each time host is down if the **Execute on every occurrence** option is selected. Servers Alive can also **wait until the execution is complete** before doing anything else. Servers Alive can also issue a command (same rules as above) when a host comes back up (after a down situation).

When entering the command to execute you may need to pass in various pieces of information to the command you are executing that identify what has broken. You can use the following variables in your command. They will be replaced with the associated information before the command is issued.

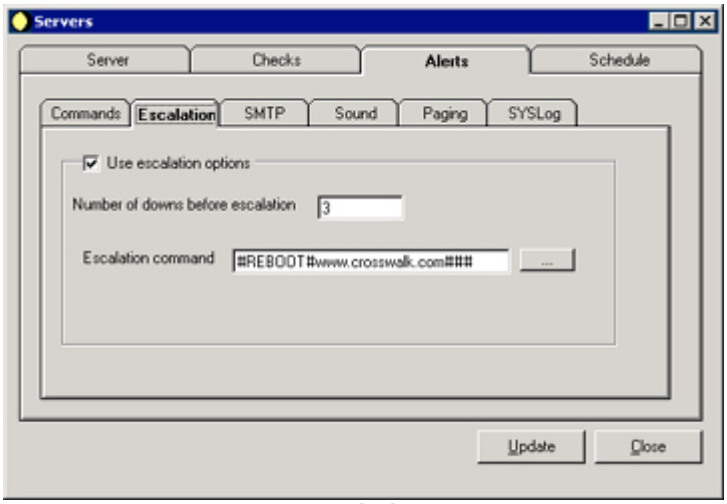
- %h for the host name
- %p for the pretty name
- %s for the status
- %t for the last checktime
- %d for the date
- %u for the unique ID of the host
- %c for the complete host/check description
- %e for extra info (for a URL checking this could contain 404 Not Found as error message)
- %a for additional info (for a ping check this will the round trip time)
- %i for hostid (used for numeric paging)
- {0d} for chr(13) – carriage return
- {0a} for chr(10) – line feed

Servers Alive will put in the logs that a reboot was successful as long as it was able to send the reboot command successfully. It does not verify that the machine actually reboots correctly. If part of the OS does not respond correctly it may not reboot despite receiving a reboot command.

Escalation

Occasionally you will need to have Servers Alive take further action on every cycle that a server stays in a down state. Perhaps you would have Servers Alive try to restart a service when it first detects a down condition. Then, if it remained down for another couple of check cycles, you could have it try to reboot the computer. This sort of setup can be accomplished by using the Escalation tab of the Alerting section. If you want to have more than two escalation steps, you will need to have multiple host entries.

You check the **Use escalation options** box to enable escalation options, enter the number of check cycles that must continue to show a server as down, and then a command. The command is entered by first pushing the button on the right of the text box then selecting the desired action. Follow the rules given in the **Commands** section above.

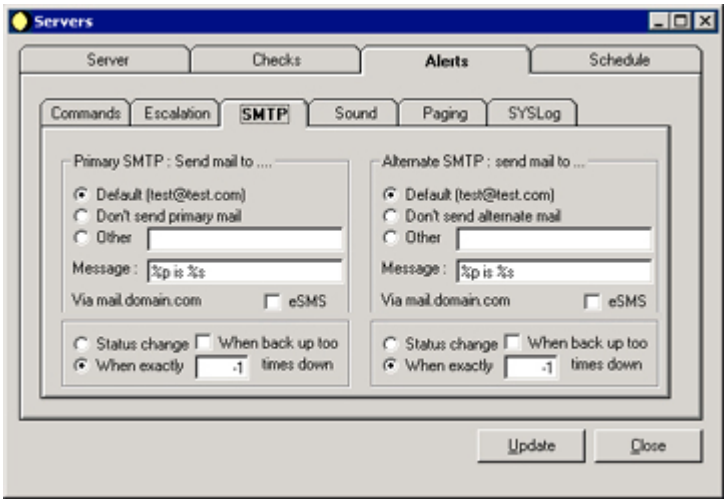


Escalation

SMTP

SMTP alerting is probably the most common alerting used. SMTP (Simple Mail Transfer Protocol) is used to send email messages to you when a down condition is detected. It is recommended that you use this as a minimum level of reporting. The SMTP option will only be enabled if you configure the global SMTP options from the SMTP tab of the SETUP.

You can give a primary and an alternate list of recipients for each host. If the message must be sent to several email addresses you can separate them with a comma (ex. user1@company.com,user2@company.com). Note that you must provide the global SMTP settings for both primary and alternate SMTP entries in the **SMTP** tab of the SETUP before you can enter any individual host settings.



SMTP

For both primary and alternate mail you can select when Servers Alive sends you a message, choosing either when the status changes or when a host is down

exactly N times. If you choose to receive an email when the host is down N times, but also want one when it comes back up, you must select the **and when back up too** option.

If you want to receive email notifications when the server has been down N times, and every subsequent cycle where it continues to stay down, then put –N in the text box. For example, if you want to have Servers Alive page you when a server has been down 3 cycles, 4 cycles, 5 cycles, etc., then you'd put –3 instead of 3 as the number.

