Contents

Using this guide .......................................................................................................................... 4

1. Overview ................................................................................................................................. 5
  1.1 General Information ............................................................................................................ 5
  1.2 Security ............................................................................................................................... 6
  1.3 Requirements ...................................................................................................................... 7
  1.4 Main Purpose ..................................................................................................................... 8

2. RTM Manager ......................................................................................................................... 9
  2.1 Installation .......................................................................................................................... 9
  2.2 Interface ............................................................................................................................ 10
  2.3 Connect .............................................................................................................................. 11
  2.4 Applications Manager ...................................................................................................... 13
  2.5 Processes Manager .......................................................................................................... 14
  2.6 Services Manager .......................................................................................................... 18
  2.7 Devices Manager ............................................................................................................. 20
  2.8 Events Manager .............................................................................................................. 22
  2.9 Performance Monitor ...................................................................................................... 25
  2.10 Shares Manager ............................................................................................................. 27
  2.11 Network Monitor .......................................................................................................... 28
  2.12 Hardware Resources ....................................................................................................... 30
  2.13 NetStat ............................................................................................................................ 32
  2.14 Security Patch Analyzer .................................................................................................. 33
  2.15 Advanced Service Control Manager, General ................................................................. 35
  2.16 Advanced Service Control Manager, Log On ................................................................. 38
  2.17 Advanced Service Control Manager, Recovery ............................................................... 39
  2.18 Advanced Service Control Manager, Dependencies .......................................................... 41
  2.19 Advanced Service Control Manager, Security ............................................................... 42
  2.20 Advanced Service Control Manager, Permissions ............................................................ 43
  2.21 Advanced Service Control Manager, Auditing ................................................................. 45
  2.22 Advanced Service Control Manager, Ownership ............................................................. 47
  2.23 Advanced Service Control Manager, SNMP Agent ........................................................ 48
  2.24 Advanced Service Control Manager, SNMP Traps ........................................................ 49
  2.25 Advanced Service Control Manager, SNMP Security ................................................... 51
  2.26 Advanced Share Manager, General .................................................................................. 53
  2.27 Advanced Share Manager, Sharing Permissions ............................................................... 54
  2.28 Advanced Share Manager, Connected Users ................................................................. 56
  2.29 Advanced Share Manager, Open Resources ................................................................. 57
  2.30 Remote Shutdown ............................................................................................................ 59
2.31 Remote Execute ................................................................. 61
2.32 Remote Lock ................................................................. 63
2.33 System Information ....................................................... 64

3. RTM Service ......................................................................................... 66
3.1 Installation .................................................................................. 66

4. RTM Console ....................................................................................... 68
4.1 Installation .................................................................................. 68
4.2 Usage ......................................................................................... 69
4.3 Examples ................................................................................... 72
Using this guide

This guide assumes you're familiar with basic functions like click, right-click and double-click, and that you're familiar with the basics of the operating system you're using. Also, we use the following conventions:

- *Italic* for file names, paths, buttons, menus, and menu items.
- **Bold Italic** for notes and comments.
- Keyboard keys with a plus sign separating keys that you press simultaneously. For example: press Ctrl+Alt+Del to restart your computer.

We strongly recommend to read this guide very carefully and thoroughly. It was designed around the understanding that its users already have basic network knowledge as well as the ability and know-how to install a Local Area Network (LAN).
1. Overview

1.1 General Information

Systems Administrators are greatly assisted by powerful tools that remotely handle a wide range of tasks on their client computers.

Remote Task Manager from SmartLine Inc is a systems control interface that can be run from any remote Windows NT/2000/XP and Windows Server 2003 computer. It is the leading enterprise remote control solution for corporate networks.

Remote Task Manager significantly reduces the total cost of network management in enterprise environments by enabling IT personnel to control tasks, processes, services, devices, shared resources, events and computer performance over LAN, WAN and the Internet.

Remote Task Manager consists of three parts: RTM Service (rtmservice.exe), RTM Manager (rtmanager.exe) and RTM Console (rtmc.exe).

RTM Service is the core of Remote Task Manager. It is installed on each client system that you want to manage remotely. RTM Service runs automatically and provides network access to the client machine while remaining invisible to that computer’s local users.

RTM Manager is the control interface Systems Administrators use to remotely manage each network computer that has RTM Service.

RTM Console is similar to RTM Manager except it uses a command line interface rather than a GUI. RTM Console’s simpler interface works even on Windows 95/98/Me so you can remotely manage Windows NT systems from a Windows 9x computer.
1.2 Security

Reliable access control functionality is the primary focus of Remote Task Manager.

Remote Task Manager uses Remote Procedure Call (RPC) technology for communication between the service and the manager. It uses the Windows user-level security subsystem for authentication.

Remote Task Manager’s security is integrated into the Windows access control subsystem. Remote computers with an installed RTM Service can only be accessed by someone with administrator privileges.

Because Remote Task Manager uses standard protocols, it operates like any other Windows administrative tool such as User Manager, Server Manager, Event Viewer, etc.

The RTM Service on each client machine checks all input data for size and type making it impossible for buffer overflow attacks.
1.3 Requirements

Remote Task Manager works on any computer using Windows NT/2000/XP and Windows Server 2003. RTM Console, a part of Remote Task Manager, can also work on Windows 95/98/Me.

There are no special requirements for using Remote Task Manager.

To use Remote Task Manager on your network, you must have a functioning TCP/IP network protocol. However, Remote Task Manager can also work on stand-alone computers.
1.4 Main Purpose

With Remote Task Manager network administrators can:

- Monitor all running tasks, processes, services, devices, shared resources and events on remote computers.
- Perform security patch assessment for the Microsoft’s operating systems and applications.
- Watch features of running tasks (the handle of the main window, process ID, etc.).
- Watch features of running processes (process ID, CPU time, privileges used, memory, priority, etc.).
- End a selected task correctly.
- Terminate a selected process at any time.
- Change priority of a selected process.
- Control which CPUs the process will be allowed to execute on.
- Stop, start, restart, pause and continue any selected service or device.
- Change startup parameters of a service or a device (name, account, startup type, dependencies, etc.).
- Change service’s repair parameters on Windows 2000/XP.
- Adjust service’s and device’s security (permissions, auditing and owner).
- Monitor a dynamic overview of the computer’s performance (CPU and memory usage).
- Monitor a dynamic overview of the network performance.
- Manage shared resources on remote computers.
- Shut down and reboot remote computers.
- Create processes on remote computers.
- Lock computers remotely.
2. RTM Manager

2.1 Installation

RTM Manager can be installed to any computer running Windows NT/2000/XP and Windows Server 2003.

To install RTM Manager just run Setup (setup.exe).

RM Manager installs to the directory of your choice. Setup tries to find a RTM Manager installation and, if one exists, Setup suggests you install RTM Manager to the same directory. If a previous installation does not exist, Setup suggests you install RTM Manager to the Program Files directory on the system drive (e.g. C:\Program Files\Remote Task Manager). You can always select another directory for installation.

You have two choices: install both RTM Manager and RTM Service using Typical setup or you can install only RTM Manager using Custom setup, then selecting the RTM Manager component.

After a successful install, you can run RTM Manager by selecting the Remote Task Manager item from the Programs menu.
2.2 Interface

RTM Manager has a user-friendly, easy-to-use interface. All functions can be accessed with either a mouse or keyboard.

In any dialog you can press the F1 button to get specific help.

The main window of RTM Manager can be resized. RTM Manager saves its size and position, and restores these at its next startup. To activate a specified tab at startup, you can specify the tab's number (from 0 to 9) in the command line, for example: rtmanager.exe tab=4.

RTM Manager has a menu at the top of its main window. Many functions are accessible through this menu.

When RTM Manager is running, an accurate miniature CPU usage gauge appears on the taskbar on the end opposite the Start button. When you touch it with the cursor, it displays the percentage of processor use in text format.

You can select Always on Top from the View menu to keep the RTM Manager on top (above) any other applications. If you run RTM Manager frequently and don't want to see its icon on your taskbar, click Hide When Minimized from the View menu. To open a hidden RTM Manager, click the RTM CPU gauge on the taskbar.

To change the columns displayed in any tab, click Select Columns in the View menu or press the F8 key. All RTM Manager columns can be resized. To sort a list on almost any tab, click the column heading you want to sort by. To reverse the sort order, click the column heading a second time. You can also enable the gridlines around list items by selecting Enable Grid in the View menu.

To refresh a current list, select Refresh Now in the Options menu or press the F5 key. You can also set the speed of a list's refresh, by selecting Update Speed in the Options menu. If you select Paused then RTM Manager will not automatically refresh the list.

You can click the right mouse button almost anywhere in RTM Manager to open a useful context menu.

The status bar always displays the total number of processes, CPU use, and virtual memory use for the connected computer.
2.3 Connect

Starting RTM Manager the first time displays the **Connect** dialog where you can select a computer to manage. Subsequent startups automatically connect to the last client computer provided that the *Restore Last Connection* item from the *Option* menu is enabled (checked). Also, you can specify the computer’s name in the command line, for example: `rtmanager.exe \server`.

To quickly access the **Connect** dialog at any time press the F3 key or select **Connect** from the *File* menu.

```
Select Computer

Computer name FRO Net Browser Computer List

Connect

X Cancel
```

Select the computer from the list of computers by pressing the *Net Browser* button. Also, you can type a computer name in the combo box located at the left side of the **Connect** dialog.

All frequently used computers are added automatically to the most recently used (MRU) list so they can be easily accessed.

```
FRO
\ACERLAPTOP
\MMX2000
\P3IIWHISTLER
\PRO
\SL_SERVER
```

RTM Manager lets you configure your own list of computers. Press the **Computer List** button to select a computer from this list. In the **Computer List** dialog you can add, edit and remove computers and comments from the list. You can also add computers from an external file by pressing the *Load* button and selecting the file. Two formats are supported — text file (.txt) and comma separated values (.csv). To save a computer listing to an external file, press the *Save* button and select the type of file to save as.
To connect to a selected computer, use the Connect button. If you don't have administrative privileges on the selected computer, RTM Manager will show the Enter Network Password dialog and you'll be able to connect under the account of any other user. The Enter Network Password dialog appears when you attempt to connect to a computer, but the domain controller (DC) does not recognize the user account you have used to log on. This often occurs when you are logged on as the administrator of a local computer and attempt to access domain resources. To access the domain resources, you must provide a valid user account and password that the domain recognizes. User accounts are a domain name followed by a backslash (\) and the user name, e.g. D1\John.

