

# Toptools 5.5 Release Notes

## **Build A.05.51**

**August, 2001**

### *Table of Contents*

[General Information](#)

[Toptools Device Manager Release Notes](#)

[CD Contents](#)

[Upgrading from Previous Versions](#)

[System Prerequisites and New Installations](#)

[Installing on non-English Versions of NT](#)

[Accessing Toptools from Your Browser](#)

[Adding Components after Initial Installation](#)

[Toptools Services](#)

[Discovery and SNMP Community Names](#)

[Support for DHCP Environments](#)

[Toptools for Desktops Release Notes](#)

[Toptools for Servers Release Notes](#)

[Toptools Remote Control Card Release Notes](#)

[Toptools for Hubs and Switches Release Notes](#)

### **General Information**

This readme file is designed to help you get started using Toptools 5.5. This release includes new features and enhancements to previous versions of Toptools.

Toptools is a web-based tool for helping you track your HP PC, Omnibook, Netserver and HP-UX computer assets, upgrade drivers and firmware, manage your HP hubs and switches, manage your HP printers, and keep track of your network resources. It is based on industry standards: SNMP, DMI, WMI, TCP/IP, and HTTP. It is designed to compliment your existing network and system administration infrastructure and investments, while helping lower the total cost of ownership by providing management from anywhere via its intuitive browser-based user interface.

The core of the Toptools application, referred to as Toptools Device Manager, runs on an HP PC, Omnibook, or HP Netserver under Microsoft Windows NT 4.0, Windows 2000 or Windows XP. Agents for PCs (DMI, SNMP, or WMI), Netservers (Windows, Netware or Linux), and HP-UX servers and workstations (DMI) need to be installed separately on the client machines. HP hubs, switches, remote control cards, and printers come with their management agents built-in. Non-HP devices, such as PCs, must also have their respective agents installed. The applications for managing Netservers, Remote Control Cards, Hubs and Switches, or Desktops and Laptops are all part of the Toptools application and can be installed at the same time as you install the Device Manager or added later.

Everything you need to install Toptools is packaged into one setup wizard. It will check your system for all prerequisites and necessary software and install all missing pieces, except for SNMP services for any version of Windows and IIS for Win2000 or WinXP, for which you must provide the relevant Windows OS CD when prompted. The wizard will guide through these steps. If you wish to update your installation later by adding components you did not add on the initial install, simply rerun the install wizard and check those components you want to add. The install wizard will do the rest.

[Return to Main Table of Contents](#)

# Toptools Device Manager 5.5 Release Notes

July, 2001

## Contents

[What's New in This Release](#)

[Security Enhancements](#)

[Known Limitations and Caveats](#)

## What's New in This Release

This release contains many new features and enhancements to previous releases of Toptools. These include the following features:

1. The System Performance Advisor is completely integrated into this release and can be used to monitor cpu, memory, io, and disk storage usage on any Windows system. The Performance menu includes the System Performance page, which shows the current performance data, grouped by custom group. The System Performance Standard Report gives a snapshot of the data collected, and there is a custom report wizard so you can create your own detailed performance reports.
2. Discovery determines if a system is running pcAnywhere, and a menu item is added to such systems in the Device Selector, which launches the web-based interface to pcAnywhere.
3. Discovery determines if a system is running NTWebAdmin and a menu item is added to such systems in the Device Selector, which launches this application.
4. You can export the contents of the right pane of the Device Selector (any detailed view including search results) to either HTML or a csv file. If you have Microsoft Excel installed on the system on which you do a csv format export, you can directly open the export in Excel.
5. You can create custom reports off the Inventory menu and save the reports in Excel or Word format.
6. Configure Actions on Alerts supports using custom groups as specific devices to initiate an action upon receipt of alerts of given severity.
7. Configure Actions on Alerts supports writing to the NT Event Log as an action.
8. There is a special report (Frequent Alerts) on the Alerts menu, which lists the top 20 alerting devices.
9. Three utilities are included in the ...hptt\bin directory:
  - Mib2Imp – this utility imports trap definitions from 3<sup>rd</sup> party vendor's MIBs for decoding traps in the alert viewer.
  - SetTTPassword – this utility enables you to change the Toptools admin password without having to uninstall the product
  - TTAddDevices – this utility imports into the database a list of devices to discover

## New Devices Supported

HP-UX workstations and servers with DMI are automatically discovered and inventoried. You must install the DMI agent on the systems and configure the Toptools Device Manager's IP address into the DMI configuration files. EMS formatted alerts can also be sent to the device manager.

1. Microsoft clusters are discovered. A new grouping in the Device Selector (Clusters) shows these clusters and drilling down will list the systems that make up the clusters.
2. APC UPS's are discovered, as well as the ability to launch the web-based embedded management application from APC. Traps can be received and are formatted.
3. IA-64 boxes running Win2000 or WInXP are discovered and inventoried.
4. HP Netservers running Linux are discovered and inventoried (requires 5.5x agents).

## Property Page Enhancements

New property pages for HP-UX workstations and servers.

1. New property pages for Microsoft Clusters.
2. New property pages for APC UPS devices.

3. Status and Configuration pages have been reworked to separate status information from configuration information, with links between these pages.
4. In the Netserver property pages an action to “locate” a system in a rack has been added in the Tools page. The Hard Disk Status and Memory Status applets have been reworked. The Configuration pages give more detailed information than before, including PCI slot and memory slot information.
5. Netservers running Linux with the latest Tootools agents (5.5 or later) have property pages similar to Windows systems.
6. Instant Support Tuner settings have been added under the Configuration tab (HP PCs and Netservers).
7. Support pages have links to HP’s PartSurfer (where you can order upgrades or replacement parts) and Smart Search where you can find support answers.
8. You can enter rack information on the Configuration/Settings page for any server or networking device. This information is written back to Netservers running the latest 5.5 agents, and written to the managed element database in any case. Once entered, this information is also available on the Identity and Configuration pages and in the detailed report page.
9. For HP PCs with both front and rear usb ports, you can enable or disable these ports from the Security/System Settings page.

### ***Inventory Reports***

1. There is a new Windows XP migration report, listing all PCs that meet minimal requirements for running Windows XP. (Similar to the Windows 2000 migration report.)
2. There is a new Racked Systems report that details all racked systems that have information entered (in the Configuration/Settings) page.
3. There is a new Server Drivers report listing all the driver versions in Netservers running the latest 5.5 agents.
4. There is a new Server Firmware report listing all the firmware versions in Netservers running the latest 5.5 agents.
5. The Hubs, Switches and Routers reports return more information on firmware versions.
6. There is a new Remote Control Cards report listing version and asset information.
7. There is a new HP9000 Server report (requires the DMI agent to be installed on the servers).

### ***Device Selector Enhancements***

1. A series of slashes (/, // or ///) is used to denote the presence of WBEM (/), the presence of Win2000 or WinXP (//), and the presence of the HP WMI agent (///).
2. From the Security/Instant Support Settings page you can set passwords and e-mail recipients for a whole collection of machines at once.
3. You can view the system performance of a specific machine.
4. You can launch hp servicecontrol manager for HP-UX systems.
5. You can launch a Telnet window for any device supporting telnet.
6. There is a new grouping for network storage devices.
7. There is a new grouping for clusters, which lists the clusters themselves as well as allowing drill down to the specific devices in the cluster.
8. You can launch the Instant Support Tuner on those systems on which it is installed.

### ***Discovery Enhancements***

1. The node limit restrictions have been removed. You can discover as many devices on you network as you want, subject only to the resources available on the Tootools server.
2. Manual additions of devices no longer read the arp cache of a device (and subsequent discovery of those devices). This limits manual adds to just those devices you want.
3. Manual additions of devices that are not PCs will automatically enable ping for the device.
4. Updating Discovery off the Device Selector menu for a single or multiple devices also updates the inventory information.
5. Discovery can identify non-HP PCs and servers better.

6. Discovery can determine the mac address of HP PCs and Netservers if they have the latest HP agents installed (SNMP not required).
7. Discovery determines if a device is part of a cluster and “relates” the devices.
8. Discovery can find HP’s SAN monitoring management agent (CommandView) and launch its pages.
9. Discovery determines if Instant Toptools is installed on a Netserver, and sets the “management url” to that application. From the Device Selector, launching the “Management Home Page” will open Instant Toptools’ web pages.

***Driver and Firmware Updates***

1. Driver, firmware and agent updates are integrated for HP PCs, HP Netservers, HP Omnibooks, and HP Visualize workstations. Note: For Netservers running Data Center be aware that updating a driver that has not been certified by Microsoft will result in a non-supported Data Center configuration.
2. You can view and deploy updates for multiple types of drivers for multiple systems simultaneously.
3. Status of updates is reported under Alerts -> Drivers/Firmware Update Status.
4. You can schedule when the Device Manager will go to the HP website and download updated information on what new drivers and firmware packages are available.