It is up to you to specify the message Servers Alive will send. You can use the variables listed below to help you create informative messages. The message and subject can contain these variables:

- %h for the host name
- %p for the pretty name
- %s for the status
- %t for the last checktime
- %d for the date
- %u for the unique ID of the host
- %c for the complete host/check description
- %e for extra info (for a URL checking this could contain 404 Not Found as error message)
- %a for additional info (for a ping check this will the round trip time)
- %i for hostid (used for numeric paging)
- {0d} for chr(13) – carriage return
- {0a} for chr(10) – line feed

With the eSMS option the messages sent by Servers Alive will be shorter. People who use an SMTP to pager gateway typically use this option.

You can change the default message via the registry. You can add/edit the following entries:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\SMTP\DefaultPrimaryMessage (string)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\SMTP\DefaultAlternateMessage (string)

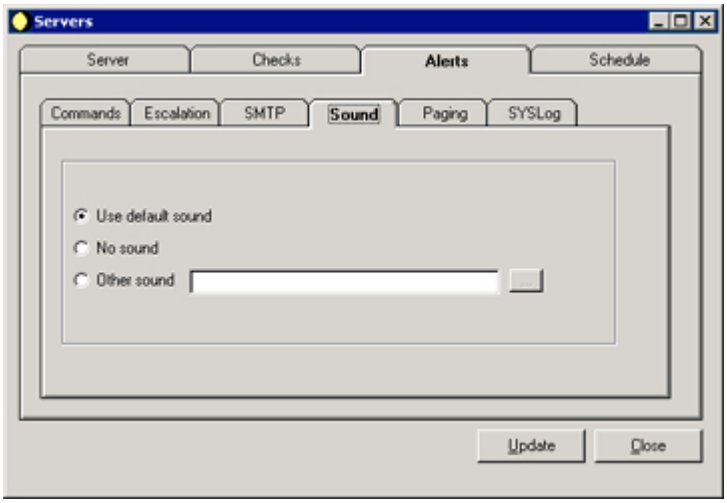
You can also change the subject of the mails send by Servers Alive via the registry. You can add/edit the following entries:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\SMTP\PrimarySubject (string)
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\SMTP\AlternateSubject (string)

You can add a custom footer message to all messages sent by Servers Alive. To do this add/edit the following registry entry:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\SMTP\CustomFooterMessage (string)

To remove the date/time from the mails you must add/edit the following registry entry:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\ExcludeDateTimeInMail (dword) value 1

Sound

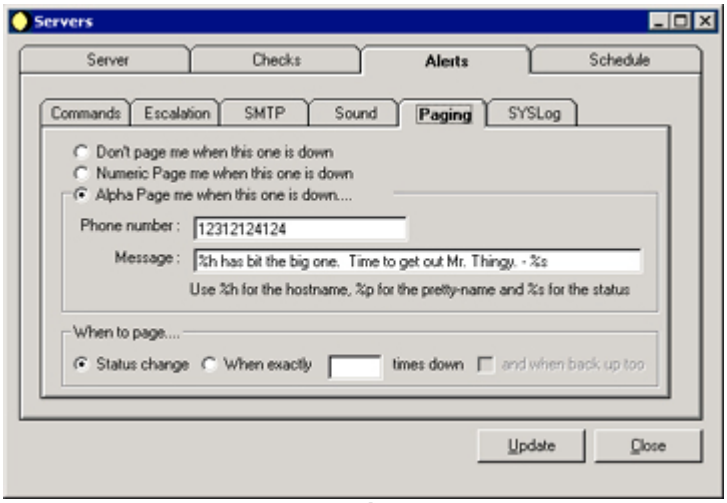
If you have the Servers Alive monitoring server near your operations staff you can use audible alerts to tell them that something is down. If you have provided a default sound in Setup then you can just choose to use the **default sound**. Otherwise you can use the **Other sound** option to choose a wav file on the computer.



Sound

Paging

Paging is another common alerting method. This important alerting option allows you to receive numeric or alphanumeric pages whenever a server is down. Before you can turn this option on for any entries you must have first configured paging in Setup.



Paging

Since numeric paging is not based on a real protocol it is not considered a 100% reliable solution. Numeric paging will use the settings that are defined in the **Numeric Paging** tab of Setup. The message that is sent to the pager is the host ID, which can be defined on a host-by-host basis. You can also, optionally, have Servers Alive send an up/down code. You can turn this on in the **Numeric Paging** tab of Setup.

The other option is **Alphanumeric paging** or **SMS messaging.** In order to send a page to your pager/GSM, Servers Alive needs the phone number (or PIN number) of the pager/GSM. You must also specify the message that Servers Alive will send to the pager/GSM. This message can contain some variables (see below). If you want to specify multiple recipients, separate them with a semicolon.

Servers Alive can page you on **status change** or when a host is down exactly N times. If you want to get paged from the Nth time on for each down situation then you should enter -N. Some people would prefer to get paged when the host is down seven times, but also when back up. For this you must select the **and when back up too** option.

The **message** can contain some variables:

- %h for the host name
- %p for the pretty name
- %s for the status
- %t for the last checktime
- %d for the date
- %u for the unique ID of the host
- %c for the complete host/check description
- %e for extra info (for a URL checking this could contain 404 Not Found as error message)
- %a for additional info (for a ping check this will the round trip time)
- %i for hostid (used for numeric paging)
- {0d} for chr(13) – carriage return
- {0a} for chr(10) – line feed

Servers Alive will queue pages if several have to be sent, but it will only send one page at a time. So if there are three pages in the queue, Servers Alive will connect to the paging company for the first page, send the page, disconnect from the paging company, re-connect to the paging company, send the second page, disconnect...