RTM Service should be installed on the remote system so you can manage that system. Remote Task Manager supports remote installing. This lets a Systems Administrator set up a service on distant machines without having to physically go to them. If the RTM Service isn't installed on the remote system you are trying to connect to, RTM Manager will suggest that you install the service. Select the RTM Service executable file (rtmservice.exe) and RTM Manager will copy it to the remote computer’s Windows system directory (e.g. c:\winnt\system32). If the service is on the client system but is outdated, RTM Manager replaces it.

RTM Manager automatically starts RTM Service if it's stopped on the system.

If you successfully connect to a computer, its name appears in the title of main RTM Manager window.
2.4 Applications Manager

The **Applications** tab shows the information about the programs that are running on the computer:

- **Task** - the caption of the application's main window.
- **PID** - the identifier of the application's process.
- **TID** - the identifier of the application's thread.
- **HWND** - the hexadecimal handle of the application's main window.
- **Status** - the current status of the application (*running* or *not responding*).

<table>
<thead>
<tr>
<th>Task</th>
<th>PID</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Photoshop</td>
<td>183</td>
<td>Running</td>
</tr>
<tr>
<td>Irbus - Outlook Express - Main Identity</td>
<td>202</td>
<td>Running</td>
</tr>
<tr>
<td>Microsoft Word - Remote Task Manager Manual.doc</td>
<td>199</td>
<td>Running</td>
</tr>
<tr>
<td>Program Manager</td>
<td>114</td>
<td>Running</td>
</tr>
<tr>
<td>Remote Task Manager (PRO)</td>
<td>252</td>
<td>Running</td>
</tr>
<tr>
<td>{D:</td>
<td>MSDEV</td>
<td>Projects</td>
</tr>
</tbody>
</table>

Windows lets users have multiple desktops with each desktop containing different applications. To control the applications that belong to a desktop, select this desktop from the desktops list.

To stop the application, select it from the list and press the *End Task* button (you can also use the context menu). RTM Manager will send a special message (*WM_CLOSE*) to the application's main window, all applications should respond to this message and close themselves correctly. If the application doesn't respond to the *End Task* request within 5 seconds, RTM Manager will show a dialog having the following three buttons:

- **Wait** - gives the application 5 seconds to finish what it is doing and then RTM Manager tries to close the application again.
- **Terminate** - terminates the application immediately. You will lose any unsaved information from this application.
- **Cancel** - cancels this dialog and returns to **Applications Manager**.
2.5 Processes Manager

The **Processes** tab shows information about the processes running on the computer:

- **Image Name** - name of the process's executable file.
- **PID** - the process identifier.
- **User Name** - the user associated with a process.
- **CPU** - how much of a CPU's time is taken by a process (%).
- **Create Date/Time** - the date and the time when a process was created.
- **Processor Time** - how much CPU time a process is using (H:mm:ss).
- **Privileged** - how much system resources is free for a process (%).
- **User** - how much system resource is used by a process (%).
- **Memory** - how much memory is used by a process (KBytes).
- **Mem. Peak** - maximal peak of memory used by a process, during all the time it's been working (KBytes).
- **Page Faults** - the number of times data has to be retrieved from disk for a process because it was not found in memory. The page fault value accumulates from the time the process started.
- **VM Size** - how much virtual memory committed to a process (KBytes).
- **VM Peak** - maximal peak of virtual memory committed to a process, during all the time it's been working (KBytes).
- **Page File Usage** - the amount of virtual memory, or address space, committed to a process (KBytes).
- **Page File Peak** - maximal peak of page file usage (KBytes).
- **Paged Pool** - the amount of the paged pool (user memory) used by a process (KBytes).
- **Paged Pool Peak** - maximal peak of the paged pool used by a process, during all the time it's been working (KBytes).
- **NP Pool** - the amount of the nonpaged pool (system memory), used by a process (KBytes).
- **NP Pool Peak** - maximal peak of nonpaged pool, used by a process, during all the time it's been working (KBytes).
- **Prior.** - priority of a process (0 - idle, 24 - real time).
- **Handles** - number of handles opened by a process.
- **Threads** - number of threads created and used by a process.
- **Parent PID** - the parent's process identifier.
- **Session ID** - the Terminal Services session ID that owns the process.

<table>
<thead>
<tr>
<th>Image Name</th>
<th>PID</th>
<th>User Name</th>
<th>CPU</th>
<th>Create Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Idle Process</td>
<td>0</td>
<td>SYSTEM</td>
<td>96 %</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>4</td>
<td>SYSTEM</td>
<td>0 %</td>
<td></td>
</tr>
<tr>
<td>SMSS.EXE</td>
<td>148</td>
<td>SYSTEM</td>
<td>0 %</td>
<td>30.06.2001 13:</td>
</tr>
<tr>
<td>WINLOGON.EXE</td>
<td>160</td>
<td>SYSTEM</td>
<td>0 %</td>
<td>30.06.2001 13:</td>
</tr>
<tr>
<td>CSRSS.EXE</td>
<td>172</td>
<td>SYSTEM</td>
<td>0 %</td>
<td>30.06.2001 13:</td>
</tr>
<tr>
<td>SERVICES.EXE</td>
<td>220</td>
<td>SYSTEM</td>
<td>0 %</td>
<td>30.06.2001 13:</td>
</tr>
<tr>
<td>LSASS.EXE</td>
<td>232</td>
<td>SYSTEM</td>
<td>0 %</td>
<td>30.06.2001 13:</td>
</tr>
</tbody>
</table>

The size of the paged and nonpaged memory pools are not precise. These values are taken from internal counters which count duplicated object handles as well as space for
If the Show 16-bit Tasks item in the Options menu is enabled (checked), RTM Manager will also enumerate all 16 bit processes that exist on the system. However, 16 bit processes don't have the following parameters:

- User Name
- Memory
- Mem. Peak
- Page Faults
- VM Size
- VM Peak
- Page File Usage
- Page File Peak
- Paged Pool
- Paged Pool Peak
- NP Pool
- NP Pool Peak
- Handles
- Threads

so these parameters will be blank.

To terminate a process, select it from the list and click on the End Process button or use the context menu that's available with a right-click of your mouse.

If SmartTerminate™ in the Options menu is enabled (checked), RTM Manager will use a special function to close a process correctly (closes all handles opened by that process, unloads all DLLs loaded by the process, etc.) If you terminate a process without the SmartTerminate™ option enabled (e.g. using the common Task Manager) then all the DLLs loaded by that process will still be used and the system will release them only after reboot. To enable SmartTerminate™, select SmartTerminate™ in the Options menu.

If you are terminating a 16 bit process, RTM Manager won't use SmartTerminate™ because it is only for 32 bit processes.

Also, you can terminate a process (and every process directly or indirectly started by that process) by selecting End Process Tree from the context menu. This function is available only for 32 bit processes.
To temporary suspend a process, select **Suspend Process** in the context menu. Rather than terminate the process that is consuming the resource (CPU, network, etc.), suspending permits you to let it continue operation at some later point in time. To resume the suspended process, select it from the list and use **Resume Process** from the context menu.

On **SMP** (multiprocessor) systems, you can control which CPUs a process will be allowed to execute on. **Select Affinity...** in the context menu and designate the CPUs allowed for the process. This function isn't available neither for 16 bit processes nor for uniprocessor systems.

You might want to increase the priority of a process, or decrease the priority of competing processes to improve their response. However, this change lasts only as long as the process runs. When the process is started again, it reverts to the original base priority class. To change the priority of a process, select **Priority** in the context menu. The following fixed values are available:

- **Realtime** - the highest possible priority. The threads of the process preempt the threads of all other processes, including operating system processes performing important tasks.
- **High** - select this value for a process that performs time-critical tasks that must be executed immediately. The threads of the process preempt the threads of normal or idle priority class processes.
- **Above Normal** - process has priority above Normal but below High. This value is available only on systems with Windows 2000 or later.
- **Normal** - select this value for a process with no special scheduling needs.
- **Below Normal** - process has priority above Low but below Normal. This value is available only on systems with Windows 2000 or later.
- **Low** - select this value for a process whose threads run only when the system is idle. The threads of the process are preempted by the threads of any process running in a higher priority class.

Changing the priority isn't available for 16 bit processes but you can change priority for a parent process (ntvdm.exe) and this will affect all 16 bit processes which belong to it.

**WARNING!** Changing the base priority class of a process to Real-Time can destabilize your system. A busy, Real-Time process can prevent other processes and system services from running.

You can see the parent process for a selected process by selecting **Go To Parent** in the context menu. RTM Manager will highlight the record associated with the process that created the selected process. There is a possibility that the parent process no longer exists in the system (e.g. it was closed) so in this case RTM Manager will not change the highlighting of the selected process.

Also, you can see the tree that represents the parent-child relationships of processes. To display the process creation tree, click on the **Process Tree** button.

![Process Tree](image-url)
2.6 Services Manager

The **Services** tab shows the information about the services that are installed on the computer.

- **Name** - name of the service.
- **Internal Name** - internal name of the service as used in the Windows database of services.
- **State** - current state of the service, which may be: *Started*, *Stopped*, *Paused*, *Starting*, *Stopping*, *Continuing* and *Pausing*.
- **Startup** - type of the service's startup (*Automatic*, *Manual* or *Disabled*).
- **Stop** - if the service accepts the *Stop* control code (Yes/No).
- **Pause & Continue** - if the service accepts the *Pause* and *Continue* control codes (Yes/No).
- **Shutdown** - if the service processes the *Shutdown* system event (Yes/No).
- **Type** - the type of service (either *Win32 Own Process* or *Win32 Share Process*).
- **Path** - fully qualified path to the service binary file.
- **Dependencies** - list of services or service groups that must start before the highlighted service.

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Startup</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Alarmer]</td>
<td>Started</td>
<td>Manual</td>
<td>C:\WINNT\Sys\</td>
</tr>
<tr>
<td>Application Management</td>
<td>Started</td>
<td>Manual</td>
<td>C:\WINNT\Sys\</td>
</tr>
<tr>
<td>ClipBook</td>
<td>Started</td>
<td>Automatic</td>
<td>C:\WINNT\Sys\</td>
</tr>
<tr>
<td>COM+ Event System</td>
<td>Started</td>
<td>Manual</td>
<td>C:\WINNT\Sys\</td>
</tr>
<tr>
<td>Computer Browser</td>
<td>Started</td>
<td>Automatic</td>
<td>C:\WINNT\Sys\</td>
</tr>
<tr>
<td>DHCP Client</td>
<td>Started</td>
<td>Automatic</td>
<td>C:\WINNT\Sys\</td>
</tr>
<tr>
<td>Distributed Link Tracking Client</td>
<td>Started</td>
<td>Automatic</td>
<td>C:\WINNT\Sys\</td>
</tr>
</tbody>
</table>

To control the service's state, use either the context menu items or the following buttons:

- **Start** - tries to start a selected service if it's stopped. **NOTE: You can't start a service if its startup type is Disabled.**
- **Restart** - tries to restart (stop and then start) a selected service if it's already started and if its *Stop* control code is set to *Yes*.
- **Stop** - tries to stop a selected service if it's either started or paused and if its *Stop* control code is set to *Yes*.
- **Pause** - tries to pause a selected service if it's started and if its *Pause* control code is set to *Yes*.
- **Continue** - tries to resume a selected service if it's paused and if its *Continue* control code is set to *Yes*.