***Alert Enhancements***

1. Paging is enabled by sending an e-mail message to your service provider, which in turn will send the page.
2. There is a new action (Test alert), which can be used to test the actions you choose.
3. You can elect to automatically delete unacknowledged alerts after “n” days. Note that you will still need to periodically “compact” the alerts database. See the on-line Help for more information.
4. There is a summary report on driver and firmware updates (success/failure).

***Security Enhancements***

Toptools uses an elaborate system to guarantee that only authorized users are allowed access. This is done via a combination of Windows user permissions and extra permissions granted via Toptools user roles. Each Toptools user is assigned to one of three roles:

1. Administrators: users that are allowed full access to all Toptools functionality.
2. Operators: users that are allowed to use Toptools to manage devices on a network, but who are not allowed to change any settings on the management server itself.
3. Users: users that are allowed “read-only” access to Toptools and to managed devices.

Assignment of these user roles is done via Windows group membership:

Windows group	Toptools user role
<management server>\Administrators	Administrator
<management server>\Toptools Admins	Administrator
<management server>\Toptools Operators	Operator
<management server>\Toptools	User

*Note that starting with HP Toptools version 5.5, these Windows groups are now always **local** to the management server. In previous versions, these groups were typically domain groups. The behavior is the same, except that administration may be simpler because local groups are allowed to have other groups as members, whereas domain groups are not.*

Toptools uses two special user accounts: a **remote access account** for accessing managed devices, and a **local service account** for running local Toptools components on the management server. The remote access account is of particular importance in Toptools security since that account is usually highly privileged. See **Remotely accessing managed devices** for more details about this account. The Toptools setup wizard will create these accounts, if desired, with the default names “Toptools admin” and “Toptools service”. The “Toptools service” account, for running Toptools components, will be local to the management server and will be a member of the local Administrators group. The “Toptools admin” account, for remote access, will be either a domain administrator or a local administrator account, depending on the rights of the user that installs Toptools. If the setup wizard cannot create a domain administrator account, then it will create a local administrator account in order to allow Toptools to run, even though a local administrator account will not give Toptools any remote access rights beyond those granted to anonymous users.

*Prior to version 5.5, Toptools used a single account named “Toptools User” both for remote access and for local services.*

Either or both of these accounts may be changed, either when Toptools is installed, or later, using a utility program called SetTTPassword

During installation, the Toptools setup wizard will prompt for both the local service account name/password and the remote access account name/password. Existing accounts may be specified instead of the suggested defaults, and Toptools will be configured to use whatever accounts are specified. If alternate names are specified, but the specified accounts do not yet exist, then the Toptools setup wizard will create the accounts with the specified names. Again, if the wizard cannot create a domain administrator account for remote access, it will create a local administrator account, even though that account will not give Toptools any remote access rights beyond “anonymous” access.

In addition to any local logon rights that are necessary for the remote access account and the local service account, the setup wizard and SetTTPassword will also grant the “Log on as a service” right to the remote access account on the domain controller, if the remote access account is a domain account. This logon right is necessary to temporarily run a service on a managed device as part of the agent deployment process. If the user doing the Toptools installation or running SetTTPassword does not have sufficient rights to make this change on the domain controller, then this step must be completed manually before agent deployment will work.

The security of the Toptools application on the management server is a function of all of these areas:

1. **The web server** (Microsoft IIS) grants access via a web browser only to members of the Windows groups detailed above. The Toptools setup wizard will configure the web application appropriately<sup>1</sup>, but administrators need to understand how those groups work in order to control access.
2. **Toptools** itself will enable or disable certain functionality depending on the role of the current user. Again, it is important to understand how the Windows group membership works in order to ensure an appropriate level of access for Toptools users.

---

<sup>1</sup> If use of a Netscape browser with Toptools is desired, then the access permissions on the “Hptt” web application must be modified to allow “Basic” authentication, since Netscape does not support Windows authentication. Note that unless SSL is used, passwords are sent in **clear text** with Basic authentication!

3. **The file system** (if NTFS) grants access to Tootools files only to members of the Windows groups detailed above. This is a further level of security that is configured by the setup wizard when Tootools is installed. Administrators need to understand that there are potential security implications if NTFS file and directory permissions are changed from the default settings. It is also important to understand the importance of NTFS itself vs. the FAT/FAT32 file system. Without NTFS, there is no file system security on Tootools files, and all users will appear to be Tootools Administrators.
4. **The management server** itself must be physically and logically protected from tampering. Due care should be given with respect to who is allowed to log on to the management server and who has access to the administrative password for the management server, etc. One should also consider who has remote access to the management server via Microsoft Terminal Services or pcAnywhere, etc. (and whether such access is encrypted).

### ***Remotely accessing managed devices***

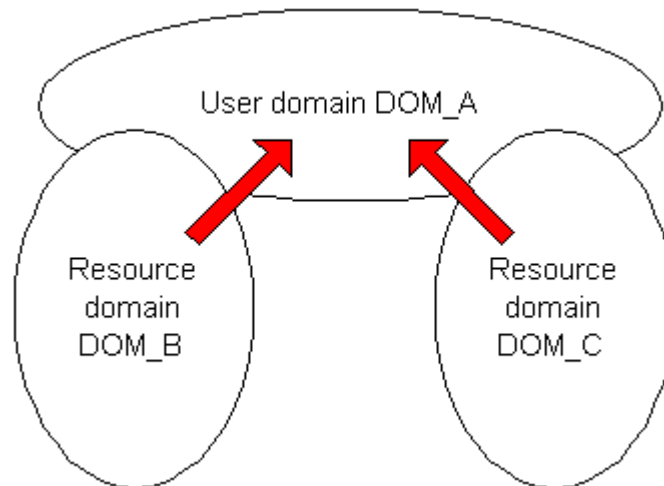
There are several areas of functionality for which Tootools needs special remote access rights: discovering the network, deploying agents, and performing some actions such as displaying Windows 2000 Properties pages<sup>2</sup>. Deploying agents requires the most rights, since the account that Tootools uses must be a local administrator on the managed device to which an agent is deployed. WMI, which is used both in Discovery and in displaying Windows 2000 Properties pages, is less stringent since all that is required is that the remote access account have WMI read access on managed devices. A security-conscious Tootools administrator could, if desired, specify an ordinary, non-administrator user account for Tootools remote access if only WMI functionality was needed (no agent pushes). Administration might be more difficult in that each managed device would have to be modified to grant WMI access to the non-administrator account, but it is possible to configure a network that way.

Much depends on whether Windows domains are used, vs. workgroups, and whether Tootools will be used to manage devices in only one domain or across multiple domains. The simplest scenario involves a single Windows domain. Domain administrators are usually also local administrators on every machine in a domain, so choosing a domain administrator account (e.g. "Tootools admin") for Tootools remote access makes administration very easy. Everything will just work as expected within that domain.

A more complex scenario involves managing multiple Windows domains. For example, some corporate networks are organized with one "user" (or "master") domain and multiple "resource" domains, as follows:

---

<sup>2</sup> Another area is Microsoft cluster management, although that area is still under investigation.



Toptools would typically be installed on a machine that is a member of one of the resource domains. However, since trust relationships (shown in red) would likely not be transitive in this scenario, a remote access account created in one resource domain could not be authenticated in the others.

The solution in this case would be to create a remote access account in the user domain and to specify that account during TopTools setup or via SetTTPassword. Unfortunately, it is not easy to grant such an account the administrative rights that are needed to manage devices in resource domains. The Windows “Domain Admins” group has the limitation that it may only have members from the same domain, so it is not possible to make the remote access account a domain administrator in each of the multiple resource domains. Rather, the remote access account must be individually added to the local Administrators group on each managed device.

Another scenario involves managing a Windows workgroup, not a domain. While much of Toptools will work, the following Toptools functionality is **not supported** in a workgroup environment:

1. Agent deployment (except HP server agent package upgrades)
2. WMI access

### ***Making changes after installation***

After Toptools has been installed, it is possible to change the password and optionally the account name that Toptools uses, either for the remote access account or for the local service account, using the SetTTPassword command-line utility. The syntax for this command is:

```
SetTTPassword {-r|-s} password ["domain\account name"]
-r = the account Toptools will use for remote access, e.g. "Toptools admin"
-s = the account Toptools will use for local services, e.g. "Toptools service"
```

If a new account name is specified, SetTTPassword will first verify that the account exists and then grant any necessary logon rights for that account. If it is the remote access account, and the account is a domain account, then SetTTPassword will also attempt to grant the “Log on as a service” right on the domain controller so that agent deployment will work. If a new local service account is specified, then the user must ensure that the account is a member of the local Administrators group.

SetTTPassword does not attempt to create a new Windows user account, nor does it attempt to change a Windows account password. SetTTPassword only stores an account name and password for use by Toptools and grants the necessary logon rights so that Toptools can use that account. Windows administrative tools may be used to configure a user account with the appropriate name and password. It is the user’s responsibility to verify that the password passed to SetTTPassword is correct.