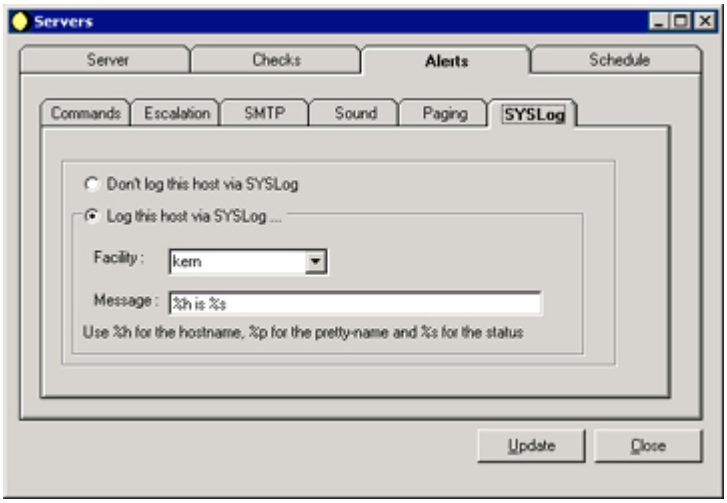
Servers Alive will wait by default ten seconds between each page it sends (if there are any left in the queue) to allow the paging hardware to reset if necessary. This timeout value can be changed by adding/editing the following registry key with the number of seconds to wait:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\Paging\Waittime (dword)

The default message that Servers Alive will present you when creating a new host entry can be defined via the registry. To turn on this feature you must add/edit the following entry:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\Paging\DefaultPagerMessage (string)

The default phone number that Servers Alive will present you when creating a new host entry can be defined via the registry. To set this number edit the following registry entry:
HKEY_LOCAL_MACHINE\SOFTWARE\DBU Consulting\Servers Alive\Paging\DefaultPagerPhoneNumber (string)

Syslog

If you want to collect all of the up/down events that Servers Alive detects into a centralized logging server, you can use the Syslog alerting option. Syslog is a standard method of sending alerts to an alerting server, and free server implementations exist for both Windows and Unix platforms. For a Windows based syslog server we recommend Kiwi Syslog Daemon, available from http://www.kiwisyslog.com/.



Syslog

For each host you can separately select whether to log it to the Syslog server. If it should be logged you must also give the message that Servers Alive will use. This message can use the following variables:

- %h for the host name
- %p for the pretty name
- %s for the status
- %t for the last checktime
- %d for the date
- %u for the unique ID of the host
- %c for the complete host/check description

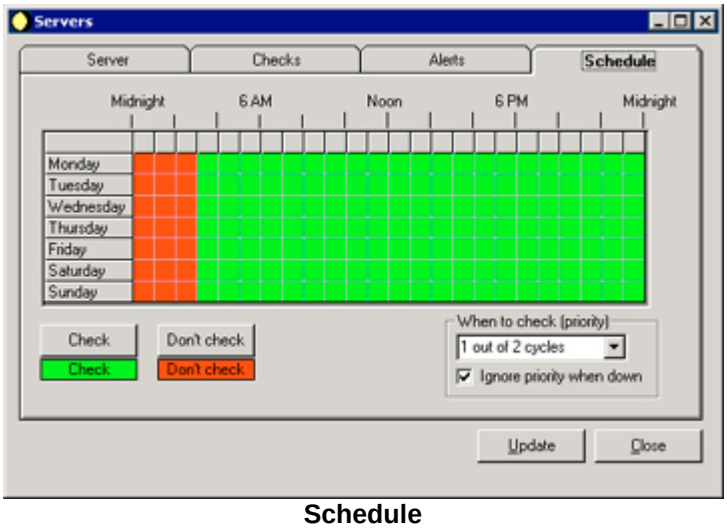
- %e for extra info (for a URL checking this could contain 404 Not Found as error message)
- %a for additional info (for a ping check this will the round trip time)
- %i for hostid (used for numeric paging)
- {0d} for chr(13) – carriage return
- {0a} for chr(10) – line feed

You must also tell Servers Alive which **facility** to use when logging to a Syslog server. For most the **kern** facility should be fine. If not, check with your Syslog server documentation to determine the best setting.

Scheduling

Many servers have a designated period of time during the week when they are unavailable. These are generally times for scheduled maintenance or backups. Instead of manually changing each host into maintenance mode every time it needs to be maintenanced, you can set up a schedule to tell Servers Alive when it should start and stop checking a host. You do this via the schedule tab.

To change the schedule you must first select a time. Each block represents an hour. You may not select a finer time scale than an hour. Use the mouse to click-drag select the hours you want to change to **Check** or **Don't check**. When you've selected the time block simply push the button that describes what Servers Alive should do during that time period. The blocks will change color to signify their changed status.