You can use the *Ctrl* or *Shift* key to select several services simultaneously.

If you try to restart or stop a service that has at least one started dependent service, RTM Manager will ask if you want to restart or stop the dependent service, also.
To see the services which depend on a selected service, select the Dependent Services item from the context menu. RTM Manager will open another copy of Services Manager that will show all the dependent services (if there are any) for a selected service.

If you wish to delete a selected service, use either the Delete item from the context menu or the Delete button. If a service is started, it will be stopped and the service record will be removed from the Windows service database.

To change parameters (name, type, dependencies, account, etc.) and adjust the security for a selected service, use either Edit from the context menu or the Edit button. RTM Manager will show Advanced Service Control Manager where you can edit all the service parameters and change the service security (permissions, audit and ownership).

To create a new service, use the Create button. RTM Manager will display the dialog where you can assign the required service parameters (such as name, type, account, etc.).

To watch the parameters of the process associated with a selected service, use the context menu and select Go To Process. RTM Manager will activate the Processes tab and highlight the record associated with the service's process. This option is not active if a service is stopped.
2.7 Devices Manager

The Devices tab shows the information about the devices that are installed on the computer.

- **Name** - name of the device.
- **Internal Name** - internal name of the device, used in the Windows database of devices.
- **State** - current state of the device, which may be: Started, Stopped, Paused, Starting, Stopping, Continuing and Pausing.
- **Startup** - type of the device's startup (Automatic, Manual, Boot, System or Disabled).
- **Stop** - if the device accepts the Stop control code (Yes/No).
- **Pause & Continue** - if the device accepts the Pause and Continue control codes (Yes/No).
- **Shutdown** - if the device processes the Shutdown system event (Yes/No).
- **Type** - the type of device (either Kernel Driver or File System Driver).
- **Path** - fully qualified path to the device binary file.
- **Dependencies** - list of services or service groups that must start before this device can start.

To control the device's state, you can use either the context menu or the following buttons:

- **Start** - tries to start a selected device if it's stopped. *You can't start the device then its startup type is Disabled.*
- **Restart** - tries to restart (stop and then start) a selected device if it's already started and if it accepts the Stop control code.
- **Stop** - tries to stop a selected device if it's either started or paused and if it accepts the Stop control code.
- **Pause** - tries to pause a selected device if it's started and if it accepts the Pause control code.
- **Continue** - tries to resume a selected device if it's paused and if it accepts the Continue control code.

You can use the *Ctrl* or *Shift* key to select several devices simultaneously.
If you try to restart or stop a device that has at least one started dependent service, RTM Manager will ask if you want to restart or stop the dependent service, also.

To see the services which depend on a selected device, select the Dependent Services item from the context menu. The RTM Manager will open the Services Manager that will show all the dependent services that exist for a selected device.

If you wish to delete a selected device, use either the Delete item from the context menu or the Delete button. If a device is started, it will be stopped and the service record will be removed from the Windows device database.

To change a parameter (name, type, dependencies, etc.) or adjust the security for a selected device, use either the Edit item from the context menu or the Edit button. RTM Manager will show Advanced Service Control Manager where you can edit all of a device's parameters or change its security (permissions, audit and ownership).

To create a new device, use the Create button. RTM Manager will display the dialog where you can assign the required device parameters (such as name, type, etc.).
2.8 Events Manager

The **Events** tab shows the information about the events.

- **Type** - the class of an event in Windows, such as: *Error, Warning, Information, Success Audit, Failure Audit*.
- **Date/Time** - the date and the time when this event was received by the event-logging service.
- **Source** - the software that logged the event, which can be either an application or a component of the system.
- **Event** - an event number to identify the specific event.
- **User** - the name of the user.
- **Computer** - the name of the computer where the logged event occurred.
- **Record N** - just an event serial number in the event log.
- **Generated Date/Time** - the date and the time when this event was generated.

You can change the current event log by selecting one of the following items:

- **System** - lets you manage the System event log. The **System** log records events registered by the Windows system components.
- **Security** - lets you manage the Security event log. The **Security** log records events registered by the Windows security manager. This helps track changes to the security system and identify any possible breach to security.
- **Applications** - lets you manage the Application event log. The **Application** log records events registered by applications.

To view extended information about a selected event, use either the **Detail** button or double-click on event's record in the list. RTM Manager will show the **Event Detail** dialog where you can see all the major information regarding a selected event:

- **Date** - shows the day this event was received by the event-logging service.
- **Time** - shows the hour, minute and second when this event was received by the event-logging service.
- **Source** - the software that logged the event, which can be either an application or a component of the system.
- **Event ID** - an event number to identify the specific event.
- **User** - the name of the user.
- **Computer** - the name of the computer where the logged event occurred.
- **Type** - the class of the event in Windows, which are: *Error, Warning, Information, Success Audit, Failure Audit*.
- **Category** - the event’s category.
- **Description** - a detailed description of the event.
- **Data** - the binary information specific to the event. It could be the contents of the processor registers when a device driver received an error, a dump of an invalid packet received from the network, a dump of all the structures in a program (when a data area is detected as corrupt) and others. This data can be useful to the writer of a device driver or an application when tracking down bugs or unauthorized breaking into the application.

To define a maximum log size and what Windows should do if the event log becomes full, use the *Settings* button. RTM Manager will show a dialog where you can change any parameter for the current event log.
If you wish to archive the current event log, use the Save button. You will need to select a file name where it will be saved. A log is saved in log-file format and you can open an archived log in Event Viewer at any time.

To clear all events from a current event log, press the Clear button. RTM Manager will suggest that you save an event log before clearing it.

Records in the Events tab can be filtered using the Event Filter dialog.
2.9 Performance Monitor

The **Performance** tab displays a dynamic overview of the computer's performance.

**CPU** - the average values of current CPU usage (green histogram) and current CPU's kernel time (red histogram), in percents.

**CPU Usage History:**
- *Total Time* - chart shows total (Kernel Time + User Time) CPU usage history (%).
- *Kernel Time* - chart shows how much time the CPU was in the kernel mode (%).
- *User Time* - chart shows how much time the CPU was in the user mode (%).

You can use the scrollbar at the bottom of each chart to scroll to the next chart.

**CPU0, CPU1, ...** : charts show the usage history for each active CPU in the system (%). RTM Manager supports systems with up to 64 active CPUs. The number of a CPU shows at the top of each chart (e.g. CPU 0, CPU 1, etc.). Only two charts can be simultaneously on the screen, so if the system has more than two CPUs, you should use the scrollbar at the bottom of the chart to the next two charts. If the system has only one or two CPUs, the scrollbar is disabled.

**Memory** - current memory usage (yellow histogram) and maximal peak of memory usage (brown histogram), in kilobytes.

**Memory Usage History** - chart shows the memory usage history (%).

**Totals** - information about currently active handles, threads and processes:
- **Handles** - total number of opened handles in the system.
- **Threads** - total number of running threads in the system.
- **Processes** - total number of running processes in the system.

**Commit Charge (Kb)** - information about memory allocated to programs and the system:
- **Total** - how much memory is currently used (KBytes).
- **Limit** - the maximal number of memory available for programs and the system (KBytes).
- **Peak** - maximal peak of memory used by the programs and system during all the time the system has been active (KBytes).
**Physical Memory (Kb)** - information about physical memory installed on the system:

- **Total** - total amount of physical memory installed on the system (KBytes).
- **Available** - amount of free physical memory (KBytes).
- **System Cache** - amount of physical memory used for system cache (KBytes).
- **System Cache Peak** - maximal peak of physical memory used for system cache during all the time the system has been active (KBytes).

**Kernel Memory (Kb)** - information about memory used by the operating system:

- **Total** - total amount of memory used by the operating system (KBytes).
- **Paged** - total amount of paged memory (KBytes). Paged memory can be used by programs when needed.
- **Nonpaged** - total amount of non-paged memory (KBytes). Non-paged kernel memory is available only to the operating system.

<table>
<thead>
<tr>
<th>Physical Memory (Kb)</th>
<th>Kernel Memory (Kb)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total</strong></td>
<td><strong>Total</strong></td>
</tr>
<tr>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>System Cache</td>
<td>System Cache</td>
</tr>
<tr>
<td>System Cache Peak</td>
<td>System Cache Peak</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Totals</th>
<th>Commit Charge (Kb)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Handles</td>
<td>3617</td>
</tr>
<tr>
<td>Threads</td>
<td>215</td>
</tr>
<tr>
<td>Processes</td>
<td>26</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Total</th>
<th>Limit</th>
<th>Peak</th>
</tr>
</thead>
<tbody>
<tr>
<td>130514</td>
<td>28980</td>
<td>20890</td>
</tr>
<tr>
<td>59532</td>
<td>320328</td>
<td>25244</td>
</tr>
<tr>
<td>71480</td>
<td>128132</td>
<td>3736</td>
</tr>
</tbody>
</table>
2.10 Shares Manager

The Shares tab shows the information about the shared resources that are available on the computer.

- **Share Name** - the shared name of a resource.
- **Comment** - a comment about the shared resource.
- **Share Type** - the type of the shared resource (*Disk Tree, Print Queue, Communication Device, Interprocess Communication* and *Special*).
- **Path** - the local path for the shared resource.
- **User Limit** - the maximum number of concurrent connections that the shared resource can accommodate.
- **Connected Users** - the number of current connections to the resource.

<table>
<thead>
<tr>
<th>Share Name</th>
<th>Comment</th>
<th>Share Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMIN$</td>
<td>Remote Admin</td>
<td>Disk Tree</td>
</tr>
<tr>
<td>C$</td>
<td>Default share</td>
<td>Disk Tree</td>
</tr>
<tr>
<td>D$</td>
<td>Default share</td>
<td>Disk Tree</td>
</tr>
<tr>
<td>IPC$</td>
<td>Remote IPC</td>
<td>Interprocess</td>
</tr>
<tr>
<td>TEMP</td>
<td></td>
<td>Disk Tree</td>
</tr>
</tbody>
</table>

To see the users connected to a selected shared resource, select the **Connected Users** item from the context menu. RTM Manager will open the dialog that will show all the connected users, if any, for a selected resource.

If you want to delete a selected shared resource, use either the **Delete** item from the context menu or the **Delete** button.

