



up.time
Version 4
Service Pack 5

May 2007

Release Notes



This document introduces the changes in [up.time](#) 4 Service Pack 5, and discusses:

- How to upgrade from a previous version of [up.time](#) 4.
- The new features and enhancements in [up.time](#) 4 Service Pack 5.

The Release Notes for [up.time](#) 4 Service Pack 5 cover the following topics:

<i>Upgrading from a Previous Version of up.time 4</i>	2
<i>New Features</i>	7
<i>Enhancements</i>	12
<i>Contacting Support</i>	18

Upgrading from a Previous Version of up.time 4

If you have installed an earlier version of [up.time](#) 4, you can upgrade to [up.time](#) 4 Service Pack 5 using the installer for your monitoring station's operating system. The upgrade process installs new features, and does not modify or delete your data.

uptime software supplies installers for:

- Upgrading the Windows Version of up.time.
- Upgrading the Linux or Solaris Version of up.time.



You do not need to update your agents or your [up.time](#) license key.

Supported Platforms

The [up.time](#) monitoring station can run on the operating systems listed below. You should refer to the uptime software support Web site for the most up-to-date list of supported platforms:

Operating System	Version(s)
Microsoft Windows XP	XP Professional
Microsoft Windows Server 2003	<ul style="list-style-type: none">• Standard• Enterprise
Solaris (32-bit SPARC)	<ul style="list-style-type: none">• 8• 9• 10
Red Hat Linux AS (x86)	4
Red Hat Linux ES (x86)	4
SUSE Linux Enterprise Server	9
AIX	5.3

Supported Databases

up.time 4 works with the following databases:

- MySQL 4.1 (the default DataStore)
- Oracle 10g
- SQL Server 2000
- SQL Server 2005

Upgrading the Windows Version of up.time

In up.time 4 Service Pack 5 the installer and upgrader for Windows are a single executable. The upgrade process is different depending on which version of up.time 4 you are currently using:

- If you are using up.time 4 with Service Pack 2 or earlier, follow the instructions below.
- If you are using up.time 4 with Service Pack 3 or higher, run the upgrader and follow the two prompts.

In both cases, the older version of up.time 4 will be removed and the Service Pack 5 will be installed. The information in your DataStore will not be deleted, and the configuration information for up.time will be saved to the folder `config-backup`.



The Windows installer only works with Windows XP and Windows Server 2003.

Before you begin, you must have administrator privileges for the system on which you will be installing up.time 4 Service Pack 5.

To upgrade the Windows version of up.time 4, do the following:

- 1 Download the installer from the uptime software support Web site.**

The installer will have a name like `up.time-<build#>-win32-x86.exe`, where `<build#>` is the number of the up.time build to which you are upgrading. For example, `up.time-4.5.100-win32-x86.exe`.

- 2 Double click the installer file.**

- 3 **On the Introduction screen, click Next.**
- 4 **If you are currently using up.time 4 with Service Pack 2 or older, the upgrade installer warns you that it will first remove your older version of up.time 4, then install Service Pack 5.**

Click **Uninstall** to continue.

The uninstall program for the previous version of up.time 4 is launched. Follow the on-screen prompts to remove the application.

Once the previous version of up.time 4 is removed, you are returned to the upgrade installer.

- 5 **Click Next.**
- 6 **Do one of the following to select the location where the version of up.time that you are upgrading is installed:**
 - Click **Next** to accept the default location (C:\Program Files\uptime software\uptime4).
 - In the **Please Choose a Folder** field, type the name of the directory where you want to install the application and then click **Next**.
 - Click **Choose** and select a directory from the **Browse for Folder** window.
 - To recover the default directory, click **Restore Default Folder**.

- 7 **Click Next.**

- 8 **On the Pre-Upgrade Summary screen, review the options that you selected and then do one of the following:**

- Click **Previous** to change the settings.
- Click **Install** to begin the upgrade process.

The upgrade process will take several minutes.

- 9 **On the Install Complete screen, click Next.**
- 10 **Click Done.**

Upgrading the Linux or Solaris Version of up.time

To upgrade the Linux or Solaris version of **up.time** 4, do the following:



You must be logged into the system on which you will be installing **up.time** 4 Service Pack 5 as the root user.