A user must be a local administrator on the Toptools management server in order to run SetTTPassword.

## **Securing the Toptools Management Server**

The Toptools Management Server is a Windows system running Microsoft's web server, either IIS or PWS. The Toptools Management Server will normally be installed on the corporate LAN. If the LAN has internet access, a firewall will normally be used to prevent anyone on the public Internet from accessing any machines inside the corporation. Thus only users with direct access to the corporate LAN can access Toptools. To prevent unauthorized users within the corporation from accessing Toptools, the security mechanisms of the web server and Windows are used.

**HP strongly recommends installing the Toptools Management Server on Windows with the NTFS file system to prevent unauthorized access to Toptools**

Several checks are made to authorize access to the web server:

- Anonymous access allows any user to access a web page. You may turn off anonymous access for the 'hptt' web directory, so that only users with valid user names and passwords can access the web server; use the 'Internet Service Manager' to make changes.
- IIS and PWS support two ways to authenticate a user:  
**Basic Authentication** will cause the web browser to display a dialog requesting the user's name and password, and this NT user name and password is passed over the network to the web server. If you are using a Netscape browser, this authentication method must be used. The Internet Service Manager can be used to change this setting.

**NT Challenge/Response** securely identifies the Windows' user without passing passwords over the wire to the web server. NT Challenge/Response is much more secure, is recommended, and is the default web server configuration. The Internet Service Manager can be used to change this setting.

- When installed on the NTFS file system only, access to Toptools can be restricted to specific users or groups of users. By default the 'hptt' web directory is restricted to users who are members of the 'Administrators' group on the Toptools Management Server, or of the 'Toptools' group defined in the domain user database. Authorized users may be added to these groups using the NT User Manager for Domains.

## **Securing Managed Devices**

The Toptools management server communicates with managed devices using SNMP, DMI, or WMI over the local network. To prevent unauthorized users within the corporation from controlling managed devices using their own copy of a management tool, passwords or community names should be set on the managed devices. Only administrators who know these passwords will then be able to set up management tools such as Toptools.

### **DMI Devices**

Any user with a DMI tool such as Toptools can look at DMI information on a PC. HP PCs have a password that can be set to prevent unauthorized access to sensitive operations such as BIOS flash, keyboard lock, and remote reboot.

**HP strongly recommends setting passwords on all DMI devices**

Toptools can set the 'Power-On' or DMI administrator's password on one or more PCs:

- Use the 'Devices' button to bring up a list of PCs, and select those to be modified.
- From the 'Actions' menu, select 'Security->Set System Passwords'
- Type in the new Administrator password for the PCs and press 'Save Admin Password'. A user password can also be set.

The PCs will be updated with the new password, and the Toptools database will store this password for use

in future operations. If a PC already has a password, or the password is set locally on the PC, then the Toptools database must be updated with this password. Follow the steps above and type in the existing password.

### ***SNMP Devices***

SNMP Devices are secured using 'Community Names', which are often separate for read access ('Get') and write access ('Set'). Most SNMP devices have a default community name of 'public' for read access to SNMP data.

**HP strongly recommends 'set' community names on all SNMP devices**

### ***WMI Devices***

Devices that support WMI, such as computers running Windows2000, are secured using NT account information. Toptools will request WMI information using the Toptools User account, which will normally have access rights to the WMI data on any PC within the same NT domain or trusted domain as the management server.

Note that for some actions like updating the BIOS or changing the BIOS' configuration of a PC the "DMI password", which is in fact the BIOS administrator's password, is still needed.

Users can be given read access to WMI data by adding them to the 'WBEM Users' group on each managed device. By default administrators have access to WMI data.

[Return to Device Manager Contents](#)

[Return to Main Table of Contents](#)

## ***Known Limitations and Caveats***

**Description:** A warning message will be generated on Win 2000 SP1 systems when collecting disk performance data.

**Workaround:** This is a problem with Win2000 SP1 only. Install Win 2000 SP2 on the systems data is being collected on.

---

**Description:** A Windows XP device appears as "Not Connected" when managed from a Toptools Device Manager running on Win2000.

**Cause:** Microsoft made a change to the WBEM security model between Win 2000 and Win XP which prevents Toptools from connecting via WBEM to an XP device.

**Workaround:** Install Windows 2000 SP2 on the system running the device manager.

---

**Description:** The "host management server" column of the Remote Control Card Report displays hex characters for some Remote Control Cards. Selecting "Related Devices" in the device selector for the server containing this card shows an unknown device. Trying to launch it displays "This page cannot be found" and trying to launch "remote control" does nothing.

**Cause:** Version B.02.03 of the Remote Control Card does not correctly support the mib used to relate the devices. (Check the Version column in the report.)

**Workaround:** A fix is forth-coming from HP. In the meantime, you can "back flash" the firmware on the RCC to version B.02.02 or earlier.

---

**Description:** If you change the user name or password for the Instant Support settings in the Configuration tab of the Property page or under the Actions->Security menu item, you need to stop and start the Instant Support tuner on the target system before they will take effect.

---

**Description:** Occasionally, a DMI alert will not be reported to the management server.

**Cause:** Most probably, the server was down when the alert was generated and the client machine removed the destination address of the management server. Discovery will re-establish this link on its next run.

**Verification:** You can verify this is the cause by selecting the PC in the device selector, selecting "Properties", go to the "Configuration" tab, select "Explore PC", select Win32 DMI service layer, SP Indication Subscription and looking for the IP address of the management server. If it is not shown, this was the cause.

**Workaround:** Wait for discovery to run.

---

**Description:** On PWS, you may get HTTP Error 403: Too many users are connected.

**Cause:** PWS supports only 10 concurrent connections. HP Tootools usually uses 3 connections for each user. Rapidly changing tabs can result in too many connections temporarily.

**Workaround:** First close the browser connection and try to re-connect. Secondly, if you expect to have several people using the product at the same time, you will have to install NT Server and IIS.

---

**Description:** Topology may give inaccurate results if two or more stations are running discovery at the same time on the same network.

**Cause:** Topology sets flags in HP Hubs as it finds them and later resets these flags. Two or more instances of topology running at the same time will collide on these flags and potentially "confuse" both of them.

**Workaround:** If you must run two discoveries on the same network, make sure they do not overlap in timing, or turn topology discovery off on one of them (in the Settings->Discovery->Settings dialog).

---

#### *Limitations of the System Performance Advisor:*

1. System Performance Advisor is not supported on Win XP RC1 at this time.
2. System Performance Advisor is designed for at most one Tootools server to collect data from any given PC. A configuration where more than one Tootools server is collecting performance data from the same PC is not supported.
3. You cannot monitor the Tootools management server using the System Performance Advisor. (Putting the Performance Agent on the same system as the Tootools Device Manager does not work.)
4. It is recommended that the Tootools Management Server have a minimum of 256 MB memory when collecting performance data. Pagefile size should be at least 10MB over the physical memory size.
5. You cannot collect performance data on an IBM system running Windows 95 or 98. The IBM DMI agent is non-standard, and so the Tootools Device Manager cannot tell which operating system it is running.
6. Factory loaded NT operating systems from IBM may not correctly add the domain administrator to the machine's admin group when it joins the domain, thus causing a security violation error when you try to turn collection on (push the performance agent) to that system. The fix is to manually add the domain administrator logon into the machine's admin group and then try to turn collection on again.
7. After you Start Collection in the System Performance Advisor, it may take some time before the data appears in various parts of the user interface. See the table below for more information:

User Interface Page	Windows 95 or 98	Windows NT
Pie Chart/Summary Table	30 min	30 min
Graphs:		
Last Hour	15 min	2 min
Last Day	3 hrs (2 pts)	2 hrs (2 pts)
Last Month	48 hrs (2 pts)	48 hrs (2 pts)
System Performance Report	Same as last day	Same as last day
Licensing Report	At start of collection	At start of collection

1. NT Workstations typically have a connection limit of 10 connections at a time. NT Servers may also have a limitation, depending on the number of licenses being managed by the License Manager. When you turn Collection On for a large number of systems where a connection limit exists, you may see the error: "Error: Connection Limit Exceeded". This is usually corrected by redoing the action, but to a smaller number of systems at a time.
2. There is a known memory leak in the Trend Analysis graphs (last hour, last day, last month). Do not leave your browser open to one of these for long periods of time (several days).
3. Occasionally Toptools will display the hostname as the device identifier, rather than the fully qualified DNS name. In these case, the "Start Collection" may fail. If this happens, open the Devices windows and invoke the action "Update Discovery" on the device. Usually this causes it to redisplay with the full DNS name. Then you can go back to the Performance Advisor page and try to start collection again.
4. Systems being monitored by Performance Advisor that are often showing "Data Unavailable", but for which you can bring up the "View Analysis" window, are typically very slow systems that are not answering the poll for the summary data within the timeout period.
5. If a system is experiencing 100% CPU usage, Toptools may not be able to get the data for the last hour Trend Analysis line chart. The chart will show up as blank.
6. When using the System Performance Report Wizard on Netscape/Unix under SSL, the back buttons may occasionally not work correctly. To fix, reload the page.
7. When running on Netscape/Unix, the browser may occasionally shutdown when you invoke the "Custom Groups to Display" menu item next to the pie charts on the main System Performance page. The workaround is to try the action again.