To change a comment, user limit or adjust the security for a selected shared resource, use either **Edit** from the context menu or the **Edit** button. RTM Manager will open **Advanced Shares Manager** where you can edit all the resource parameters and change the resource security (*sharing permissions*).

To create a new shared resource, use the **Create New** button. RTM Manager will display a dialog so you can assign the required resource parameters, such as **name**, **type**, **path**, etc.
2.11 Network Monitor

The **Networking** tab displays a graphical representation of network performance. It provides a simple, qualitative indicator that shows the status of the network(s) that are running on the computer. It is useful as a quick reference for determining the amount of network bandwidth being consumed. Please note that the Networking tab is available only if the TCP/IP protocol has been installed.

**Network Usage History:**

- **Total Traffic** - chart shows total (Out. Traffic + In. Traffic) network utilization based on the initial connection speed for the interface (%).
- **Out. Traffic** - chart shows outgoing traffic for the interface (%).
- **In. Traffic** - chart shows incoming traffic for the interface (%).

You can use the scrollbar at the bottom of each chart to scroll to the next chart.

- **Name** - name of the network adapter (interface).
- **Description** - description of the network adapter.
- **Utilization** - network utilization percentage based on the initial connection speed for the interface.
- **Speed** - connection speed of the interface taken from the initial connection speed.
- **Bytes Sent** - the total number of bytes sent on the connection to date.
- **Bytes Received** - the total number of bytes received on the connection to date.
- **Bytes** - the total number of bytes sent and received on the connection to date.
- **Unicasts Sent** - the total number of bytes requested to be transmitted to unicast addresses by higher-level protocols.
- **Unicasts Received** - the total number of bytes received from unicast addresses by higher-level protocols.
- **Unicasts** - the total number of Unicasts Sent and Unicasts Received packets to date.
- **Nonunicasts Sent** - the total number of bytes requested to be transmitted to nonsubnet-unicast addresses by higher-level protocols on the connection to date.
- **Nonunicasts Received** - the total number of bytes from nonsubnet-unicast addresses delivered to higher-level protocols by on the connection to date.
- **Nonunicasts** - the total number of **Nonunicasts Sent** and **Nonunicasts Received** packets to date.
- **MAC Address** - the **Media Access Control (MAC)** address for the network adapter.
- **Legend** - indicates a color of the chart in **Network Usage History** for the interface.
- **Actual Speed** - current connection speed.

<table>
<thead>
<tr>
<th>Name</th>
<th>Utilization</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel EtherExpress PRO/100B PCl LAN Adapter</td>
<td>0.07 %</td>
<td>100 Mbps</td>
</tr>
<tr>
<td>Intel EtherExpress PRO/100B PCl LAN Adapter</td>
<td>0.06 %</td>
<td>10 Mbps</td>
</tr>
</tbody>
</table>

You can see an extended information for a selected interface by selecting **Properties...** in the context menu.

**Network Interface Properties**

Name: Local Area Connection
Description: Intel 8255x-based Integrated Fast Ethernet
Type: Ethernet
MAC Address: 00-A0-C9-23-25-5C
Speed: 100 Mbps
MTU: 1500

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.2</td>
<td>255.255.0.0</td>
</tr>
</tbody>
</table>

- **Name** - name of the network adapter (interface).
- **Description** - description of the network adapter.
- **Type** - type of the interface (**Ethernet**, **PPP**, **SLIP**, etc.).
- **MAC Address** - the **Media Access Control (MAC)** address for the network adapter.
- **Speed** - connection speed of the interface taken from the initial connection speed.
- **MTU** - Maximum Transmission Unit (a maximum frame size that cannot be exceeded).
- **IP Address** - the IP address associated with the interface.
- **Subnet Mask** - the subnet mask for **IP Address**.
2.12 Hardware Resources

The **Hardware Resources** tab displays information about resource assignments and possible sharing conflicts among DMA, I/O, IRQs, and Memory resources on the computer.

- **Resource** - resource that is being used by the device.
- **Device** - name of the device.
- **Interface Type** - type of the interface (Isa, PCI, Internal, Plug and Play, etc.) that is being used by the device.
- **Internal Name** - internal name of the device, used in the Windows database of devices.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Device</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRQ 0</td>
<td>System timer</td>
<td></td>
</tr>
<tr>
<td>IRQ 1</td>
<td>Standard 101/102-Key or Microsoft Natural PS/2 Keyboard</td>
<td>Plug and Play</td>
</tr>
<tr>
<td>IRQ 5</td>
<td>Printer Port (LPT1)</td>
<td>Isa</td>
</tr>
<tr>
<td>IRQ 6</td>
<td>Standard floppy disk controller</td>
<td>Plug and Play</td>
</tr>
<tr>
<td>IRQ 7</td>
<td>Adaptec SlimSCSI 16-Bit PCMCIA SCSI Host Adapter</td>
<td>Isa</td>
</tr>
<tr>
<td>IRQ 8</td>
<td>System CMOS/real time clock</td>
<td>Plug and Play</td>
</tr>
</tbody>
</table>

You can change the current list by selecting one of the following items:

- **DMA** - information about the system’s direct memory access. DMA transfers data between system memory and hardware devices without passing it through the CPU. The **Resource** column displays the DMA channel that is being used by the device, which is listed in the **Device** column.

- **I/O** - information about the communication channel among hardware devices. The **Resource** column displays the resource that is used by an I/O device, which appears in the **Device** column.

- **IRQs** - information about interrupt request channels on the system, and indicates which devices are assigned to each channel. The **Resource** column displays the IRQ channel that is being used by the device, which is listed in the **Device** column.

- **Memory** - information about memory address ranges which are being used for communication between devices and the operating system. The **Resource** column displays the memory address of the device that is listed in the **Device** column.
To change a parameter (name, type, dependencies, etc.) or adjust the security for a selected device, use the Edit item from the context menu. RTM Manager will show Advanced Service Control Manager where you can edit all of a device's parameters or change its security (permissions, audit and ownership). This option is active only if a device has an internal name.

To watch the parameters of the device in the Windows database of devices, use the context menu and select Go To Device. RTM Manager will activate the Devices tab and highlight the record associated with the device. This option is active only if a device has an internal name.
2.13 NetStat

The **NetStat** tab displays the current TCP/IP network connections (TCP and UDP endpoints). *Please note that the NetStat tab is available only if the TCP/IP protocol has been installed.*

- **Image Name** - the name of the process that owns a connection.
- **PID** - the process identifier.
- **Local Address** - the connection’s local address.
- **Local Port** - the connection's local port.
- **Remote Address** - the connection's remote address (exists only if the TCP connection is active).
- **Remote Port** - the connection's remote port (exists only if the TCP connection is active).
- **State** - the connection's state: **LISTENING**, **ESTABLISHED**, **CLOSING**, etc. (only for TCP connections).
- **Protocol** - the protocol that is used to open a connection (**TCP** or **UDP**).

<table>
<thead>
<tr>
<th>Image Name</th>
<th>PID</th>
<th>Local Address</th>
<th>Local Port</th>
<th>Remote Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>3</td>
<td>localhost</td>
<td>1234</td>
<td>5678</td>
</tr>
<tr>
<td>System</td>
<td>3</td>
<td>localhost</td>
<td>1234</td>
<td>5678</td>
</tr>
<tr>
<td>System</td>
<td>3</td>
<td>localhost</td>
<td>1234</td>
<td>5678</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>376</td>
<td>localhost</td>
<td>1234</td>
<td>5678</td>
</tr>
<tr>
<td>svchost.exe</td>
<td>376</td>
<td>localhost</td>
<td>1234</td>
<td>5678</td>
</tr>
<tr>
<td>PLService.exe</td>
<td>552</td>
<td>localhost</td>
<td>1234</td>
<td>5678</td>
</tr>
</tbody>
</table>

To toggle the display of resolved names, click **Resolve Addresses**. If **Resolve Addresses** is checked, RTM Manager tries to resolve IP addresses and ports to their name (**DNS**) versions, otherwise it shows their numeric representation.

You can close active TCP connections (those are labeled with a state of **ESTABLISHED**) by pressing the **Close Connection** button (you can also use the context menu).

To watch the parameters of the process associated with a selected connection, use the context menu and select **Go To Processes**. RTM Manager will activate the **Processes** tab and highlight the record associated with the connection's process.
2.14 Security Patch Analyzer

The **Security Patch Analyzer** tab performs security patch assessment for the following operating systems and applications: Windows NT 4.0/2000/XP/Server 2003, IIS 4.0/5.0, SQL Server 7.0/2000, MSDE 2000, MDAC 2.5-2.8, MSXML 2.6/3.0/4.0/5.0, IE 5.01 and later, Exchange 5.5/2000/2003, Windows Media Player 6.4 and later, Microsoft Virtual Machine, Microsoft Office and so on. *Please note that the Security Patch Analyzer tab is available only if the Microsoft XML Parser (MSXML) version 4.0 or later has been installed.*

- **Product Type** - the product affected by the patch.
- **Status** - identifies the type of notice.
- **Bulletin** - refers to the Microsoft Security Bulletin article that explains the patch.
- **Patch Name** - the name of the patch's executable file.
- **QNumbers** - refers to the Microsoft Knowledge Base article that contains information about the patch.
- **Title** - the brief description of the flaw.
- **Reason** - the reason why the patch was considered not found.
- **Included In** - the name of the service pack (Cumulative Rollup package) the patch has been included in.
- **Location** - the link that can be used to download the patch.

<table>
<thead>
<tr>
<th>Product Type</th>
<th>Status</th>
<th>Bulletin</th>
<th>Patch Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDAC 2.6</td>
<td>Missing Service Pack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSXML 3.0</td>
<td>Missing Service Pack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Office XP</td>
<td>Missing Service Pack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows NT Workstation 4.0</td>
<td>Missing Patch</td>
<td>M501-041</td>
<td>Q299444i.iex</td>
</tr>
<tr>
<td>Windows NT Workstation 4.0</td>
<td>Missing Patch</td>
<td>M502-029</td>
<td>Q313126i.iex</td>
</tr>
<tr>
<td>Windows NT Workstation 4.0</td>
<td>Missing Patch</td>
<td>M503-037</td>
<td>VBA64-K8822</td>
</tr>
</tbody>
</table>

Security Patch Analyzer can determine which critical security updates are applied to a system by referring to an Extensible Markup Language (XML) file (mssecure.xml) that is continuously updated and released by Microsoft. The XML file contains information about which security updates are available for particular Microsoft products.

When you run Security Patch Analyzer, RTM Manager should download a copy of the compressed XML file (mssecure.cab) and then decompresses the CAB file to the RTM’s directory on your local computer. *The machine must be capable of obtaining the patch database XML file from a location on the Internet (via http).*
To view extended information about a selected patch, use either the *Detail* button or double-click on patch’s record in the list. RTM Manager will show the **Properties** dialog where you can see all the major information regarding a selected patch.