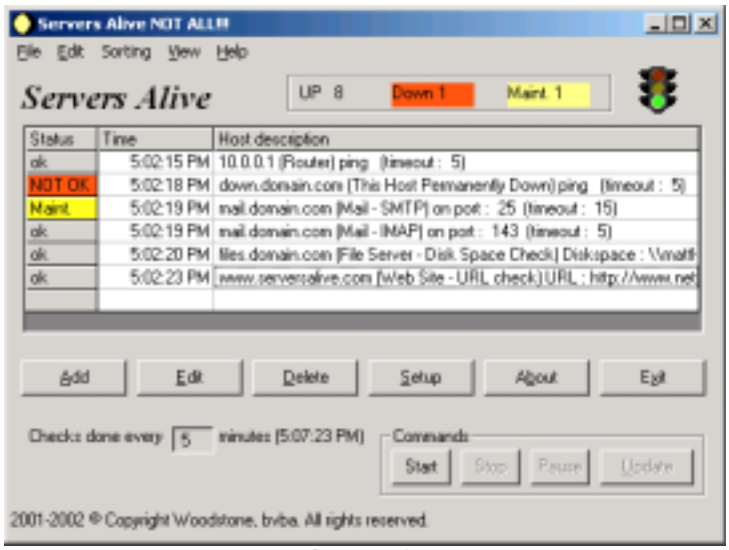


Schedule

You also have another scheduling option on this page. If the entry represents a server that does not need to be checked as frequently as others, you can tell Servers Alive to only check it periodically. You do this by selecting its check **priority** in the bottom-right drop down box.

You can also check the **ignore priority when down** to have Servers Alive check it on every check cycle when it goes down, until it comes back up.

The main interface includes a listing of all entries that have been created. It shows the last detected condition, and, when a check cycle is in progress, will show what is currently being checked. You can use the interface to control the check cycle, work with dependences, and to make global changes to all entries.



Main Interface

Open and Save

Under the File menu you have the option to **Open** a new list of entries and to **Save** your current listing. Save will prompt you for a location and name to save the list of entries. Select an easy to remember location and name. If you want Servers Alive to load a listing by default you can set that under the **Startup** tab in Setup.

Creating Hosts Based on a Template

Under the Edit menu you have an option called **New Host based on**. You can use this option to create similar entries, based on an already created entry. If you have many web servers, for instance, you can create an entry to check one web server, and then use this option to quickly create similar checks for the others.

To use this option first select your already created entry. Then either press CTRL-D or select **Edit->New Host based on**. When the dialog box comes up

change the host, and any other particular information that needs changing. When you are finished click OK.

Finding Hosts

In long host lists you can use the **Find** feature on the edit menu to quickly locate a specific host. Please note that you can only search on the Pretty Name of the host.

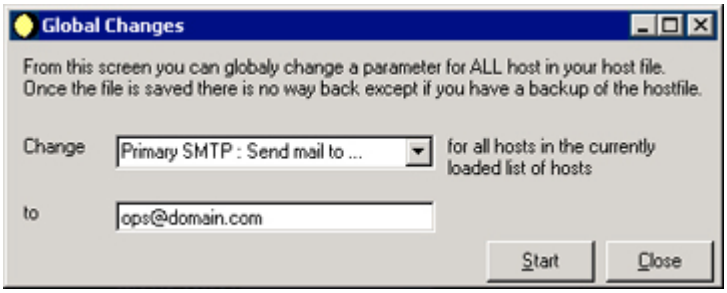
Deleting Hosts

You have two options for deleting hosts. You can delete them on a host-by-host basis, or for more extreme circumstances, delete all hosts at once. Before using either option you must confirm your decision to prevent accidents. If you accidentally delete all your entries, do not close Servers Alive, as it may have been configured to automatically save any changes in Setup. First re-open the default host list and verify that all hosts are still listed. Then select Save to verify that your copy will be available the next time Servers Alive loads.

Woodstone bvba recommends that you backup your entry listing on a regular basis.

Making Global Changes

Occasionally you will need to make entry revisions on a global level. Perhaps you have changed your paging provider, or need to send all primary SMTP messages to a new address. In this case you will use the **Global Change (replace)** option under Edit to make the changes.



Global Changes Dialog Box

When you select the **Global Change** option you are presented with a dialog box. First go through the top list to find the parameter that you need to change. Then type the new value in the bottom text box. When you are ready hit the Start button to begin making changes. It is suggested that you stop the current check cycle and make a backup of your entry listing before making any changes.

You can make global changes to the following fields:

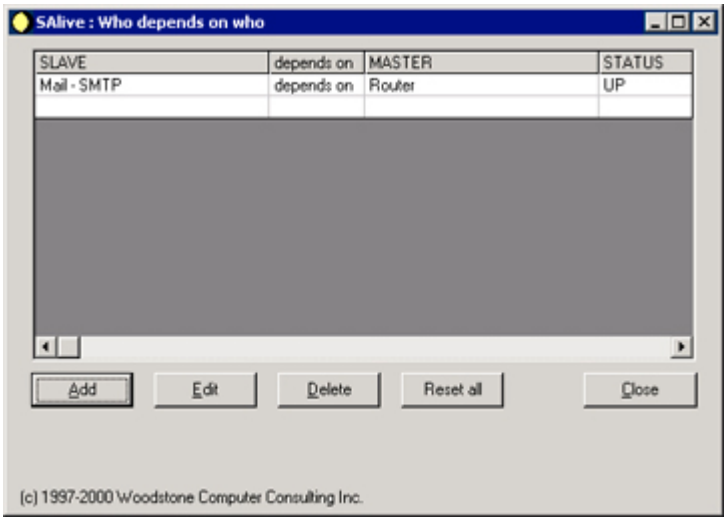
- Primary SMTP Message
- Alternate SMTP Message