---

**Description:** An exported Custom Report does not display the page number correctly.

**Cause:** Limitation of current version of Crystal Reports

**Workaround:** Within Word, delete the "page # of #" from the footer.

---

**Description:** A custom report exported to Excel format does not print correctly.

**Cause:** When the report is exported, Crystal Reports sets the print area to 1%.

**Workaround:** Within Excel go to the Page Setup screen and change the scaling to 100%

---

**Description:** Generating a very large Custom Report might take multiple minutes, causing the Custom Reports applet to time out with the message *Failed to connect to server*.

**Workaround:** If generating a Custom Report takes more than five minutes, the browser will time out and the only message is *Failed to connect to server* in the upper right area of the report. To workaround this problem, a configuration change must be made on the system running the browser (*not* on the Toptools server). You can make the change by using the Windows Explorer

on the client to browse to the `hptt\bin` directory on the *Toptools* server and double-clicking the file named `IncreaseBrowserTimeout.reg`. This will modify the timeout setting for you on the client.

**Description:** Sometimes a Custom Report will fail to be created, giving the error message *CPEAUT error occurred on server. 20618*

**Workaround:** If this occurs the first time you run a new report, go back to the previous page using the **Back** button at the bottom of the screen (not the browser's Back button). Then click on the **Next** button. If this occurs when running an existing custom report, go back to More Reports and re-run the report.

**Description:** Running a Custom Report after stopping and starting just the World Wide Web Publishing Service results in the error "ActiveX component can't create object."

**Cause:** The Crystal Reports components were not unloaded during a stoppage of just the World Wide Web Publishing Service. This happens whenever a Toptools utility that has to stop the WWW publishing service runs, such as the `TTDBErase.exe` or `mib2imp.exe`.

**Workaround:** Close the browser. From the Control Panel, Services applet, stop IIS Admin Services and then start World Wide Web Publishing Service. Restart your browser.

**Description:** pcAnywhere is not discovered on the Management Server itself.

**Cause:** Winsock is timing out when an attempt is made to contact the pcAnywhere host.

**Workaround:** None at this time. This only affects the system on which Toptools is installed.

[Return to Device Manager Contents](#)

[Return to Main Table of Contents](#)

## CD Contents

The main directories and contents of the CD are the following

Acrobat	Acrobat reader for viewing pdf-formatted manuals. The install wizard will install this for you if needed.
ApplicationNotes	Contains a deployment guide (also in the Manuals directory) and papers on specific desktop functionality.
Demo	A short animated introduction to Toptools. Click on <code>intro.htm</code>
Ie	Internet Explorer 5.5. The install wizard will install this if the version of your IE is less than 4.01 SP2 (JVM 2436).
Iis	NT Option Pack 4.0 for NT Server. The install wizard will install this for you if needed.
Index Files	Files for autorun
HPMibs	Contains the MIB files for HP networking products
Manuals	All the manuals and user guides in pdf format and html format.
Mdac	Microsoft data access components. The install wizard will install this for you if needed.
Meds Export Consolidation	Contains utilities for exporting the MEDS database to XML and importing it to SQL 7 or SQL 2000. Sample reporting queries are included.
Netdwnld	Download files for updating HP Hubs and Switches

Nt4sp	NT 4.0 Service Pack 6a. The install wizard will install this for you if needed. (Only installed if your Service Pack is 4 or lower or if the snmp service needs to be installed.)
Training	Contains a web-based tutorial. Double click on 'index.htm' to run.
pcAnywhere	Contains an evaluation copy of pcANYWHERE v 10.0 which may be installed from this cd onto machines of your choosing.
Pws	NT Option Pack for NT 4.0 Workstation. The install wizard will install this for you if needed.
Servers	Latest version of Auto Alert for Net servers
TT4d	Toptools for Desktops components. The install wizard will install this for you if selected.
TT4DAgents	Local agents for HP Vectras, Kayaks, Visualize PCs, Onmibooks, and Jornadas. You must install these agents on all client HP PCs.
Tt4s	Netserver components. The install wizard will install this for you if selected.
Ttcore	Toptools Device Manager core components. The install wizard will install this for you if needed.
Tths	Toptools for Hubs and Switches components. The install wizard will install this for you if selected.
Wbem	Microsoft WMI instrumentation. The install wizard will install this for you if needed. You can also copy the contents of this file to NT 4.0 workstations or servers and install it manually on them.
Wja	HP WebJetAdmin. The install wizard will install this component if selected.
Setup.exe	Main installation program. Always run this program to install Toptools Device Manager or its components

[Return to Main Table of Contents](#)

### **Upgrading from Previous Versions**

*From Toptools Device Manager versions 3.x, 4.x, Value Packs 1.0 or 4.5*

The install wizard will force an uninstall of these versions before installing version 5.5. Do not save any data when prompted during the uninstall.

*To manually uninstall a previous version perform the following steps:*

- 1) In the Control Panel Services Applet, set the Startup option for HP Toptools Services to Manual.
- 2) Reboot the system.
- 3) Run Toptools uninstall from the Add/Remove program in the Control Panel.

[Return to Main Table of Contents](#)

### **System Prerequisites and New Installations**

*If this is a brand new installation, follow these instructions:*

*Hardware requirements*

266MHz processor or faster

128MB RAM

150 MB page size or more (virtual memory)

100 MB free disk space if installing Device Manager plus Toptools for Desktops and/or Toptools

Net servers Components

Additional 75MB if installing Toptools for Hubs and Switches

Additional 20 MB if installing WebJetAdmin server

(**Note:** At least 400MB is required to install all the required Microsoft components on a computer that has only the Windows NT operating system installed.)

Super VGA (16-bit color display) video monitor and interface card. Though Toptools will display in 800x600 resolution, using a higher resolution is recommended to reduce the need to scroll certain pages.

Any LAN adapter card supported by the system

Mouse or other supported pointing device

*Installing the software:*

You should be a domain administrator to install Toptools 5.5. If you are not, you must at least be a local administrator. The WMI/WBEM functionality will not be available unless you install as a domain administrator.

*Special note on NT service packs and SNMP services*

Many systems are shipped with some Service Pack already installed. Installing the SNMP service will cause an SNMP dll mismatch if the Service Pack level is greater than 3. The Service Pack then needs to be reinstalled. The install wizard will guide you through installing the SNMP service and then it will install service pack 6a.

*Required software:*

The PC or Netserver on which you will be installing Toptools **must** have at least

TCP/IP services and protocols installed

A fixed or reserved IP address (if you are using DHCP)

SNMP services. You will be prompted to install SNMP services from your OS CD if they are not already installed.

IIS installed on Win2000 or WinXP. You will be prompted to install this from your OS CD if it is not already installed.

The system must be correctly configured into DNS and it should be a member of a domain, but not required.

To manage IPX nodes, install Microsoft IPX/SPX services and NetWare Client Services.

*Note: the Toptools installation wizard will install ALL the required software below*

1. Log on as a domain administrator and run the Toptools install wizard. It will inspect your system for any missing components and install them for you.
  - Service Pack 6a if the Service Pack level is less than 5 or if install detects a mismatch of SNMP dlls. (Not required for Win2000 or WinXP.)
  - NT Option Pack 4.0 (web server and Internet Service Manager- PWS or IIS). If you are installing on Win2000 or WinXP and you did not previously install the web server, you will be prompted to insert your OS CD for this step.
  - Web browser update (IE 5.5). (Not required for Win2000 or WinXP).
  - Task scheduler (from IE add-ons). (Not required for Win2000).
  - MDAC (Microsoft Data Access Components). (Not required for Win2000 or WinXP.)
  - WBEM core. (Not required for Win2000 or WinXP).

There may be reboots required as installation proceeds, but it will pick up where it left off.

*There is a feature that will automatically re-logon if reboots are necessary while installing the MS components.* Be sure to use the same user name and password for each reboot.

2. After installing the required OS components, the wizard will proceed to install those components of Toptools that you select. When asked for a password for the Toptools admin and services accounts, type in passwords that conform to your local password requirements.
3. The wizard will then give you an opportunity to fine tune how discovery will run, including entering the community name of your gateway if required. See the section Discovery and SNMP Community Names below for more details on the relationship between SNMP community names and discovery.

4. Upon completion, it will either ask you if you wish to reboot if install detected one is necessary or it will ask if you wish to start the Toptools services now. If a reboot is necessary, the Toptools services will start up automatically upon reboot. Otherwise, they will start up immediately.