![Properties Dialog](image)

<table>
<thead>
<tr>
<th>Patch Details</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status:</td>
<td>Missing Patch</td>
</tr>
<tr>
<td>MS Severity:</td>
<td>Critical</td>
</tr>
</tbody>
</table>

| CVEID:        | CAN-2003-0347 |
|---------------|--| |
| Bugtraq ID:   | 9524 |
| Included In:  | Office XP SP3 |
| Posted:       | 2003/03/03 |
| Revised:      | 2003/03/03 |
| Supported:    | Yes |

**Title**

Flaw in Visual Basic for Applications Could Allow Arbitrary Code execution (822715)

**Bulletin ID:** [MS03-037](#)

[Microsoft Knowledge Base Article: 822715, 822035, 822036, 822150](#)

**Summary**

Microsoft VBA is a development technology for developing client desktop packaged applications and integrating them with existing data and systems. Microsoft VBA is based on the Microsoft Visual Basic development system. Microsoft Office products include VBA and make use of VBA to perform certain functions. VBA can also be used to build customized applications based around an existing host application. A flaw exists in the way VBA checks document properties passed to it when a document is opened by the host application. A buffer overrun exists which if exploited successfully could allow an attacker to execute code of their choice in the context of the logged on user. In order for an attack to be successful, a user would have to open a specially crafted document sent to them by an attacker. This document could be any type of:

- File C:\Program Files\Common Files\microsoft shared\vbs\vba6\vbes.dll has a file version [6.3.31.3] that is less than what is expected [6.4.35.03]
2.15 Advanced Service Control Manager, General

Use this tab to view or change the general parameters of a device or service. This tab is also used when creating a device or service.

<table>
<thead>
<tr>
<th>Service Name:</th>
<th>Alerter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name:</td>
<td>Alerter</td>
</tr>
<tr>
<td>Path to executable:</td>
<td>C:\WINNT\System32\services.exe</td>
</tr>
<tr>
<td>Description:</td>
<td>Notifies selected users and computers of administr</td>
</tr>
</tbody>
</table>

Service Name: - the internal name of a service or device used in the Windows database of services or devices.

Display Name: - the name of a service or device.

Path to executable: - the fully qualified path to a service's or device's binary file.

Description: - a comment explaining the purpose of a service or device.

Status: - the current state of a service, which may be: Started, Stopped, Paused, Starting, Stopping, Continuing or Pausing.

Start parameters: - any number of arguments, separated by spaces, which are passed to a service or device when it is starting. If the service or device isn't in the stopped state, these parameters are ignored.

Error Control - specifies the severity of an error if a service or device fails to start during startup, and determines the action taken by the startup program if failure occurs. One of the following values can be specified:
- **Ignore** - the startup (boot) program logs the error but continues the startup operation.

- **Normal** - the startup program logs the error and displays a message box pop-up but continues the startup operation.

- **Severe** - the startup program logs the error. If the last known good configuration is being started, the startup operation continues. Otherwise, the system is restarted using the last known good configuration.

- **Critical** - the startup program logs the error, if possible. If the last known good configuration is being started, the startup operation fails. Otherwise, the system is restarted with the last known good configuration.

**Service** - specifies the type of service or device. One of the following values can be specified:

- **Win32 Own Process** - a service type that indicates a service that runs in its own process.

- **Win32 Share Process** - a service type that indicates a service that shares a process with other services.

- **Kernel Driver** - a device type that indicates a device driver.

- **File System Driver** - a device type that indicates a file system driver.

**StartUp** - specifies when to start a service or device. One of the following values can be specified:

- **Automatic** - specifies a device or service started by the Service Control Manager automatically during system startup.

- **Manual** - specifies a device or service started manually by the user.

- **Disabled** - specifies a device or service that can no longer be started.

- **Boot** - specifies a device started by the System Loader.

- **System** - specifies a device started during system initialization.

To control the state of a service or device, use the following buttons:

- **Start** - tries to start the selected device or service if it's stopped. **NOTE: you can't start a device or service if its startup type is Disabled.**

- **Restart** - tries to restart the selected device or service if it's started.
- **Stop** - tries to stop the selected device or service if it's either started or paused and if it was set to accept the *Stop* control code.

- **Pause** - tries to pause a selected device or service if it's started and if it was set to accept the *Pause* control code.

- **Continue** - tries to resume a selected device or service if it's paused and if it was set to accept the *Continue* control code.

If you try to restart or stop a device or service that has at least one started dependent service, **Advanced Service Control Manager** will ask if you want to restart or stop the dependent service, also.
2.16 Advanced Service Control Manager, Log On

Use this tab to view or change logon parameters of a service and to enable or disable a device or service for hardware profiles. This tab is also used when creating a device or service.

**Log On As** - specifies the account name the service process will have when it is run, which can be:

- **System account** - the service will be logged on as a *LocalSystem* account.
- This account: - the account name in the form of DomainName\Username. On Windows NT systems, this parameter is available only for *Win32 Own Process* services.

**Allow system to interact with desktop** - a flag that indicates a service application that can interact with the desktop. This parameter is available only for a service that was logged on as a *LocalSystem* account.

**Choose User...** - shows the dialog where you can select any user that is available on the system. If the **Log On As** is set to **System** account, this button is disabled.

**Password:** - a password for a user account specified in This account:. If the **Log On As** is set to **System** account, this parameter is disabled.

**Confirm Password:** - here you must type a password for a user account once more to avoid a mistake.

To enable or disable a device or service for a hardware profile, select the hardware profile you want to configure and press the **Enable** or **Disable** button. Using Ctrl and Shift you can enable or disable several hardware profiles simultaneously. Use the System applet in Control Panel to create hardware profiles and set their order of preference.
2.17 Advanced Service Control Manager, Recovery

Use this tab to view or change service recovery parameters. This tab represents the action the service controller should take for each failure of a service. **It is available only on Windows 2000/XP systems.**

<table>
<thead>
<tr>
<th>Action to take when service fails:</th>
</tr>
</thead>
<tbody>
<tr>
<td>First attempt:</td>
</tr>
<tr>
<td>Second attempt:</td>
</tr>
<tr>
<td>Subsequent attempt:</td>
</tr>
<tr>
<td>Reset 'Fail Count' to zero after:</td>
</tr>
<tr>
<td>Restart service delay</td>
</tr>
<tr>
<td>Run file:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>First attempt:</strong></th>
<th><strong>Restart the Service</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Second attempt:</strong></td>
<td><strong>Run a File</strong></td>
</tr>
<tr>
<td><strong>Subsequent attempt:</strong></td>
<td><strong>Reboot the Computer</strong></td>
</tr>
<tr>
<td><strong>Reset 'Fail Count' to zero after:</strong></td>
<td>0 Hour(s)</td>
</tr>
<tr>
<td><strong>Restart service delay:</strong></td>
<td>1 Minute(s)</td>
</tr>
<tr>
<td><strong>Run file:</strong></td>
<td><strong>test.bat</strong></td>
</tr>
<tr>
<td><strong>Command line parameters:</strong></td>
<td><strong>Append 'Fail Count' to end of command line /Fail=%1%</strong></td>
</tr>
</tbody>
</table>

**First attempt:** - specifies the action the service controller should take on first failure of a service.

**Second attempt:** - specifies the action the service controller should take on second failure of a service.

**Subsequent attempt:** - specifies the action the service controller should take on all subsequent failures of a service.

- **Take No Action** - specifies that no action is to be taken.
- **Restart the Service** - the service controller tries to restart the service.
- **Run a File** - the service controller tries to run an external file.
- **Reboot the Computer** - the service controller tries to reboot the computer.

**Reset 'Fail Count' to zero after:** - indicates the length of time, in hours, after which the failure count is reset to zero if there were no failures in that time.

**Restart service delay** - specifies the time to wait before performing the **Restart the Service** action, in minutes. This parameter is available only if the **Restart the Service** was selected.
Run the following file: - specifies the path to the executable file to execute in response to the Run a File service controller action. This process runs under the same account as the service. This parameter is available only if the Run a File was selected. **Do not specify programs or scripts that require user input.**

Command line parameters: - specifies the arguments for a program specified in the Run the following file:. This parameter is available only if the Run a File was selected.

Append 'Fail Count' to end of command line (/fail=%1%) - a flag that indicates whether or not the /fail=%1% argument is to be added to the command line or not. The service controller replaces %1% with the value from the internal failure count. This parameter is available only if the Run a File was selected.

Reboot Computer Information... - shows the dialog where you can specify the message to be broadcast to server users before rebooting in response to the Reboot the Computer service controller action. This button is enabled only if the Reboot the Computer was selected.
2.18 Advanced Service Control Manager, Dependencies

Use this tab to view or change the dependencies of a service or device. This tab is also used when creating a service or device.

Load Order Group - names of the load ordering group of which this service or device is a member. The startup program uses this list to load groups of services or devices in a specified order with respect to the other groups in the list. You can place a service or device in a group so that another service or device can depend on that group.

Dependencies - names of services or load ordering groups that must start before this service or device. Dependency on a service or device means that this service or device can only run if the service it depends on is running. Dependency on a group means that this service can run if at least one member of the group is running after an attempt to start all members of the group.

Services - list of the services available in the system.

Service Groups - list of the load ordering groups available in the system.

To add dependencies to a service or device, select the name of either the service (using Services) or of the load ordering groups (using Service Groups), then use the << button to add these to the Dependencies list. You can use the Ctrl or Shift key to select several records simultaneously from both Services and Service Groups.

To remove dependencies from a service or device, select their records in the Dependencies list then use the >> button. You can use the Ctrl or Shift key to select several records simultaneously.
2.19 Advanced Service Control Manager, Security

Use this tab to view or change a service's or device's security parameters.

To view or set permission information on a service or device, use the Permissions button.

When a service or device is created, the Service Control Manager assigns default permissions to the service or device object. You can use this dialog to change default permissions.

Please note that granting certain access privileges to untrusted users can allow them to interfere with the execution of your service or device, and might allow them to run applications under a LocalSystem account.

To view or set auditing information on a service or device, use the Auditing button.

Auditing can inform you of actions that could pose a security risk and also identify the user accounts from which audited actions were taken. Note that auditing only tells you what user accounts were used for the audited events. When an audited event occurs, an entry is added to the Windows security log. The security log can be viewed using the Events Manager tab.

To view or take ownership of a service or device, use the Ownership button.

The user who creates a service or device is the owner of that object. The owner of a service or device can always grant permissions on that object, even if a member of the Admins group has revoked his or her explicit permissions on that object.
2.20 Advanced Service Control Manager, Permissions

Use this dialog to view or change user permissions for a service or device.