1 From the uptime software support Web site, download the upgrade installer.

The installer will have a name like `up.time-<build#>-<platform>-upgrade.bin`, where `<build#>` is the number of the **up.time** build to which you are upgrading, and `<platform>` is the operating system on which you are installing the upgrade. For example:

- Linux: `up.time-4.5.100-rhes4-x86-upgrade.bin`
- Solaris: `up.time-4.5.100-solaris8-sparc-32-upgrade.bin`



Ensure that you download the upgrade and not the full release of **up.time** 4.

2 Enter the following command at the command line to run the upgrade installer:

```
sh up.time-<build#>-<platform>-upgrade.bin
```

For example, to upgrade **up.time** on a Linux system type the following:

```
sh up.time-4.5.100-rhes4-x86-upgrade.bin
```

It can take up to several minutes for the components of the installer to be extracted from the `.bin` file. Wait while this process completes.

3 On the Introduction page, press Enter to continue.

4 Do one of the following to select the location where the version of up.time that you are upgrading is installed:

- Press Enter to accept the default location, `/usr/local/uptime4/`.

- Type a new location at the command prompt and then press Enter.



The uptime user account must be able to access the directory that you specify.

5 On the Pre-Upgrade Summary page, review the installation options and then do one of the following:

- Type back and then press Enter to change any of the settings.
- Press Enter begin the installation process.

6 On the Install Complete page, press Enter.



It can take up to a minute for the [up.time](#) services to start. Wait before attempting to log into the monitoring station.

New Features

up.time 4 Service Pack 5 contains the following new features:

- Support for Splunk
- Monitoring Station for AIX
- Support for SQL Server 2005

Support for Splunk

Splunk is a third-party search engine that indexes log files and data from the devices, servers, and applications in your network. Using Splunk, you can quickly analyze your logs to pinpoint problems on a server or in a network, or ensure that you are in compliance with a regulatory mandate or Service Level Agreements. You install Splunk on a server in your data center.

up.time 4 Service Pack 5 can integrate with Splunk, and offers two Splunk monitors: the Splunk Query Monitor and the Live Splunk Listener Monitor.

You can configure action profiles to work with the up.time Splunk monitors. From the **Current Issues** section of the **My Portal** panel, you can check the Splunk logs for information about the outage by clicking the Splunk icon (**splunk**>) beside the names of services that are in WARN or CRIT states. This icon also appears in the **System Outages** window.

To use Splunk with up.time, you will need to add the following entries to your uptime.conf file:

- splunk.url=
The URL of the server on which your Splunk search pages is hosted. For example, http://webportal:8000.
- splunk.username=
The user name required to log into your Splunk search page.
- splunk.password=
The password required to log into your Splunk search page.

- `splunk.soapurl=`
The URL that points to the SOAP management port which Splunk uses to communicate with the splunkd daemon. For example, `https://webportal:8089`.

You must set up the port on which the Splunk server listens for requests on the server itself. See the *Splunk Admin Manual* for more information.

The following options have been added to the **Add Action Profile** window for action profiles that will work with the **up.time** Splunk monitors:

- **Splunk Hostname**
The host name of the server on which Splunk is running.
- **Logging Port**
The port on which the Splunk server is listening for logging requests. This port is configured in Splunk.
- **Use SSL**
Select this option to securely access the Splunk server via SSL.

Splunk Query Monitor

You can use the Splunk Query monitor to perform Splunk queries on log files so that you can pinpoint an error condition. To use this monitor, you specify the following:

- The Splunk query string that you want to use to search log file for an error condition. For example, entering the following query string:

```
host::mailServer sendmail error hoursago::2
```


Will search log files, that were generated for the system named mailServer, for the word `sendmail` and `error` that were logged within the last two hours.
- The result count of Splunk query, which enables **up.time** to alert you when the number of results that match your Splunk query exceeds the warning and critical thresholds that you set.

For information about configuring the Splunk Query monitor, see “Splunk Query Monitor” in the *up.time 4 User Guide*.

Live Splunk Listener Monitor

Live Splunks are scheduled searches of one or more Splunk queries that are saved on the Splunk server. A Live Splunk automatically runs a search, can initiate an alert, and perform actions based on that alert. You can, for example, set up a Live Splunk to search for all critical error conditions.