[Return to Main Table of Contents](#)

### ***Installing on non-English Versions of NT or Win2000***

Toptools will install and run on non-English versions of NT or Win2000 (except the Turkish version of Win2000 due to a problem with the Java VM) **provided** all the Microsoft components that are localized are at the same release level as the English ones Toptools requires. These are

<b>Component</b>	<b>Localized NT Version</b>	<b>Localized Win2000</b>
NT Service Pack	SP5 or SP6a	Not applicable
NT Option Pack	4.0 (need IIS or PWS plus Internet Service Manager)	Not applicable
IE 4.0 SP 2 or IE5.0	Java Virtual Machine 2436 or Java Virtual Machine 3167 respectively	Part of system
Task Scheduler for IE 4.0 SP2	4.71.1645.1 (from IEAK)	Part of system
Task Scheduler for IE 5.0	4.71.1959.1 (from IEAK)	Part of system
MDAC	2.1.1a	Part of system
Adobe Acrobat Reader 4.0	4.0	4.0

Follow these steps to install Toptools 5.5 onto a non-English Windows NT system:

1. Install SNMP service in local language.
2. Install Service Pack in local language
3. Install Internet Explorer (see above requirements) in local language. This must be done even if you intend to use Netscape. Use the Custom Setup and select the "Microsoft Virtual Machine" radio button to install Java.
4. Install the Windows NT 4.0 Option Pack in local language.
5. Install the Task Scheduler from the local IE add-on pack. Toptools will rely on the Windows Task Scheduler for scheduled operations.
6. Install localized version of Acrobat Reader 4.0

Follow these steps to install Toptools 5.5 onto a non-English Windows 2000 system:

1. Install SNMP service in local language
2. Install IIS in local language
3. Install Acrobat Reader 4.0 in local language

Now that all the prerequisites have been installed in the local language, you can start the setup program of the English version of Toptools. Install whatever Toptools applications you desire (the Device Manager and WBEM agent will be installed onto the Toptools server by default).

[Return to Main Table of Contents](#)

### ***Accessing Toptools from Your Browser***

You must either be a domain administrator or a member of one of the Toptools groups to access the Toptools functionality. You can access the Toptools functionality from any system using the browser versions in the table below: ***Netscape 6.0 is not supported.***

<b>Client System</b>	<b>Browsers</b>
WinNT or Win9x	IE 4.01 SP2 (JVM 2436) IE 5.0 (JVM 3167) IE 5.5 IE 6.0 Netscape 4.61 or later
Win2000	IE 5.01 IE 5.5 Netscape 4.72 or later
HP-UX 10.20	Netscape 4.51 (use the Sun fonts) Netscape 4.61 (use the Sun fonts)
Sun Solaris 2.6	Netscape 4.51 IE 5.0

**Notes on Netscape:**

In order to access Toptools via a Netscape browser, you must set the *Directory Security* on the following virtual directories to “Basic Authentication” on the system where you install Toptools.

<b>Installed Components</b>	<b>Virtual Directories to set “Basic Authentication”</b>
Device Manager	Hptt
Device Manger + Desktops or Netservers	Hptt
Hubs & Switches	Hptt, hpttTopology, Scripts

To do this:

- Start the Internet Service Manager
  - For PWS:** Start->Programs->Windows NT 4.0 Option Pack->Microsoft Personal Web Server->Internet Service Manager
  - For IIS:** Start->Programs->Windows NT 4.0 Option Pack->Microsoft Internet Information Server->Internet Service Manager
- Select the “Hptt” virtual directory, right mouse to bring up the context menu and select Properties.
- Select the “Directory Security” tab; click the “Edit” button; select Basic Authentication. OK out of the dialog. Do not change any other settings in this dialog.
- Repeat for the “Viewer” virtual directory.
- Repeat for the “hpttTopology” virtual directory if you installed Toptools for Hubs & Switches.
- Repeat for the “Scripts” virtual directory if you installed Toptools for Hubs & Switches.

On HP-UX systems, you should set the browser fonts to be the Sun fonts rather than the HP fonts: set MOZILLA\_JAVA\_FONT\_PROPERTIES to \$MOZILLA\_HOME/java/classes/sun.

In all cases of using Netscape, the “afc11.zip” file must be present in the java\classes directory. Toptools will sense the presence or absence of this file the first time you connect to it via Netscape and walk you through installation of this file. Do not unzip it.

Netscape does not handle sizing of java applet windows as cleanly as IE and you will experience refresh problems if you attempt to size your browser windows.

Do not use Netscape on the system on which you install Toptools 5.5.

**Browser Settings**

Browser settings are extremely important for performance. Be sure to set your browser to exclude using a proxy for your domain:

On IE4.01 SP2: Internet Options - Connections - Advanced - Exceptions.

On IE 5.x: Tools - Internet Options - Connections - Lan Settings - Advanced.

On Netscape: Edit - Preferences - Advanced - Proxies - select Manual then View.  
On IE, be sure to check “Bypass proxy server for local addresses” as well as entering the domain in the exceptions list on the Advanced page.

It is also helpful to set your browser to check for newer versions of stored pages on every visit to the page.

To launch Toptools from your browser, the url to the management server should include your domain (e.g., <http://machine.company.com/hppt>). The product will start up. If you set up NTFS on the management server, and set your IIS to basic security (required for using Netscape), you will be challenged for your username and password (domain\username for Netscape). This is no different for Toptools than for any other web-based application.

When the welcome screen comes up and the left panel is displayed, you may begin to use Toptools. If this is your first experience with Toptools, click on the Guided Tour for a quick review of the capabilities and features.

The menus down the left panel bring up the selected functionality in the right panel. The Devices menu will open a separate window with the Device Selector. This is the main window from which to access individual devices on your network. Expand any of the categories in the left side by double clicking. For example, double click on “PCs and workstations” to see a list on the right of all the PCs and workstations currently discovered. Select one and double click to launch the management page for that device or right click to see a list of possible actions you may take. While initial discovery is running, you should periodically press the "Refresh" button in the Device Selector to update its contents of devices and their capabilities.

[Return to Main Table of Contents](#)

### ***Adding Components after Initial Installation***

To add any component or components after you have done an initial installation, just rerun the install wizard and check those components you wish to add. The wizard will do the rest.

[Return to Main Table of Contents](#)

### ***Toptools Services***

After installation Toptools 5.5 will automatically discover devices on your network: PCs, servers, printers, hubs, switches, routers, Unix workstations, and their management capabilities, including whether or not they have embedded web servers. This process takes anywhere from a few minutes to perhaps an hour depending on the size of your network. A small network of less than 100 devices will be discovered within five to ten minutes or so. A larger network (say 1500 nodes) may take around half an hour. Discovery finds the devices using pings and reading ARP cache information, and then proceeds to inventory them, using SNMP, DMI, and WMI to gather the information.

During this time, the data is continuously being updated and you can watch the progress by starting the web browser and going to the Settings/Discovery page.

[Return to Main Table of Contents](#)

### ***Discovery and SNMP Community Names***

In order for Toptools to identify a device with only SNMP, the “read” community name that Toptools uses must match that on the device. By default, Toptools uses “public”. If after discovery runs, a device shows

in the Other category with “No Agent”, but you know it does have an SNMP agent, the most likely cause is that the community name on the device is not “public”. Follow these steps to change the community name that Toptools uses for these devices (this does not change the community name on the device):

- In the navigation frame, click **Devices** and select **Device Types** from the menu.
- Select the **Others** tab.
- Select the devices you want in the list at the right (you can do multiple devices if they have the same community names).
- Click the right mouse button on one of the selected devices.
- Select the **Security** menu item and then **Set SNMP Passwords (Communities)**.
- Type in the "read" community name (twice) for the selected devices and click **Set Read Password**.
- With the same devices selected, click the right mouse button and select **Update Discovery** from the popup menu. Or, alternatively, rerun discovery.

You can also specify the read and write communities when adding devices manually:

- Point the browser at the Toptools home page.
- In the navigation frame, click **Settings** and select **Discovery** from the menu.
- Select the **Additional Devices** tab.
- Type in the address or DNS name of the device.
- Type in the Read community name.
- Click the **Add Device** button.

If you choose to only run discovery by manually adding devices and leaving discovery “not scheduled”, you still need to enable at least IP, ping and web-server discovery on the Settings->Discovery->Settings page.

[Return to Main Table of Contents](#)

## **Support for DHCP Environments**

Toptools will discover devices in a network that are DHCP clients. For Toptools to detect that a device changes IP addresses (due to DHCP), the network must also be using either DNS (Domain Name Services) or WINS. The DNS or WINS server must be coordinated with the DHCP server so that the same name for a device is updated as DHCP changes IP addresses on a device. If a DNS or WINS environment is not present, Toptools may note IP address changes for a device as a possible duplicate IP address alert.