**Service Name:** - indicates the name of a service or device.

**Owner Name:** - indicates the owner's name of a service or device.

**Accounts** - indicates the name of a user or users group.

**Access Type** - specifies the type of access for a user or users group, which can be:

- **Allowed** - indicates that all selected rights will be allowed for a selected user or users group.

- **Denied** - indicates that all selected rights won't be allowed for a selected user or users group.

**Rights** - the list of all available rights for a service or device, which can be:

- **Start** - enables the starting of a service or device.

- **Stop** - enables the stopping of a service or device.

- **Pause** - enables the pausing and continuing of a service or device.

- **User Defined Control** - enables a user-defined action for a service or device.

- **Query Status** - enables the querying of the status (state) of a service or device.
- **Interrogate** - enables the requesting of a service or device to update its current status information.

- **Enum Dependencies** - enables the enumerating of dependencies for a service or device.

- **Query Configuration** - enables the reading of a service's or device's configuration.

- **Change Configuration** - enables the changing of a service's or device's configuration.

- **Delete** - enables the deleting of a service or device.

- **Query Security** - enables the reading of a service's or device's security.

- **Change Security** - enables the changing of a service's or device's security.

- **Change Owner** - enables the changing of a service's or device's owner.

To add a new user or users group to an account's list, use the *Add* button. You can add several accounts simultaneously.

To delete a record from the account's list, use the *Remove* button. Using *Ctrl* or *Shift* you can remove several records simultaneously.

If you wish to set default permissions for a service or device, use the *Set Default* button. Default permissions are enabled by using one of the following access selections:

- the *Everyone* account has *Query Configuration*, *Query Status*, *Enum Dependencies*, *Interrogate* and *User Defined Control* rights.

- members of the *Power Users* group and the *LocalSystem* account have *Start*, *Stop* and *Pause* rights, plus all the rights granted to *Everyone*.

- members of the *Administrators* and *System Operators* groups have all rights.

*Please note that granting certain access privileges to untrusted users can allow them to interfere with the execution of your service or device, and might also allow them to run applications under the LocalSystem account.*
2.21 Advanced Service Control Manager, Auditing

Use this dialog to view or change auditing parameters for a service or device.

Service Auditing

Service Name: Alerter
Owner Name: SYSTEM

<table>
<thead>
<tr>
<th>Accounts</th>
<th>Rights</th>
<th>Success</th>
<th>Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everyone</td>
<td>Start</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Stop</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Pause</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>User Defined Control</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Query Status</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Interrogate</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Enum Dependecies</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Query Configuration</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Change Configuration</td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>

Service Name: - indicates the name of a service or device.
Owner Name: - indicates the owner's name of a service or device.
Accounts - is the name of the user or user group.
Rights - the list of all available actions which can be audited:

- **Start** - audit a start action.
- **Stop** - audit a stop action.
- **Pause** - audit a pause/continue action.
- **User Defined Control** - audit a user-defined action.
- **Query Status** - audit a query-the-status (state) action.
- **Interrogate** - audit an update-current-status-information action.
- **Enum Dependecies** - audit an enumerate-dependencies action.
- **Query Configuration** - audit a read-configuration action.
- **Change Configuration** - audit a change-configuration action.
- **Delete** - audit a delete action.
- **Query Security** - audit a read-security action.
- **Change Security** - audit a change-security action.
- **Change Owner** - audit a change-owner action.

**Success** - enables the audit of successful actions.

**Failure** - enables the audit of non-successful actions.

To add a new user or group to an account’s list, use the **Add** button. You can add several accounts simultaneously.

To delete a record from an account’s list, use the **Remove** button. Using **Ctrl** and **Shift** you can remove several records simultaneously.

If you wish to set the default auditing parameters for a service or device, use the **Set Default** button. The default auditing parameters enable the **Everyone** account for all non-successful actions.

To be able to audit a service or a device, you must first use **Local Security Policy Snap-in** (on Windows NT 4.0 you must use the **Audit Policy** dialog of **User Manager**) to enable the auditing of object access events. You can enable the auditing of successful events or of failed events or of both. This establishes the global object-access auditing policy for the system. The global policy determines whether or not object-specific auditing will occur, whether or not to record access events for a particular service or device. To enable this level of auditing detail, you must also specify the type of auditing to be performed for that service or device.
2.22 Advanced Service Control Manager, Ownership

Use this dialog to view or change the owner of a service or device.

![Owner dialog]

Service Name: - indicates the name of a service or device.

Owner Name: - indicates the owner name of a service or device.

To take ownership over a service or device, use the Take Ownership button.

The user who creates a service or device is the owner of that object. The owner of a service or device can always grant permissions on that object, even if a member of the Admin group has revoked his or her explicit permissions on that object.
2.23 Advanced Service Control Manager, SNMP Agent

The simple network management protocol (SNMP) agent provides the related management system with information on activities that occur at the Internet Protocol (IP) network layer. Use this tab to view or change the agent properties of the SNMP service.

Contact: - the name of the person to contact, such as the network administrator.

Location: - the physical location of the computer or the contact.

Physical - this computer manages physical devices, such as a hard disk partition.

Applications - this computer uses any applications that send data using the TCP/IP protocol suite. This service should always be enabled.

Datalink and subnetwork - this computer manages a bridge.

Internet - this computer is an IP gateway (router).

End-to-end - this computer is an IP host. This service should always be enabled.

If you change Contact or Location SNMP settings, your changes take effect within a few minutes.
2.24 Advanced Service Control Manager, SNMP Traps

Use this tab to view or change trap destinations of the SNMP service. The SNMP service generates trap messages if any specific events occur. These messages are sent to a trap destination. For example, an agent can be configured to initiate an authentication trap if a request for information is sent by an unrecognized management system.

**Community name** - the list of community names to which this computer will send trap messages. Community name is a name used to group SNMP hosts. This name is placed in SNMP messages sent between SNMP-managed devices such as Windows 2000-based server computers and SNMP management stations. Typically, all hosts belong to *Public*, which is the standard name for a common community of all SNMP hosts.

You can assign groups of hosts to SNMP communities for limited security checking of agents and management systems or for administrative purposes. Communities are identified by community names that you assign. A host can belong to multiple communities at the same time, but an agent does not accept a request from a management system outside its list of acceptable community names.

Please note that there is no relationship between community names and domain or workgroup names.

Press the *Add* button to add new community name or press the *Remove* button to delete a selected community from the list.
Trap destinations - the list of trap destinations for a community selected in the Community name list. Trap destinations consist of the computer name or the IP or IPX address of the management system. The trap destination must be a network-enabled host that is running SNMP management software. Trap destinations can be configured by a user, but the events (such as a system reboot) that generate a trap message are internally defined by the SNMP agent.

Press the Add button to add new computer name, IP or IPX address to a selected community. To edit a trap destination, press the Edit button. Press the Remove button to delete a selected trap destination from the list.

If you change existing SNMP settings, your changes take effect immediately. The SNMP service does not need to be restarted for your settings to take effect.
2.25 Advanced Service Control Manager, SNMP Security

Use this tab to view or change SNMP security of the SNMP service. SNMP provides security through the use of community names and authentication traps. You can restrict SNMP communications for the agent, allowing it to communicate with only a specific list of other SNMP management systems.

Send authentication trap - authentication is the process of verifying that a host name or address is valid. When the SNMP agent receives a request that does not contain the correct community name or is not sent from a member of the acceptable host list, the agent sends an authentication trap message to one or more trap destinations (management systems), indicating the failure of authentication.

Accepted community names - the service requires at least one default community name. Public is the common community name that is universally accepted in all SNMP implementations. The community names configured here are used in trap destinations. If an SNMP request is received from a community which is not on this list, it will generate an authentication trap.

You can add multiple community names, and delete or change the community name.

Please note that if you remove all the community names, including the default name Public, SNMP does not respond to any community names presented.

Community rights - a permission level can be selected, determining how the SNMP agent processes requests from a selected community. For example, you can configure the
permission level to block the SNMP agent from processing any requests from a specific community.

Accept SNMP packets from any host - in this context, the source host and list of acceptable hosts are the source SNMP management system and the list of acceptable management systems. No SNMP packets are rejected on the basis of the name or address of the source host or the list of acceptable hosts.

Accept SNMP packets from these hosts - in this context, the list of acceptable hosts means the acceptable SNMP management systems. When this radio button is selected, only SNMP packets received from the hosts in this list are accepted. Otherwise, the SNMP message is rejected and an authentication trap sent. This selection provides greater security than using a community name, which might contain many hosts.

Press the Add button to add the host name, IP or IPX address to this list. To edit a selected record, press the Edit button. Press the Remove button to delete a selected host name, IP or IPX address from the list.

The default SNMP Security tab settings are one community name, Public, and Accept SNMP packets from any host. For greater security, these settings should be changed to a specific community name of your choice and Accept SNMP packets from these hosts, with a list of hosts. The settings should be monitored and updated on an ongoing basis.

If you change existing SNMP settings, your changes take effect immediately. The SNMP service does not need to be restarted for your settings to take effect.
2.26 Advanced Share Manager, General

Use this tab to view or change the general parameters for shared resources. This tab is also used when creating a shared resource.

Share Name: - the share name of a resource. This parameter is enabled when creating new shared resource.

Path: - the local path for the shared resource. This parameter is enabled when creating new shared resource.

Comment: - the comment about the shared resource.

Share Type: - the type of the shared resource. This parameter is enabled when creating new shared resource. One of the following values can be specified:

- Disk Tree
- Print Queue
- Communication Device
- Interprocess Communication

Special: - a flag that indicates a special share reserved for interprocess communication (IPC$) or remote administration of the server (ADMIN$). Can also refer to administrative shares such as C$, D$, E$, and so forth. This parameter is enabled when creating new shared resource.

User Limit: - the maximum number of concurrent connections that the shared resource can accommodate:

- Maximum Allowed - the number of connections is unlimited.
- Allow ... Users - used to specify the number of concurrent connections that the shared resource can accommodate.

Connected Users: - the number of current connections to the resource.
2.27 Advanced Share Manager, Sharing Permissions

Use this tab to view or change user permissions for a shared resource. There are a few special resources, such as `IPC$`, `ADMIN$`, `C$`, etc. that have hard-coded (unchangeable) permissions. These special resources are tools for network administrators and their security settings cannot be viewed or changed.