- Primary SMTP: Send Mail to...
- Alternate SMTP: Send Mail to...
- Ignore Priority When Down...
- NT service check password
- NT process check password
- Pager number
- Syslog message
- NT performance check password
- NT service check username
- NT process check username
- NT performance check username
- Alpha paging enabled
- Primary SMTP subject
- Alternate SMTP subject
- Disk space check username
- Disk space check password

Dependencies

As an option you can supply Servers Alive with a list of dependencies between your various checked entries. The availability of a server or host can depend on the availability of another server or host. For example if your network contains a router, and your mail server is behind the router, there is no use in checking the mail server if the router is down. You could say that your mail server depends on the router being up. To accommodate this situation Servers Alive allows you to ignore certain hosts if others are already marked as up or down.

You edit dependencies by selecting the **Dependencies** option from the Edit menu. You will be presented with the Dependencies manager, which allows you to add, edit, and delete dependencies. You can define entries that rely on other entries being up, but you can also have them depend on other entries being down. For more explanation see the following example.



Dependencies

Example:
You have a router with a leased line connection to your ISP and a backup line via that same router to another ISP. If the leased line is down, you want to be sure that the backup lines is up to continue serving traffic, but you don't want to check the backup line **unless** the primary line is down, so...

[Backup line interface] depends on [Leased Line interface] being DOWN.

So if the [Leased Line interface] is up, the [Backup line interface] will not be checked. If the [Leased Line interface] is down, the [Backup line interface] will be checked.

The order the hosts are listed in the GUI is very important when using dependencies. If HOST_B depends on HOST_A (being up or down) then HOST_A **must** be checked before HOST_B in the list of hosts, so it must appear first. For more information on reordering your hosts, see the section on Sorting below.

Team Alerting

Servers Alive has a great option for companies that use large technical teams to handle their support. You can use team alerting to send alerts to multiple people based on schedules for each individual. This way, you can tell Servers Alive what people are responsible for various servers, and let it alert them as appropriate based on their schedule of availability.

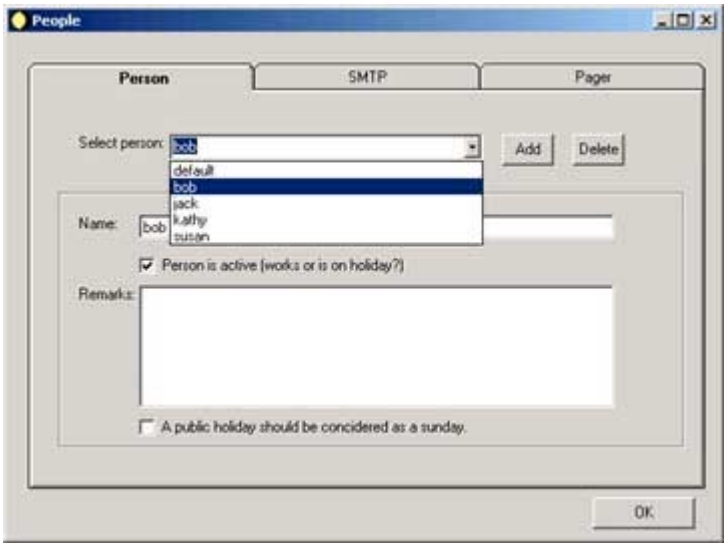
To use team alerting you must setup Person and Team entries that define who should be alerted, and when. To do this you use the **People** and **Teams** options from the Edit menu.

Example:
Suppose your company has four people who are responsible for your servers. These four people are named Jack, Bob, Susan, and Kathy. During the day, when all four are at the office, you want them all to receive any alert, but the four need some time when they are not on call. After looking at their schedules, you determine that each one of them can take a weeknight.

For the weekend you decide to pair Jack and Kathy, and Bob and Susan into sub-teams. Jack and Kathy will handle Friday night and Saturday. Bob and Susan will handle Sunday and Monday morning before the office opens. By having two people receiving the weekend pages they can travel on weekends if necessary. In order to allow Jack and Kathy to not receive any pages Saturday night, they will go off call at 11PM that night.

So, for all four, here is their schedule:
Bob: All Business Hours, Monday Night, Saturday 11PM – Monday 8AM
Jack: All Business Hours, Tuesday Night, Friday 5PM - Saturday 11PM
Kathy: All Business Hours, Wednesday Night, Friday 5PM - Saturday 11PM
Susan: All Business Hours, Thursday Night, Saturday 11PM – Monday 8AM

To set this up you would first go to the Edit menu and select **People**. You will need to set up entries for all four people. Hit the **Add** button on the right and enter each person's name. Don't be alarmed that you cannot enter any capital letters. This is normal. After you have added each person go back to each one and check the **Person is active** box. This means that they can be paged or emailed. If a person goes on vacation you can come back and remove the check mark. When you finish your screen should look like the following:



Adding People Entries

One caveat with setting up a person's schedule is in how Servers Alive deals with public holidays and alerting. By default a public holiday is not treated specially.