[Return to Main Table of Contents](#)

## **Toptools for Desktops 5.5 Release Notes**

July, 2001

### **Contents**

[What's New in This Release](#)

[Known Limitations and Caveats](#)

### **What's New in This Release**

- The WMI agent now supports Windows XP.
- There is a new Windows XP supported PCs report, listing all PC that meet minimal requirements for running Windows XP. (Similar to the Windows 2000 supported PCs report.).

- Some PCs may be eligible for a free upgrade to Microsoft Windows XP. From inside Windows XP supported PCs report, you can generate a file with the candidate PCs and directly upload the file to the HP's Web Site.
- There is a new Class Issues report, used to detect potential epidemic problems on the installed based discovered by Toptools.
- The "Resources Monitoring" feature was completely replaced by the System Performance module provided by Toptools Device Manager core components. The "Configure Resource Monitoring" menu action and all its submenus will not be displayed anymore. Also, the monitoring links in the Identity/Status page (Memory Usage, CPU Usage, Disk Usage and LAN Usage) were removed.
- e-Diagtools page: the "Diagnose & Troubleshoot" page displays the support ticket graphically. e-Diagtools page: the "Warranty & Support" functionality was moved to the Support page.
- e-Diagtools pages (properties and actions): the welcome message delay and welcome message display settings were removed.
- Menu actions that require the WMI agent to be present on the target machine will only be displayed for machines that contain it.
- "Get Latest Support Info..." button removed from "Add Printer" and "Agent Deployment" pages, since this functionality is provided through a new "Updates" tab in the "Drivers/Firmware" page.

[Return to Desktop Contents](#)

### **Known Limitations and Caveats**

**Description:** Add Printer function on PCs running Windows NT: the new printer will be totally operational. However, the icon shown by the command Start > Settings > Printers will be that of a local printer rather than a network printer. Also, if you click Properties on the printer icon, no port will be listed, and you will need to press Cancel to exit.

**Description:** Add Printer function on PCs running Windows 9x: if there is no Windows user (logged in or having pressed "Cancel") on one of the target PCs, the printer driver will be installed correctly, but no connection to the printer will be established. Thus, such PCs will not have access to the printer, and you will need to repeat the Add Printer operation later.

**Description:** When doing an agent deployment, the user is prompted to select THE package to be deployed. In case of a heterogeneous selection (NT4 and WMI machines) the action is still offered but no single agent package can be installed on both operating systems

**Workaround:** First select the machines by doing a search on the operating system (or sorting on the "WBEM column in the device selector). The non Windows 2000 machines may be "unknown" (empty string) but the Windows 2000 machines are properly recognized as Windows 2000, even without an agent.

[Return to Desktop Contents](#)

[Return to Main Table of Contents](#)

## **Toptools Netserver Components 5.5 Release Notes**

July, 2001

### **Contents**

[What's New in This Release](#)

[Known Limitations and Caveats](#)

## What's New in This Release

### *Netserver Property Pages*

1. Netserver pages are reworked to separate status information from configuration information, with links between these pages.
2. An action to "locate" a system in a rack has been added in the Tools page.
3. The Hard Disk Status and Memory Status applets have been reworked.
4. The Configuration pages give more detailed information than before, including PCI slot and memory slot information.
5. There are now property pages for Netservers running Linux with the Netserver agents (5.50 or later)
6. You can configure Instant Support Tuner settings under Configuration tab.
7. Support pages have links to HP's PartSurfer (where you can order upgrades or replacement parts) and Smart Search where you can find support answers.
8. You can enter rack information on the Configuration/Settings page for any server or networking device. This information is written back to Netservers running Netserver agents 5.50, and written to the managed element database in any case. Once entered, this information is also available on the Identity page and in the detailed report page.

### *Group Actions – Revision Management*

Managing drivers, firmware, utilities and agents has been added as a group action to Netservers running Windows NT 4.0 or Windows 2000. Netserver agents version 5.50 is required on the Netservers.

### *New Cluster Alert support*

For Netservers running Windows 2000 Advanced Server with two node cluster support and agents version 5.50, Toptools Device Manager will be able to receive cluster alerts from the nodes.

[Return to Server Contents](#)

## Known Limitations and Caveats

**Description:** When cluster services are installed, Windows 2000 Advanced Server and Windows 2000 Data Center Server enable a feature called Event Log Replication. Once enabled, events logged in the system, security or application log on each node in the cluster are replicated to the corresponding logs on the other nodes. With this feature enabled, the Agents running in the cluster will collect events that appear to be duplicates.

The duplicate events generate network traffic and they may cause more notifications than you are expecting. Therefore, we recommend disabling Event Log Replication to avoid these issues. To do this, follow the instructions detailed in Microsoft Knowledge Base article Q224969. We recommend that you disable Event Log Replication for all nodes in your Windows 2000 clusters.

---

**Description:** When viewing Alerts in Toptools Device Manager Alert Log, you may see duplicate alerts for clusters even if you have disabled the event duplication in the cluster. The reason is that events are forwarded from both cluster nodes. If you don't want to see duplicated alerts, you could filter the alerts by computer name.

---

**Description:** NetWare does not allow System Location and Contact to be set permanently from the Configuration/Settings page.

**Workaround:** To change the System Location and Contact do it locally on the NetWare server or use RCONSOLE to do it remotely.

---

**Description:** Disk Array Information displays under mass storage section in the report page.  
**Cause:** The DAC (Disk Array Controller) contains a SCSI controller chip and it responds to the SCSI adapter query, so it will show up as a SCSI controller in our SCSI controller table. Logical drives configured under a DAC controller will be shown as SCSI devices connected to the DAC, with the capacity of the logical drive also shown as the capacity of the device under SCSI devices.

---

**Description:** Support for the Mylex Disk Array Controller:  
Toptools For Servers will not display RAID configuration for the Mylex Disk Array Controller. Toptools For Servers Eventlog will display the traps received from the Mylex DAC. The Mylex DAC will show up as a SCSI controller in the SCSI controller table. Logical drives configured under a DAC controller will be shown as SCSI devices connected to the DAC, with the capacity of the logical drive also shown as the capacity of the device under SCSI devices. Also, the Hard Disk Status supports the Mylex DAC controller.

---

**Description:** ATAPI CD ROM showing under the SCSI devices  
**Cause:** Atapi.sys is the device driver that drives IDE devices, and Atapi.Sys is marked in Windows NT as a SCSI device driver. The SCSI Adapters tool scans this entry when it displays devices.

---

**Description:** In the Configuration/Settings page, 16 Bit characters cannot be used to set the Contact name and System Location.

---

**Description:** The physical memory amount shown on the overall page is 1 MB less than the actual physical memory because it is showing the maximum physical memory available to NT.

---

**Description:** In the Toptools Configuration tab, under the "Physical Storage\SCSI Controller" entry of the Configuration tree, a SCSI controller with multiple channels will show up as multiple SCSI controllers.

---

**Description:** On managed servers running SCO Unix 5.0, the Toptools Configuration tab may incorrectly indicate that a Disk Array Controller (DAC) exists when in fact no DAC is installed. The DAC entry would show up underneath the "Physical Storage" entry of the Configuration tree.

---

**Description:** Toptools will not display SCSI information for NetServers running NetWare with only one SCSI device.

---

**Description:** The Hardware Event Log cannot be printed or saved in the sorted order.

---

**Description:** Component: HP NetRAID-4M SNMP agents version 2.3.1.3975  
NOS: NT 4.0, Windows 2000, NetWare 4.2, NetWare 5.1  
The Device Usage and State fields for HP NetRAID-4M containers are displayed as "Unknown" if there are multiple NOS partitions within the container. These fields are displayed in the HP NetRAID-4M entry of the Physical Storage tree located in the Configuration tab of Toptools for Servers.  
This issue will be resolved in a future release of the HP NetRAID-4M SNMP agents.

*Hard Disk Status page Issues:*

**Description:** *(Netscaler agents 4.51 or earlier)* The Hard Disk Status Disk Drive Locator may indicate an error when attempting to flash the activity LED on removable media devices such as CD-ROMs. This error should be ignored.

---

**Description:** The Hard Disk Status Disk Drive Locator may indicate an error when attempting to flash the activity LED on NetRAID devices even though it was able to flash the LED. This error should be ignored.

---

**Description:** *(Netscaler agents 5.03 or earlier)* When running NT, changes reflecting inserted or removed hot swap devices attached to SCSI Controllers will not be displayed by Tootools until the system is rebooted.

---

**Description:** *(Netscaler agents 4.51 or earlier)* Killing the Internet Explorer browser while the Power LED is flashing will leave the LED flashing until the Tootools Hard Disk Status Disk Drive Locator is started again or the OS is rebooted.

---

**Description:** The Hard Disk Status page will display "unknown" in the SCSI/RAID Controller's Target ID and Description, SCSI Device's Vendor or RAID Device's Array Configuration columns for devices that cannot be found in the system.

---

**Description:** The "Repair" tab used for disk drive BIOS update is only available for NetRAID drives whose current status is "Failed", "Ready", or "hot-swap".