<table>
<thead>
<tr>
<th>Share Name: TEMP</th>
<th>Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounts</td>
<td>Access Type</td>
</tr>
<tr>
<td>Everyone</td>
<td>Allowed</td>
</tr>
<tr>
<td></td>
<td>List Directory</td>
</tr>
<tr>
<td></td>
<td>Read</td>
</tr>
<tr>
<td></td>
<td>Write</td>
</tr>
<tr>
<td></td>
<td>Delete/Rename</td>
</tr>
<tr>
<td></td>
<td>Execute</td>
</tr>
<tr>
<td></td>
<td>Change Security</td>
</tr>
<tr>
<td></td>
<td>Take Ownership</td>
</tr>
</tbody>
</table>

*Share Name*: - the name of a resource.

*Accounts* - the name of a user or users group.

*Access Type* - specifies the type of access for a user or users group, which can be:

- *Allowed* - all selected rights will be allowed for a selected user or users group.
- *Denied* - all selected rights will NOT be allowed for a selected user or users group.

*Rights* - the list of all available rights for a shared resource, which can be:

- *List Directory* - enables the reading of a directory's contents.
- *Read* - enables the reading of a file or directory.
- *Write* - enables the writing to a file or directory.
- *Delete/Rename* - enables the deleting and renaming of a file or directory. Please note that on Windows NT 4.0 this right also automatically enables the Execute right.
- **Execute** - enables the executing of a file. *Please note that on Windows NT 4.0 you cannot disable this right if the Delete/Rename right is enabled. You must disable the Delete/Rename first.*

- **Change Security** - enables the changing of a file's security.

- **Take Ownership** - enables the changing of a file's owner.

To add a new user or users group to an account's list, use the *Add* button. You can add several accounts simultaneously.

To delete a record from the account's list, use the *Remove* button. Using *Ctrl* or *Shift* you can remove several records simultaneously.
2.28 Advanced Share Manager, Connected Users

Use this dialog to view a list of all the users connected over the network to the shared resource. Or, you can disconnect one or all of the users connected to the resource.

<table>
<thead>
<tr>
<th>Share Name:</th>
<th>IPC$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected Users:</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Users</th>
<th>Computer</th>
<th>Opens</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Users</td>
<td>SL_SERVER</td>
<td>0</td>
<td>2:67:53:55</td>
</tr>
<tr>
<td>All Users</td>
<td>TERMINAL4</td>
<td>1</td>
<td>0:15:59</td>
</tr>
<tr>
<td>vit</td>
<td>DIR</td>
<td>0</td>
<td>0:16:16</td>
</tr>
<tr>
<td>ashot</td>
<td>PRO</td>
<td>3</td>
<td>0:10:25</td>
</tr>
<tr>
<td>All Users</td>
<td>BUHGS</td>
<td>0</td>
<td>0:00:14</td>
</tr>
<tr>
<td>All Users</td>
<td>PRO</td>
<td>0</td>
<td>0:00:14</td>
</tr>
</tbody>
</table>

- Disconnect
- Disconnect All
- In Use

**Share Name:** - indicates the name of a resource.

**Connected Users:** - the total number of users connected to the selected shared resource.

**Users:** - this column lists the users who are connected to the selected shared resource. Each entry consists of a user account icon, followed by a user name. In some cases, the All Users name may be displayed instead of the user name.

**Computer:** - the computer name of the connected user's computer.

**Opens:** - the number of resources opened by the user.

**Time:** - the hours, minutes and seconds that have elapsed since the user first connected to the selected shared resource.

To disconnect a user from all shared resources, select the user name from the list and press the **Disconnect** button. You can use the **Ctrl** or **Shift** key to select several records simultaneously.

To disconnect all users from all shared resources, press the **Disconnect All** button. *Please note that warn users before disconnecting them. If you do not, they may lose data.*

While you are remotely administering another computer, your user account is listed as a connected user for the IPC$ share, it will not be disconnected.

To view a list of the files, directories, pipes, etc. opened by the selected user, press the **In Use** button.
2.29 Advanced Share Manager, Open Resources

Use this dialog to view a list of the files, directories, pipes, etc. that are opened by the user selected in the Connected Users dialog. With this dialog you can also close an open resource or all open resources.

![Open Resources on \SL_SERVER dialog]

**User:** - this column shows the user who has opened the resource. An open resource could be:

- a file
- a named pipe
- a print job in a print spooler
- a communication-device queue
- a resource of an unrecognized type

In some cases, a print job is shown here as an open named pipe.

**Path:** - the path of the open resource.

**Permissions:** - the permission granted when the resource was opened:

- **R** - permission to read a resource.
- **W** - permission to write to a resource.
- **C** - permission to create a resource.
- **E** - permission to execute a resource
**Locks:** - the total number of file locks on open resources.

To close the resource, select the resource's record from the list, then press the *Close Resource* button. You can use the *Ctrl* or *Shift* key to select several records simultaneously.

To close all resources, press the *Close All Resources* button. *Please note that warn connected users before closing resources. If you do not, they may lose data.*

While you are remotely administering another computer, your connection is displayed here as an open named pipe. It will not be closed.
2.30 Remote Shutdown

Use this dialog either to shutdown a remote computer or to abort the shutting down of a remote computer.

Press the F4 key or select Remote Shutdown from the File menu to quickly access the Remote Shutdown dialog at any time.

- **Computer Name** - the name of the computer you wish to shutdown. You can either type in the name or select it from the list. An empty string indicates the local computer (Local Machine).

- **Net Browser** - shows a dialog where you can select any computer available in your network.

- **Computer List** - lets you select any computer from the custom list of computers.

- **Timeout** - a time (in seconds) that the warning message should be displayed.

- **Reboot After Shutdown** - specifies whether the computer is to restart immediately after shutting down.

- **Forces Processes To Terminate** - specifies whether applications with unsaved changes are to be forcibly closed.

- **Message to display in the shutdown dialog box:** - a warning message to display in the shutdown dialog box (if the Timeout is zero then the message will not be displayed).
To shutdown or reboot a selected computer, press the *Shut down the computer* button.

The warning message will be displayed on the computer (if the *Timeout* is not zero) and the computer will be shut down or rebooted after the number of seconds has elapsed as specified in *Timeout*. If the *Timeout* is not zero, you will be able to abort the process of shutting down.

RTM Manager will show the **Abort Shutdown** dialog with the following buttons:

- **Abort Shutdown** - use this button to abort the shutting down of the computer.
- **Close** - use this button to return to the **Remote Shutdown** dialog without aborting the computer's shutting down.

If the process of shutting down was already started on a selected computer, RTM Manager will show the **Abort Shutdown** dialog and you will be able to abort the computer's shutdown (see above).
2.31 Remote Execute

Use this dialog to create new processes on a remote computer.

Press the F6 key or select Remote Execute from the File menu to quickly access the Remote Execute dialog at any time. Also, you can use the New Task... button in the Applications Manager.

- **Computer Name** - the name of the computer you wish to create a process on. You can either type its name or select it from the list. An empty string indicates the local computer (Local Machine).

- **Net Browser** - shows the dialog where you can select any computer that is available in your network.

- **Computer List** - lets you select any computer from the custom list of computers.

- **Run As:** - specifies whether a process will be created under the account of a current user or under the account of any other user.

- **User** - specifies the user account used when logging onto a process. If Run As: is unchecked then the current user account will be used.

- **Password** - a password for the user account specified in User (above). If Run As: is unchecked then this parameter is ignored.

- **...** - shows a dialog where you can select any user available on the system. If Run As: is unchecked then this button is disabled.
- **Load User Profile** - specifies whether a user's profile will be loaded or the default profile will be used.

- **Prepare Environment** - specifies whether an environment for the user will be loaded or the default environment will be used. If **Load User Profile** is unchecked then this parameter is ignored.

- **Allow application to interact with desktop** - specifies whether a process will be created that has access to a user's desktop or not. You can either specify the desktop name, which is case insensitive, or leave it empty so the **Default** desktop will be used.

- **Command Line** - specifies the path to the executable file and any number of arguments for the program that are separated by spaces.

To create a process on a selected computer, use the **Execute** button.
2.32 Remote Lock

Use this dialog to lock a remote computer. Using **Remote Lock** is similar to pressing `CTRL+ALT+DEL` then clicking *Lock Workstation* on the local computer.

Press the *F7* key or select *Remote Lock* from the *File* menu to quickly access the **Remote Lock** dialog at any time.

- **Computer Name** - the name of the computer you wish to lock. You can either type in the name or select it from the list. An empty string indicates the local computer (*Local Machine*).

- **Net Browser** - shows the dialog where you can select any computer that is available in your network.

- **Computer List** - lets you select any computer from the custom list of computers.

To lock a selected computer, press the *Lock Workstation* button.
2.33 System Information

Use this dialog to see an extended information about the operating system (OS) and computer.

Press the SysInfo button to quickly access the System Information dialog at any time. Please note that the System Information dialog is available only in the full (registered) version of Remote Task Manager!

### System Information

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kernel Version</td>
<td>Uniprocessor Free</td>
</tr>
<tr>
<td>Product Version</td>
<td>5.0.2195</td>
</tr>
<tr>
<td>Service Pack</td>
<td>2</td>
</tr>
<tr>
<td>Installed</td>
<td>11.05.2001 22:22:38</td>
</tr>
<tr>
<td>Started</td>
<td>24.01.2002 21:50:13</td>
</tr>
<tr>
<td>Last Shutdown</td>
<td>24.01.2002 1:12:26</td>
</tr>
<tr>
<td>Registered Organization</td>
<td>SmartLine, Inc.</td>
</tr>
<tr>
<td>Registered Owner</td>
<td>Ashok Oganesyan</td>
</tr>
<tr>
<td>Product Id</td>
<td>51073-335-6221665-09593</td>
</tr>
<tr>
<td>System Root</td>
<td>C:\WINNT</td>
</tr>
<tr>
<td>System Partition</td>
<td>\Device\Harddisk\Volume1</td>
</tr>
<tr>
<td>Page File</td>
<td>C:\pagefile.sys (Min: 2 MB, Max: 2 MB)</td>
</tr>
<tr>
<td>System Identifier</td>
<td>AT\AT COMPATIBLE</td>
</tr>
<tr>
<td>BIOS Date</td>
<td>12/15/99</td>
</tr>
<tr>
<td>Video BIOS Date</td>
<td>06/10/99</td>
</tr>
<tr>
<td>Processors</td>
<td>1</td>
</tr>
<tr>
<td>Processor Type</td>
<td>x86 Family 6 Model 0 Stepping 1, GenuineIntel</td>
</tr>
<tr>
<td>Processor Speed</td>
<td>~498 MHz</td>
</tr>
<tr>
<td>Hotfixes</td>
<td>9</td>
</tr>
</tbody>
</table>
| Q302755           | Windows 2000 Hotfix [Pre-SP3] [See Q302755 for ...]
| Q299796           | Windows 2000 Hotfix [Pre-SP3] [See Q299796 for ...]
| Q299553           | Windows 2000 Hotfix [Pre-SP3] [See Q299553 for ...]
| Q298012           | Windows 2000 Hotfix [Pre-SP3] [See Q298012 for more info]
| Q285651           | Windows 2000 Hotfix [Pre-SP3] [See Q285651 for ...]
| Q285156           | Windows 2000 Hotfix [Pre-SP3] [See Q285156 for ...]
| Q279471           | Windows 2000 Hotfix [Pre-SP3] [See Q279471 for ...]