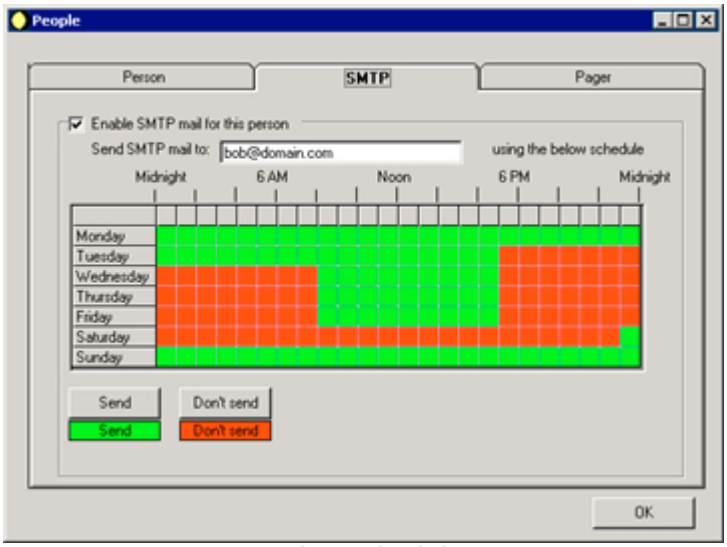
If you want you can have Servers Alive treat public holidays as a Sunday by checking the "A public holiday should be considered as a Sunday" checkbox. This means that if a holiday falls on a Tuesday, you can have Servers Alive check everyone's Sunday schedule instead of his or her Tuesday schedule to determine whom to alert. The list of holidays can be changed via the **Special** tab in the **Advanced** section of setup.

Next you have to set up each person's email and pager schedule. For the purposes of this example we will only look at the SMTP option. Select **bob** and then select the **SMTP** tab.

First we would check the **Enable SMTP mail for this person** box and enter an email address for Bob. By default Bob is scheduled to receive email alerts all the time (since every time block is green). We need to select the time periods when Bob is not on-call and turn them off.

First let's handle the weekdays. Bob is on call Monday night, but he is off-call Tuesday, Wednesday, and Thursday nights. Select each night that Bob is off call and hit the **Don't send** button to turn them off.

Now let's deal with Bob's weekend schedule. Bob goes off-call on Friday at 5PM (the end of the work day), so go to the row labeled Friday and select everything from Friday 5PM on, then click the **Don't send** button. Bob stays off call until 11PM Saturday night, so select the entire row labeled Saturday, up to 11PM. Then click the Don't Send button. Bob's schedule is now set, and he will not receive emails during the time period that he is off call. Your screen should look like the following:



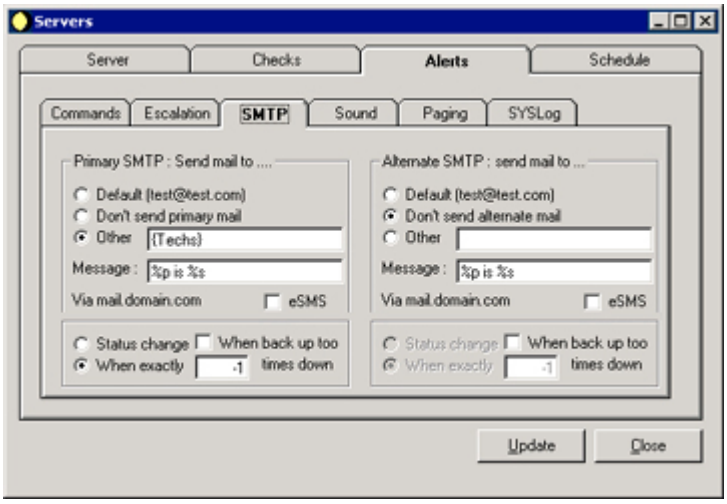
Bob's Schedule

Now that you've seen how to set up one person, you can do similar schedules for the other three people.

The final step is to add all four people into a Team. You could create teams with whatever combination of the four you needed to, depending on what they were responsible. You might include some of them in a team called "Web" that dealt with your web servers, and others in a team that dealt with your network, etc. By setting everyone up in a Team you can simply add a Team name to the alerting section of a host entry, and then modify the Team when necessary.

To add all four people to a team you would go to the Edit menu and choose **Teams**. To create a team you would hit the **Add** button, and give the team a name. Finally, in the bottom of the dialog box, you would select all the team members. Since we are only creating one team you would select all four people.