The Live Splunk Listener monitor enables you to capture the information generated by a Live Splunk. This monitor is very similar to the [up.time External Check](#) monitor, and uses the script `liveSplunkHandler.py` (which is bundled with [up.time](#), in the `scripts` folder) to return Live Splunk information to the monitoring station.

For information about configuring the Live Splunk Listener monitor, see “Splunk Query Monitor” in the *up.time 4 User Guide*.

Before you can monitor Live Splunks, you must:

- Edit the script `liveSplunkHandler.py` to point to the [up.time](#) monitoring station. Do the following to edit the script:
 - i **Navigate to the `scripts` folder on the monitoring station.**
 - ii **Open the file `liveSplunkHandler.py` in a text editor.**
 - iii **Find the following entry in the file:**

```
# Specify the up.time server and port
# by setting the following two variables
host = "localhost"
port = "9996"
```
 - iv **Change the values for `host` and `port` to the host name and port of the monitoring station.**
 - v **Save the file and exit the text editor.**
- Copy the script `liveSplunkHandler.py` from the `scripts` folder on the monitoring station to the folder `/data/splunk/bin/scripts` on the Splunk server.
- Configure a Live Splunk. For information on configuring Live Splunks, see the Splunk user manual.

When setting up your Live Splunk, select the **Run the shell script option** on the configuration page. Then, enter the path to `liveSplunkHandler.py`, along with the script options, in the field:

Run the shell script
`/data/splunk/bin/scripts/liveSplunkHandler.pl --host="dev-latest" --port=9996 --message="failed login (windows)" --status=1 -`

Monitoring Station for AIX

The [up.time](#) monitoring station can now run on AIX version 5.3 on pSeries POWER architectures. You can install the monitoring station on the base AIX file system or on a Logical Partition.

This allows [up.time](#) and the installer to exceed the default system resource limits, which can otherwise interfere with the ability of the application to perform monitoring and analysis.

Installing the Monitoring Station on AIX

To install the [up.time](#) monitoring station on AIX, do the following:

1 Type the following command:

```
sh up.time-4.0.<build#>-aix.bin
```

where `<build#>` is the number of the [up.time](#) build that you are installing, for example: `up.time-4.5.100-aix.bin`

It can take up to several minutes for the components of the installer to be extracted from the `.bin` file. Wait while this process completes.

2 Follow the instructions in the section “Installing the Monitoring Station on Solaris, Linux or AIX” in the *up.time 4 User Guide*.

When you install the [up.time](#) monitoring station on AIX 5.3, the installer creates a user called `uptime` and adds the following lines to the end of the file `/etc/security/limits`:

```
uptime:  
  fsize = 2097151  
  core = -1  
  cpu = -1  
  data = -1  
  rss = -1
```

```
stack = -1
nofiles = 2000
```

Support for SQL Server 2005

Users of [up.time 4 Service Pack 5](#) can use SQL Server 2005 as the DataStore for the application. To do this, you will need to change the following database settings in the file `uptime.conf`:

- `dbDriver=`
The database driver that is used to connect the monitoring station to the DataStore. For SQL Server, the supported driver is `net.sourceforge.jtds.jdbc.Driver`.
- `dbType=`
The type of database that is being used to store data from [up.time](#) – in this case, `mssql`.
- `dbHostname=`
The name of the system on which the database is running.
- `dbPort=`
The port on which the database is listening.
- `dbName=`
The name of the database.
- `dbUsername=`
The name of the default database user, which is `uptime`.
- `dbPassword=`
The password for the default database user, which is `uptime`.

For more information, see “Database Settings” in the *up.time 4 User Guide*.

Enhancements

up.time 4 Service Pack 5 contains the following enhancements:

- Enhancements to the Windows Event Log Scanner
- Other Enhancements

Enhancements to the Windows Event Log Scanner

The Windows Event Log Scanner has been re-written to include a more flexible set of checking options. These options enable you to better see and understand the information that is coming from a Windows system, and to check various system event logs.

The monitor template for the Windows Event Log Scanner contains the following fields:

- Event Log Type (Mandatory)
Choose one of the following types of event log to search:
 - Application
A log that records events generated by programs running on the server.
 - System
A log that records the activity of various components of the operating system.
 - Security
A log that records events such as login attempts and attempts to access files.
- Number of Lines
The number of lines in the log file that up.time will scan for the criteria specified in the monitor template. The default is 100.
- Match event ID with
A number that identifies the type of event.