- **Kernel Version** - type of the OS's kernel (uniprocessor or multiprocessor, free or debug/checked).
- **Product Type** - type of the installed OS (e.g. Windows .Net Server).
- **Product Version** - the OS version (including major version, minor version and build number).
- **Service Pack** - version of the installed Service Pack (if any).
- **Installed** - the date and the time when OS was installed.
- **Started** - the date and the time when OS was started.
- **Last Shutdown** - the date and the time when OS was shut down last time.
- **IE Version** - version of Internet Explorer (including major version, minor version and build number).
- **Registered Organization** - registration information (if any) that was entered during Windows Setup.
- **Registered Owner** - registration information (if any) that was entered during Windows Setup.
- **Product Id** - serial number that was entered during Windows Setup.
- **System Root** - the path to the directory where the Operating System is installed.
- **System Partition** - name of the active (boot) partition in the native format.
- **Page File** - the path to a page (swap) file. Also, this parameter shows initial and maximum limit (MBytes) for the page file.
- **System Identifier** - indicates the computer’s type.
- **BIOS Version** - version of the system BIOS.
- **BIOS Date** - date of the system BIOS.
- **Video BIOS Version** - version of the video card’s BIOS.
- **Video BIOS Date** - date of the video card’s BIOS.
- **Video BIOS String** - data the Video BIOS reports to the Operating System (data such as an extended version number).
- **Video Adapter String** - data the Video Adapter (video card) reports to the Operating System (data such as the Video Adapter name).
- **Video Chip** - type of chipset the video card uses.
- **Video DAC** - type of DAC (Digital-to-Analog Converter) the video card uses.
- **Video Memory** - total amount of physical memory installed on the video card.
- **Display Refresh Freq**. - current vertical refresh rate for the display (Hz). The refresh rate for a monitor is the number of times the screen is redrawn per second (frequency).
- **Display Setting** - current display’s resolution (in pixels) and number of bits used to represent the color of each pixel (bits per pixel).
- **Processor(s)** - number of processors and processor’s name.
- **Processor Type** - type of the processor (family, model and stepping).
- **Processor Speed** - processor's approximate frequency (MHz).
- **Hotfixes** - number of installed hot fixes (if any).

To save the system information listing to an external file, press the **Save** button and select the type of file to save as.
3. RTM Service

3.1 Installation

RTM Service can be installed to any computer running Windows NT/2000/XP and Windows Server 2003.

To install RTM Service just run Setup (setup.exe).

RTM Service installs to the directory of your choice. Setup tries to find a RTM Service installation and, if one exists, Setup suggests you install RTM Service to the same directory. If a previous installation does not exist, Setup suggests you install RTM Service to the Program Files directory on the system drive (e.g. C:\Program Files\Remote Task Manager). You can always select another directory for installation.

You have two choices: install both RTM Service and RTM Manager using Typical setup or you can install only RTM Service using Custom setup, then selecting the RTM Service component.

Also, Setup supports unattended (silent) setups. This gives an install that can be used from within a batch file. If you want to install RTM Service without user intervention run Setup with the /s parameter (e.g. c:\setup.exe /s). There is a special configuration file for silent setups — setup.ini. Setup.ini must be in the same directory where setup.exe is located. With this file, you can customize the installation parameters. For example, to install only RTM Service, setup.ini should look like:

```
[Install]
Service = 1
Manager = 0
Documents = 0
```

If you have purchased a license for Remote Task Manager, you can also specify the location of its registration file in the setup.ini file so Setup automatically registers new versions of a service:

```
RegFileDir = C:\Directory
```

where C:\Directory is where your registration file is located.

You can also specify a destination directory for Remote Task Manager:

```
InstallDir = C:\Program Files\Remote Task Manager
```
If you want to run a program (e.g. batch file) after a successful install, you can specify the *Run* parameter:

\[\text{Misc}\]
\[\text{Run} = C:\\mybatchfile.bat\]

Remote Task Manager supports remote installation to help a Systems Administrator to set up a service on remote machines without ever having to physically go to them. If the RTM Service isn't installed on the remote system you are trying to connect to, RTM Manager will suggest that you install the service. Select the RTM Service executable file (*rtmservice.exe*) and RTM Manager will copy it to the remote computer. The RTM Service executable file will be copied to the Windows system directory (e.g. *c:\winnt\system32*) if this service doesn't exist on this system. If the service exists on this system but is too old, RTM Manager will copy the executable file to the directory of the old file and the old file will be replaced.
4. RTM Console

4.1 Installation

RTM Console can be installed to any computer running Windows NT/2000/XP, Windows Server 2003 and Windows 95/98/Me.

To install RTM Console just run Setup (setup.exe).

RTM Console installs to the directory of your choice. Setup tries to find a RTM Console installation and, if one exists, Setup suggests you install RTM Console to the same directory. If a previous installation does not exist, Setup suggests you install RTM Console to the Program Files directory on the system drive (e.g. C:\Program Files\Remote Task Manager). You can always select another directory for installation.

You should install RTM Console using Custom setup, then selecting the RTM Console component.

After a successful install, you can run RTM Console from the command line:

C:\Directory\Remote Task Manager\rtmc.exe

where C:\Directory is where RTM Console is installed.
4.2 Usage

Typing `rtmc` displays RTM Console’s usage syntax:

```
rtmc -command[=parameter] [-switch1[=parameter]] [-switchN[=parameter]]
```

Commands:

- `?` - displays all commands and switches with brief descriptions.
- `desk` - displays all active desktops on a computer.
- `app[=<desktop>]` - displays all running applications. You can either specify a desktop name - which is case insensitive - or leave it empty so the default (Default) desktop is used.
- `proc[=<PID>]` - displays all running processes or detailed information for any specified process. You can use the `term`, `suspend`, `resume` and `thread` switches (see below) with this command.
- `perf[=nousage]` - displays the computer's performance. Specify `nousage` to stop calculating the CPU usage.
- `lock` - locks a computer. Using the `lock` command is similar to pressing `CTRL+ALT+DEL` then clicking Lock Workstation on a local computer.
- `shut[=<message>]` - shuts down a computer or aborts the shutting down of a computer. You can use the `reboot`, `force`, `timeout` and `abort` switches with this command.
- `exe=<command line>` - creates new processes on a computer. The `command line` parameter is the name of the process's executable file. Also it can contain any number of arguments that are separated by spaces. You can use the `profile`, `env`, `int`, `runasuser` and `runaspass` switches with this command.
- `net` - displays information about the network connections.

Switches:

- `comp=<computer>` - specifies the computer you want to manage. RTM Service must be installed and running on that computer.
- `user=<username>` - if you want to connect to a remote computer and the account you are executing in does not have administrative privileges on the remote system then you must login as an administrator using this switch. The parameter `username` is a domain name followed by a backslash (`\`) and the user name, e.g. `D1\John`.
- `pass=<password>` - a password for the user account. If `user` is not specified then this switch is ignored.
- **auth=<1...6>** - level of authentication to be performed on the remote call.

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>performs no authentication</td>
</tr>
<tr>
<td>2</td>
<td>authenticates only when RTM Console establishes a relationship with RTM Service</td>
</tr>
<tr>
<td>3,4</td>
<td>verifies only that all data received is from the expected source</td>
</tr>
<tr>
<td>5</td>
<td>authenticates and verifies that none of the data transferred between RTM Console and RTM Service has been modified</td>
</tr>
<tr>
<td>6</td>
<td>authenticates all previous levels and encrypts the argument value of each remote call</td>
</tr>
</tbody>
</table>

- **term[=nosmart]** - terminates a specified process. Specify nosmart to stop use the SmartTerminate™ technology. This switch is valid only with the proc command (PID must be greater than zero).

- **suspend** - suspends a specified process. This switch is valid only with the proc command (PID must be greater than zero).

- **resume** - resumes a specified process. This switch is valid only with the proc command (PID must be greater than zero).

- **thread** - displays all threads for a specified process. This switch is valid only with the proc command.

- **priority=<0…5>** - changes the priority of a specified process (0 - idle, 5 - real time). This switch is valid only with the proc command.

- **reboot** - specifies whether the computer is to restart immediately after shutting down. This switch is valid only with the shut command.

- **force** - specifies whether applications with unsaved changes are to be forcibly closed. This switch is valid only with the shut command.

- **timeout=<seconds>** - a time (in seconds) that a warning message is to be displayed. The warning message will be displayed on the computer (if timeout is not zero) and the computer will be shut down or rebooted after the number of seconds has elapsed as specified in timeout. This switch is valid only with the shut command.

- **abort** - if the process of shutting down was already started on a selected computer, you can abort that computer's shutdown. This switch is valid only with the shut command.

- **profile** - specifies a user's profile is to be loaded instead of the default profile. This switch is valid only with the exe command.

- **env** - specifies an environment for the user is to be loaded instead of the default environment. If profile is not specified then this switch is ignored. This switch is valid only with the exe command.

- **int[=<desktop>]** - specifies whether a process will be created that has access to a user's desktop or not. You can either specify the desktop name - which is case
Insensitive - or leave it empty so the default (Default) desktop is used. This switch is valid only with the exe command.

- runasuser=<user> - specifies whether a process will be created under the account of a current user or under the account of any other user. The parameter user is a domain name followed by a backslash (\) and the user name, e.g. D1\John. This switch is valid only with the exe command.

- runaspass=<password> - a password for the user account specified in runasuser. If runasuser is not specified then this switch is ignored. This switch is valid only with the exe command.

You must enclose with quotation marks any parameters that contain spaces, e.g. rtmc -exe="C:\Program Files\My App\myapp.exe".
4.3 Examples

The following command displays all running applications for the default (Default) desktop on pro:

```
rtmc -app=default -comp=pro
```

This command shows extended information for the system process (PID = 8) on acerlaptop:

```
rtmc -proc=8 -comp=acerlaptop
```
This command locks the local system:

`rtmc -lock`

D:\MSDEV\Projects\RIM\rtmanager\Release>rtmc -lock
Remote Task Manager Console v1.0
Copyright © 2001 SmartLine, Inc. www.ntutility.com
Computer: Local Machine <Windows NT 4.0.1381 Service Pack 6>
Workstation has been locked!
D:\MSDEV\Projects\RIM\rtmanager\Release>