Now that you have created a team, how do you use it? You can use both team and people definitions in your alerting. When setting up an entry you can use either a team or person entry on the SMTP and Paging alert tabs. When using a person entry you should enclose the person's name in parentheses, like **(person)**. When using a team definition enclose the team name in curly braces, like **{team}**. The following screen demonstrates a host entry that has been instructed to send alert emails to a team called "Techs":



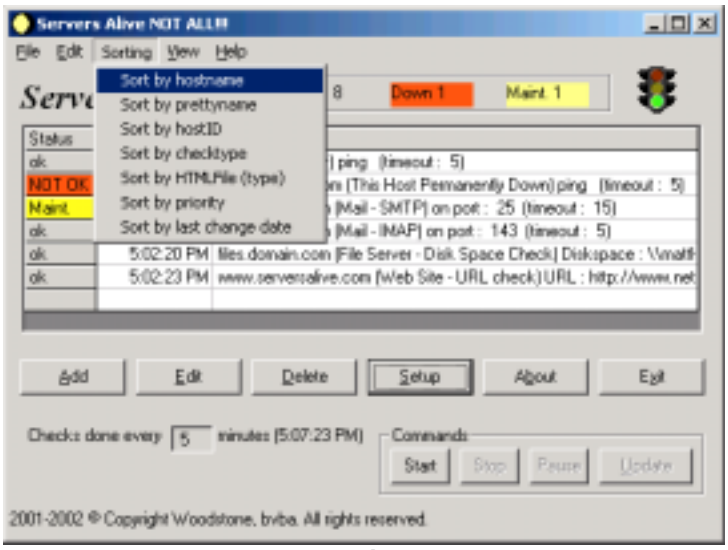
Team Entry

Sorting Entries

There are many different sorting options available under the **Sorting** menu. While these will help you keep your entry list well managed, they can have an impact on other functions that you should be aware of.

Servers Alive does a check cycle starting from the top of the entry list working to the bottom of the list. It does not keep track of or care about the order that hosts were entered. It only looks at the final ordering in the GUI. If you need certain hosts to be checked in a specific order then you must make sure that the hosts are

ordered as you want in the GUI listing. If you are using dependences this is especially important. See the section on Dependencies for more information.



Sorting

You can accomplish this in various ways. You could put special characters at the beginning of the host's pretty name, so that when you sort by pretty name they end up in the correct order. Another method is to manually assign ascending host IDs to each host in the order that you want them checked. With this you can sort by Host ID to keep hosts in the order you choose without changing their display wording.

The **Sorting** options are:

- **Hostname** – Sorts by the hostname entry.
- **Prettyname** – Sorts by the prettyname entry.
- **HostID** – Sorts by Host ID. You can manually change this in the host entry.
- **Checktype** – Groups all checks of a similar type together.
- **HTMLFile** – Groups all checks that appear on the same HTML file together.
- **Priority** – Groups all checks of the same priority (frequency checked) together.
- **Last Change Date** – Find out what was changed most recently.

View

You can use the View menu to hide or show the **Status Frame** and the **Edit buttons**. The status frame is right under the menu bar. It shows how many entries were up, down, and in maintenance during the last check cycle. The edit buttons are below the entry list (Add, Edit, Delete, Setup, About, Exit).

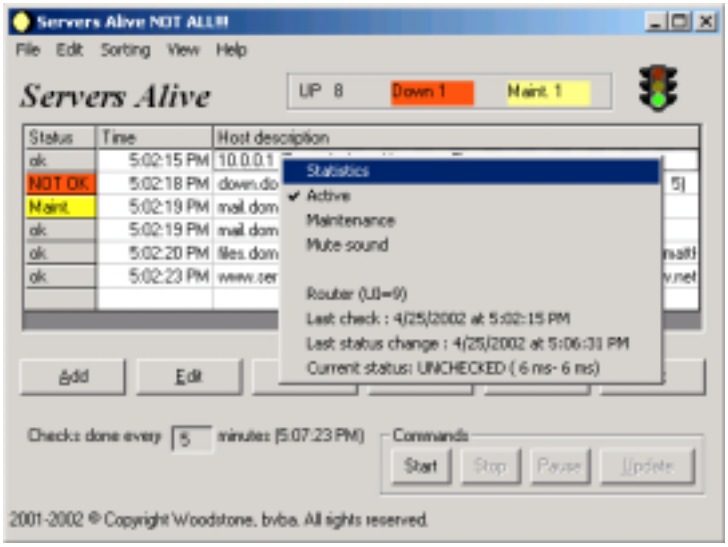
Start, Stop, Pause, and Update

There are four command buttons in the lower right-hand corner of the Servers Alive interface, called Start, Stop, Pause and Update. Use these buttons to control the check cycle. If you **Pause** the check cycle it will stop where it is and allow you to **Resume** when ready. Note, however, that it will only pause until the next schedule check cycle, at which time it will start checking entries again automatically. If you need to stop the check cycle for a long period of time, use the **Stop** button instead. When you are ready to resume use the **Start** button. **Update** will force Servers Alive to immediately begin a new check cycle.

Active and Maintenance Modes

There are two modes that an entry can be in, **Active** and **Maintenance**. Hosts are only included in the check cycle if they are active. Most entries will stay in active mode all the time, and only be switched to maintenance mode when some work is being performed on them. If you have regularly scheduled maintenance periods for a server, you should use the **Schedule** tab in the host entry to schedule periods when it will automatically be switched to maintenance mode.

You can change an entry from Active to Maintenance state, and back, by selecting the entry, right clicking on it, and then selecting either **Active** or **Maintenance** from the menu.