- Match event type with
The type of event to search for, which can be one of the following:
 - Information
Describes the successful completion of a task.
 - Warning
Indicates that a problem may occur in the future.
 - Error
A problem, which may involve the loss of data or system integrity, has occurred.
 - Success Audit
Found in the Security log, this describes the successful completion of an audited security event.
 - Failure Audit
Found in the Security log, this describes the failure of an audited security event.
- Match computer name with
The name of the computer on which the event occurred.
- Match category with
The way in which the application, system component, or application module that triggered the event classifies the event. A category can be, for example: System Event (in the Security Log); or Installation, CI Service, or wrapper (in the Application and System logs).
- Match source with
The application, system component, or application module that triggered the event.
- Search description for
Enter the string for which you want to search in the event log, for example:

```
The WMI Performance Adapter service entered the running state
```


`up.time` evaluates this string as a regular expression.

Other Enhancements

up.time 4 Service Pack 5 contains the following additional enhancements:

- The Service Monitor Metrics report has two new options:
 - Show all non-ranged metrics on one chart
This option combines all of the variables that you selected in one chart. Any ranged metrics will appear in their own charts.
 - Display charts as stacked area
Each chart in the report will have two or more data series stacked on top of each other, rather than the line graph that usually appears in the report.
- A new column, labelled ACK, was added to the **Service Status** section of **Global Scan**. When the current status of a monitor is acknowledged, it appears in the ACK column instead of in the WARN or CRIT column.

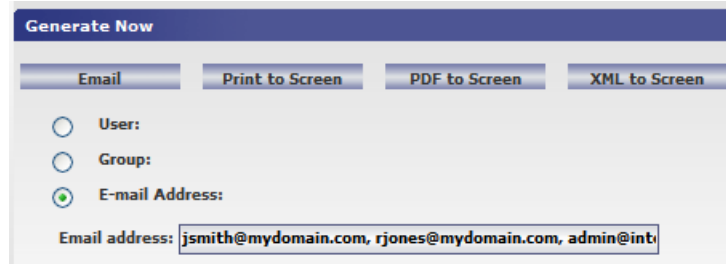
Service Status					
OK	WARN	CRIT	MAINT	UNKN	ACK
1	0	0	0	0	0
2	0	0	0	0	0
0	0	1	0	2	0
4	0	0	0	0	0
5	0	0	0	0	0
2	1	0	0	0	0
1	0	0	0	0	0
0	0	0	0	1	1

To enable the ACK column, add the following entry to the file `uptime.conf`:

```
acknowledgedSeparate=true
```

- When a service is in a maintenance period, the status of that service is coloured blue in **Global Scan**.
- The bar chart in the **Global Scan** panel has been renamed **Recent Outages**. This bar chart only displays outages whose time stamps are relative to the current time.

- You can now email reports to multiple recipients by entering their email addresses (separated by commas or semi-colons) in the **Email address** field of the report definition page, as shown below:



The screenshot shows a dialog box titled "Generate Now" with four buttons: "Email", "Print to Screen", "PDF to Screen", and "XML to Screen". Below the buttons are three radio buttons: "User:", "Group:", and "E-mail Address:". The "E-mail Address:" radio button is selected. Below the radio buttons is a text field labeled "Email address:" containing the text "jsmith@mydomain.com, rjones@mydomain.com, admin@int".

- You can add an HMC managed system to [up.time](#) using the `addsystem` command line utility. The format of the entry for the HMC managed system in the hosts file is:

```
Host Name: 10.1.2.42
Display Name: HMC Managed Server
HMC Hostname: 10.1.1.255
Type: pSeries LPAR Server (HMC)
Managed Server: Server-7610-31C-SN01B030K
Username: hscroot
Password: hscroot
```

See “Adding Multiple Systems to [up.time](#)” in the *up.time 4 User Guide* for more information.

- The `netcat` utility (used to execute commands on agents across a network connection) has been replaced with a new utility called `agentcmd`.