---

**Description:** *(Netscaler agents 4.51 or earlier)* After updating a drive, the new drive version information will not be available to this program for up to an hour. The version change can be verified immediately on the TT drive configuration page or by bouncing the SNMP service and reentering the HDD wizard

---

**Description:** *(Netscaler agents 4.51 or earlier)* Multiple "Update failed. Unknown SCSI error: 244" message boxes are presented after a disk BIOS update operation has completed on systems where NetRAID rebuild is set to occur automatically.

**Cause:** NetRAID begins to rebuild before the update completion status is obtained.

**Workaround:** Close the browser.

---

**Description:** HPDA devices that do not have events associated with them will not be displayed. Only event information will be available in the Drive Wizard. The Drive Utility Status, Locate, and Repair tabs are not displayed. HPDA configuration information for logical devices is available through the HP Local Tootools for Servers Configuration page under SCSI Devices.

---

**Description:** In the Disk Drive Wizard, the RAID level for NetRAID 4M will always be reported as "None" for disk drives with RAID levels greater than 5.

[Return to Server Contents](#)

[Return to Main Table of Contents](#)

## Toptools Remote Control Card Group Actions Release Notes

July, 2001

*The Toptools Remote Control Card is an optional accessory for HP Netserver systems that provides remote management capabilities regardless of the state of the server.*

### Contents

[What's New in This Release](#)

[Known Limitations and Caveats](#)

### What's New in This Release

#### Group Actions

In conjunction with HP Toptools Device Manager software, you can perform actions on a group of Toptools Remote Control Cards or a group of HP Netserver systems which have Toptools Remote Control cards installed. You can perform the following actions:

##### *Card Group Actions*

- Add user
- Delete user
- Change user password
- View users
- Update card firmware

##### *Server Group Actions*

- Power on
- Power off

[Return to RMC Contents](#)

### Known Limitations and Caveats

**Description:** The “host management server” column of the Remote Control Card Report displays hex characters for some Remote Control Cards. Selecting “Related Devices” in the device selector for the server containing this card shows an unknown device. Trying to launch it displays “This page cannot be found” and trying to launch “remote control” does nothing.

**Cause:** Version B.02.03 of the Remote Control Card does not correctly support the mib used to relate the devices. (Check the Version column in the report.)

**Workaround:** A fix is forthcoming from HP. In the meantime, you can “back flash” the firmware on the RCC to version B.02.02 or earlier.

---

**Description:** Each group action requires a login username and password.

For security purposes you must login before executing each group action. Each group action must be launched from the Toptools Device Manager through the Action Menu. The browser’s Back button cannot be used to execute consecutive group actions.

To login to multiple cards, you must have an account with the same username and password on each card. In addition, your user account must have administrator privileges in order to perform group actions.

---

**Description:** HP recommends using Remote Control firmware version B.02.00 or greater when executing group actions, although earlier versions of the firmware will function correctly. Upgrading the card's firmware from a 1.x to a 2.x version using group actions is supported. The firmware upgrade maintains the card's configuration, including usernames and passwords. If the firmware is ever downgraded from 2.x to 1.x, the username and passwords are no longer valid. You can reset the default username (ADMIN) and password (ADMIN) by using the Remote Control utility that is provided on the HP Netserver Navigator CD.

---

**Description:** Server group actions require Netserver Agents 4.51 or greater on the HP Netserver.  
**Cause:** HP recommends that the HP Netserver, which contains the Remote Control card, should be running with Netserver Agents 4.51 or greater when executing group actions. The agents provide the Toptools Device Manager with a mapping of the HP Netserver and its Remote Control card. They also provide the NOS graceful shutdown capability and ASR. Agents, version 4.50 or earlier, may not function correctly with server group actions. The server group actions effected are power on and power off, also the Related Devices action. Problems mainly show up after changing the Remote Control card's IP address or after replacing the Remote Control card.

---

**Description:** The double quote (“) and backslash (\) characters are not supported in Remote Control card user names or passwords.

**Cause:** The double quote and backslash characters are special characters for the Remote Control card and should not be used in user names and passwords. This is true for both group actions and the Remote Control cards web interface.

[Return to RMC Contents](#)

[Return to Main Table of Contents](#)

## Toptools for Hubs and Switches 5.0 Release Notes

July, 2001

### Contents

[Toptools for Hubs & Switches](#)  
[System Configuration](#)  
[Free Software for Managed Hubs and Switches](#)  
[Networking Environment](#)  
[Policy Management](#)  
[Discovery](#)  
[Maps](#)  
[Firmware Downloader](#)  
[Traffic Monitor](#)  
[Known Limitations and Caveats](#)  
[Support and More Information](#)

### Toptools for Hubs & Switches

This section provides useful information about installing and operating HP Toptools for Hubs & Switches Version R.02.04, on Microsoft Windows NT or Win2000. HP Toptools for Hubs & Switches is a network management application that provides device management and traffic

monitoring for HP hubs, bridges, and switches. It is a component of the HP Tootools collection of management software that also controls servers, PCs, and a myriad of other computer equipment.

See also the [Hardware Requirements](#) in the “System Prerequisites and New Installation” section near the beginning of this document.

[Return to Hubs & Switches Contents](#)

## **System Configuration**

### **Video Driver**

The Matrox Millennium 1 or 2 video card may cause a system crash when drawing a topology map, if configured using more than 32K colors (24-bit or 32-bit mode). When this happens, your system will have to be rebooted. To prevent this problem, make sure you have the latest Windows NT 4.0 video driver. The driver can be obtained from the World Wide Web at this URL:

<http://www.matrox.com/mga/drivers/home.htm>

### **BIOS on the HP Kayak PC**

Problems running some Tootools services have been observed on HP Kayak PCs with older versions of BIOS. If you install Tootools for Hubs & Switches on a Kayak PC, be sure to install the most recent available version of BIOS before running Tootools.

### **HP Vectra XA**

Problems have occurred running Tootools for Hubs & Switches on older HP Vectra XA computers (with processors slower than 200MHz). This does NOT apply to the HP Kayak XA computer. The computer may lock up, especially when doing mesh discoveries.

### **Consumption of Virtual Memory**

Running Internet Explorer with the Traffic Monitor page up continuously over time consumes virtual memory. Left unattended for a long enough period, it may slow the operation of Tootools and other applications running on that computer.

*Solution:* close the browser window every couple of days and reinvoke it. Then bring up Tootools. This frees up the lost virtual memory.

### **Delay in Absence of DNS server**

If your network does not have a DNS server, there is a wait of at least 4 minutes when you attempt to access a device through the web browser interface - the browser will appear to hang. Thereafter, performance remains sluggish. If your network has a DNS server, this is not a problem.

*Workaround:* Add the IP address and alias of every device you want to manage to the file `drivers/etc/hosts`. This file must be edited on every PC from which net management will be done through the web browser interface.

[Return to Hubs & Switches Contents](#)

## **Free Software for Managed Hubs and Switches**

For managed hubs and switches, Hewlett-Packard provides **free** software (also termed *firmware*) on the HP ProCurve website. To determine whether you have the latest software, and to access software updates on the web, go to the HP ProCurve website (<http://www.hp.com/go/procurve>), then click on **Support** and look for the link to use for accessing and downloading software.

[Return to Hubs & Switches Contents](#)

## Networking Environment

### HP Web JetAdmin Causes Security LEDs to Light

Using HP Web JetAdmin on your network will cause the security LED on network devices to light. This happens because Web JetAdmin tries to access network devices using a nonstandard community name, "internal". This community name conflicts with those already known to Toptools. Web JetAdmin does not otherwise affect the operation of your network devices.

[Return to Hubs & Switches Contents](#)

## Policy Management

### Automatic Configuration Management

#### *Multihomed Network Management Stations*

If your network management station is multihomed (i.e., it has more than one connection to the network) the **Deliver all device alerts to HP Toptools** and **Implement features in the "Trap Receivers" tab** checkboxes will be grayed out. You cannot use Automatic Configuration Management to configure trap receivers from a dual-homed management station.

#### *Using Automatic Configuration Management To Synchronize Your Devices*

You may have hubs or switches on your network that have been modified, manually or through the web interface, that you now want to get into sync with each other through the Automatic Configuration Management feature. To open them all in the Automatic Configuration Management page and then click the **Apply** button will not do the job; you must change at least one field in order to put the changes into effect.

If you do not want to change any field from the default values, you must change one field, click the **Apply** button, then change the field back and click **Apply** again.

### Quality of Service Manager

It is important to understand that the setting of policies and group operations should be done on a network-wide level. The QoS Manager expects to be the only configuration tool used to configure traffic prioritization on all QoS-capable HP devices on the network. Once the user configures some type of prioritization through the QoS manager, those changes for that type of prioritization will be used to override any configured information in each QoS capable HP device, even as new ones are discovered. The only way to have that type of prioritization not override similar configurations in new devices is to delete the QoSData file in the data directory of the 'hpwnd' directory under 'hptt'. This will erase all QoS information defined through the QoS Manager and it will no longer try to keep consistent policies on the network.