Switching Mode on an Entry

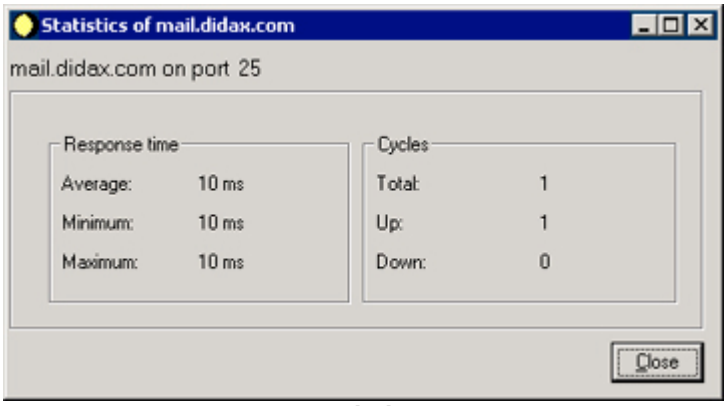
Checking a Single Entry

You can have Servers Alive recheck a single entry that has gone down to verify its condition. You do this by first clicking the **Stop** button to stop any check cycle currently in progress. Find the entry, and double click on the left-most

column of the entry (where it says ok, NOT OK, or Maint). Servers Alive will check that single entry and show the status in the left-most column.

Statistics

Servers Alive maintains statistics on the availability of the servers you monitor. You can access these statistics by first selecting an entry, then right clicking on the entry and selecting the **Statistics** option. The statistics box will contain response time statistics, showing the minimum, maximum, and average response times, and will show how many times the server was detected as up and down. There is currently no way to extract this information for reporting purposes.



Statistics

External Checks

One of the nicest options available in Servers Alive is the ability to write your own custom checks and have them included in the check cycle. These checks can do any task that you are capable of programming, and many people in the Servers Alive community have made external checks that are available for you to use. Woodstone bvba has also provided some external checks for you to use.

Writing External Checks

External checks can be written in any practically any language. They can be actual compiled programs, interpreted scripts, or as simple as a batch file. There are only a few requirements for an external check. The external check must not rely on user input, and it must return an errorlevel to Servers Alive. Servers Alive uses the returned errorlevel to determine if the check succeeded or failed. For more information on running an external check in Servers Alive see the section on External Checks above.

Woodstone bvba Supplied Checks

Woodstone bvba has supplied some example external checks to you. They are located in a subdirectory of the Servers Alive install directory called **external**. In that directory you will find the executable for each check, and a small text file that describes its use. Following is a short description of what each does. Please read the associated text file for more details.

- **CheckODBC** – Checks an ODBC data source. It will attempt to connect to a data source with parameters you give to it. It does not attempt to read or write any data from the data source.
- **Countfiles** – Countfiles will connect to a path you supply (can be a network share) and return an errorlevel equal to the number of files/directories that match your pattern criteria. The pattern is a standard file name wildcard pattern (such as *.*, *.log, or text?.txt).
- **SATelnet** – Satelnet automates connecting to a TCP port, reading data, and passing in commands. This is ideal for checks where you need to connect to the telnet port of a remote machine, log in, issue some commands, and evaluate the result. For information on the many options available in this external check please read the associated text file.
- **SMTP2POP3** – This application gives you a more detailed check of a mail server than simply checking to see if the SMTP and POP3 ports are open. This application will, when properly configured, send an email

through the SMTP server, and then collect that same email through the same or a different POP3 server. This verifies that the entire mail delivery process is functioning.

Legal Addendums

Following are various statements that detail the proper use of Servers Alive. If you have any questions regarding the following sections please contact legal@woodstone.nu.

License Agreement

This license agreement covers your use of the Woodstone bvba's Servers Alive, its executable files and documentation, hereinafter referred to as *the Product*.

The Product is Copyright © 1997-2002 Woodstone bvba. You may use it and distribute it according to this following License Agreement. If you do not agree with these terms you must remove the Product from your system.

By incorporating the Product in your work or distributing the Product to others you implicitly agree to these license terms.

This License Agreement covers the current version of The Product. Woodstone bvba reserves the right to modify the terms of this License Agreement at any time, and without prior notification, in future releases of The Product.

Statement Of Copyright

The Product is, and remains, Copyright © 1997-2001 Woodstone bvba.

Conditions Of Use

The Product is provided in one form: as a ready-to-run installation kit consisting of executable programs, release notes, etc. (the *Product Executable*).

You may freely use and distribute the Product Executable so long as you provide the complete and unmodified original Product Executable installation kit as supplied by Woodstone bvba.

Disclaimer Of Warranty

The Product is provided as free software, in the hope that it will be useful. It is provided "as-is", without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the quality and performance of the Product is with you. Should the Product prove defective, the full cost of repair, servicing, or correction lies with you. The freeware version is limited to checking

10 hosts. You can register the product and then you will be able to check up to 1000 hosts.

Technical Support

Limited technical support can be had from support@woodstone.nu. There is a mailing list dedicated to the use of Servers Alive that is very helpful. To sign up for the list go to http://www.woodstone.nu/salive/subscribe.html. Full guaranteed technical support is subject to a Woodstone bvba support license. For current prices and conditions please email support@woodstone.nu.

Conditions

For commercial distributors, other licensing conditions may be negotiated with respect to technical support and redistribution rights. Before reselling Servers Alive you must contact Woodstone bvba to negotiate a redistribution license.