As with `netcat`, you would normally use `agentcmd` in a script on the monitoring station to return the results of an agent-side script, validate the status of those results, and return the status to [up.time](#). There are two scenarios in which you can use `agentcmd`:

- With an agent on a system that has been added to [up.time](#). In this case, the hostname is in the [up.time](#) DataStore.
- With an agent that has been deployed on a system that has not been added to [up.time](#). If there is no agent on the system, or there are network problems, `agentcmd` returns the following error message:

```
ERR Unable to contact Agent (10.1.2.34 on port 9998)
```

The command line syntax of `agentcmd` is:

```
agentcmd <-/+s> <-p #> hostname command
```

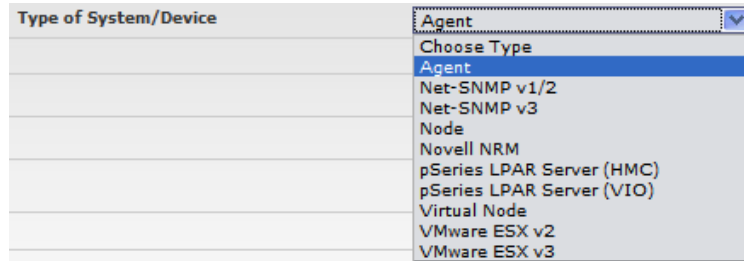
Where:

- `-s` = do not use an SSL connection to the agent. This is the default.
- `+s` = connect to the agent using SSL.
- `-p #` = connect to the agent on the specified port. The default is 9998.
- `hostname` = the name or IP address of the host on which the agent is running.
- `command` = the agent command to run.

For example, to get basic system information from an agent running on the server Solaris1, type the following command:

```
agentcmd -s Solaris1 sysinfo
```

- In the **Add System** window, the contents of the **Type of System/Device** drop down list are now in alphabetical order.



- When you generate one of the following reports for a group or a view, only agent systems appear in the report:
 - Resource Usage
 - Multi System CPU
 - CPU Utilization Summary
 - CPU Utilization Ratio
 - Wait I/O

- Enterprise CPU Utilization
- File System Capacity Growth
- Server Virtualization
- On the **View Service** page, you can now click the host names. Doing this will take you to the information screen for the host.
- You can use the `$(DISPLAYNAME$` variable to include an entity's display name in **up.time** in a custom alert. For more information, see “Custom Alert Format Variables” and “Working with Custom Alert Formats” in the *up.time 4 User Guide*.
- You can disable archiving of your DataStore from the **Archive Policy** page of the **Config** panel.
- The Service Metrics graph has been moved to the Graphing tab, which now also appears for entities from which performance data is not collected.

Contacting Support

uptime software delivers responsive customer support that is available to both licensed and demonstration users. uptime software offers user support through the following:

- Documentation
- Telephone
416 868 0152
- E-mail
support@uptimesoftware.com
- Web site
<http://support.uptimesoftware.com>

Contacting uptime software

uptime software inc.
555 Richmond Street West,
PO Box 110
Toronto, Ontario
M5V 3B1

Main Telephone Line: 416 868 0152
Main Fax Line: 416 868 4867

Copyright © 2007 uptime software inc.

uptime software inc. considers information included in this documentation to be proprietary. Your use of this information is subject to the terms and conditions of the applicable license agreement.

Restricted Rights Legend

This product or document is protected by copyright and distributed under licenses (see “up.time End User License Agreement”) restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of up.time and its licensors, if any.

Third party software is copyright and licensed from uptime software suppliers.

Documentation is provided “as is” and all express or implied conditions, representations, and warranties including any implied warranty or merchantability are disclaimed, except to the extent that such disclaimers are held to be legally invalid.

Trademarks

up.time® is a registered trademark of uptime software inc.

IBM is a registered trademark of International Business Machines Corporation.

Oracle is a registered trademark, and the Oracle product names are registered trademarks or trademarks of Oracle Corporation.

Microsoft, Windows, Microsoft SQL Server, and other such trademarks are registered trademarks of Microsoft Corporation.

Sybase, PowerBuilder, and other such trademarks are the registered trademarks of Sybase Incorporated.

Solaris, UltraSparc, and other such trademarks are the registered trademarks of Sun Microsystems Incorporated.

All other trademarks belong to their respective companies, property owners, and organizations.

Notes