[Return to Hubs & Switches Contents](#)

## Discovery

### Community Names

In order for Toptools for Hubs & Switches' discovery to identify a device, the device must have a "public" community name. If it doesn't have one, discovery will find the device but not identify it. See the section [Discovery and SNMP Community Names](#) for more information on setting community names for discovery.

### Devices

For HP bridges and older hubs (see Note 1), there is only one community name, and it has only one access level ("write"). Therefore, for these devices, the "read" community and the "write" community are one and the same. (There is a hidden community name of "public" which has

appropriate "read" level access. This can be used in Toptools for Hubs & Switches as the "read" community name.)

For newer hubs (see Note 2) and switches (see Note 3) you can specify multiple community names with different access levels. Only two of them, "read" and "write", can be used by Toptools for Hubs & Switches. (There is no hidden "public" community name. Either "public" is explicitly configured, or it does not work even to "read".) The method used to configure the community names differs between hubs and switches. Here's how you can define them on each (using the console interface) to provide the maximum security (i.e., to provide each community name with the minimum access required for use by network management).

On hubs (see Note 2):

1. From the main menu on the device console, select "2. Management Access Configuration..." (or "5. Managers/Password Change...", depending on the device).
2. Select "2. Community Name" (or "2. Configure community name").
3. For the "read" Community, set Read View = User; Write View = Discovery.
4. For the "write" Community, set Read View = Full; Write View = Full.

**Note:** The procedure for some devices is slightly different but fairly straightforward. See your hardware documentation for detailed instructions.

On switches (see Note 3):

1. From the main menu on the device console, select "Configuration...".
2. Select "SNMP Communities...".
3. For the "read" Community, set MIB View = Operator; Write Access = Restricted.
4. For the "write" Community, set MIB View = Manager; Write Access = Unrestricted.

For even greater security with either hubs or switches, you can specify the addresses of those stations from which SNMP requests are to be allowed. This is done in the list of "Authorized Managers" associated with each community name. Be sure to include the station on which Toptools is installed.

Note 1: Hubs and bridges with the following model numbers: J2355A, J2410A, J2413A, J2415A, J2600A, J2601A/B, J2602A/B, J2610A/B, J2611A/B, J2612A, J2630A, J2631A, J2632A, 28692A, 28674B, 28682A, 28688B, 28699A, 28688A, 28673A, 28674A

Note 2: Hubs with the following model numbers: J3200A, J3202A, J3204A, J3301A, J3303A

Note 3: Switches with the following model numbers: J3100A/B, J3245A, J3175A, J3177A, J3298A, J3299A, J4110A, J4120A, J4121A, J4122A

See the section [Discovery and SNMP Community Names](#) for how to configure the network management software to use these community names.

**Tip:** You may want to add routers manually as well, and define their community names. This will further improve the discovery process.

**Note:** There are some caveats for the devices you fix with the above procedures:

1. The topology of some of these devices, especially the older models, might not display properly.
2. From the **Devices** page, the **Update Firmware...** option fails to work. The HP Download Control dialog box will not launch.
3. The Closeup View for models J3100A, J3125A, J3175A, and J3177A cannot be invoked from the Devices page or any topology map.
  1. The SNMP Trap Configuration option in the **Devices** page will not work.
  - 2.

There is a workaround for items 1, 2, and 4. Retain the "public" community name for those devices, specifying "read" capability. You can then add security for all the devices named in item

4 above, except J3125A, J3126A, and J3233A, by specifying an Authorized Manager for each device.

[Return to Hubs & Switches Contents](#)

## **Maps**

### **Display of servers and Unix workstations**

Servers and Unix workstations appear in the "Switches and Hubs Only" map, even though they're not technically switches or hubs. If the device (whether a switch or not) shows up in more than one segment, it will appear in all maps at the Switch level map and below, i.e., Switches and Hubs Only.

### **User Snapshot Maps and Security**

Under certain circumstances, when attempting to generate maps on a client machine when you are already logged into the Toptools web host, a User Snapshot might not be generated while attempting any of the following operations:

- requesting a full network map from the current map list
- drilling down on a segment to a lower level map
- creating a new view of an existing map (Circular, Hierarchical, etc.)
- locating a node/segment map from Traffic Monitor or the current map.

If you are logged into the computer that hosts the Toptools web server and try to perform the above operations on a different PC client using the same login, an error will occur and the map will not be generated. The reason is that the request for a map must pass through Toptools security, under which a login and password must be supplied. Since your server login is already in effect, the system does not see the need to go through security. This produces the error. Generating a map under these circumstances requires a separate login on the client. Therefore, it is recommended that if you have a login on the Toptools server you also have a separate, different login on whatever PC client you may use. This prompts Toptools to ask for a login and password. Once passed, the map will be supplied.

### **Error During Navigation to New Map**

If you get an error while navigating to a new map from a current map, just close the map window and re-select the original map from the map list.

### **Failure to Connect to a Server**

When you request a new map view, go to a segment view, or do a Locate from Traffic Monitor or the current map, *and* if you have an incorrect version of the `vbajet32.dll` file in `\winnt\system32\`, you will get an error message stating that you cannot connect to the server. The version of this file commonly found on computers, 5.0.7122, is the cause of the problem. The correct version for Toptools, 3.0.6908, is included in the Toptools for Hubs & Switches directory.

*Solution:* Copy the version of `vbajet32.dll` from the `\hptt\hpwnd\system\` directory to your `\winnt\system32\` directory.

[Return to Hubs & Switches Contents](#)

## **Firmware Downloader**

### **Downloading Firmware**

For the Download Manager to work, the new firmware must be accessible to your network. The firmware files, which may be obtained from the World Wide Web or HP Customer Care Center,

must reside on the hard drive of the computer running Toptools. Place all the files in this directory: \hptt\hpwnd\dld.

**Note:** This assumes you are using the directories automatically set up during the Toptools installation.

### **Unsupported HP Devices**

The following HP bridges and hubs are not supported by the Download Manager under Toptools:

- HP 28673A 10:10 LAN Bridge
- HP 28674A/B Remote Bridge
- HP 28688B EtherTwist Hub Plus/12
- HP 28682A Fiber Optic Hub Plus
- HP 28699A EtherTwist Hub Plus/48
- HP 28692A ThinLAN Hub Plus
- HP J2355A EtherTwist Hub Plus/24S

[Return to Hubs & Switches Contents](#)

## **Traffic Monitor**

### **Auto-negotiation and Segment Speeds**

The traffic management applications are totally dependent on an accurate representation of the network topology. One difficulty in keeping the topology information up to date in Toptools is when segments renegotiate a different link speed after discovery. This can occur for a variety of reasons. If a segment's speed changes, discover and topology must be manually rerun in order for Toptools to recognize the changed segment speed. In order to guarantee accurate rediscovery, the MEDS database should be cleaned before rediscovery.

If the network is not rediscovered, the traffic management applications will present utilization as a factor of the differing speed. For example, if a 10MB segment is renegotiated to 100MB, traffic management will show a utilization that is 10x too high for that segment.

[Return to Hubs & Switches Contents](#)

## **Known Limitations and Caveats**

**Description:** Two internal processes, TMServer and MapFactory, may crash with a Dr. Watson error and a crash log is created. These errors were not reproducible during TT4H&S testing. If you get one of these errors, save the log file, then stop and restart Toptools. If the error reappears, contact your local HP Support office.

**Description:** There is a problem with some Toptools for Hubs & Switches applications being run remotely with Internet Explorer version 4. The following applications will not work: Network Performance Advisor, Traffic Data Collector Settings, and Maps. It is recommended that anyone accessing the Toptools server remotely upgrade to Internet Explorer 5.

### **Automatic Configuration Management of HP Switch and Routing Switch products**

For devices:

- 6208M Switch,
- 6308M Routing Switch,
- 9304M Routing Switch, and
- 9308M Routing Switch

there is no default write community name. To allow Tootools to perform automatic management of configuration policies on these devices, a write community name must be configured. This can be accomplished by opening a telnet session with the device and performing the following CLI commands:

```
>enable
>config terminal
>snmp-server community public rw
>write mem
```

where "public" is the new write community name.

### **Device View not supported on Netscape Browser from a Unix system**

When using a Netscape browser from a Unix system, the menu item "Device View" is not supported in this release when selecting a hub or switch *without* an embedded web server (no wrench icon or house icon in the device list). You can only launch the "Device View" for such devices when physically running on the Tootools Server.

### **Community name = PUBLIC**

The community name PUBLIC must remain on the devices in order for the Device Manager application to function correctly. The Device Manager application is launched from the "Device Types" dialog under the menu item "SNMP/Trap Configuration..." and is used to set trap thresholds on a device.

### **Changes will be lost unless you hit "Apply Group Settings"**

Changes made to groups will not be made until they are applied using the "Apply Group Settings" button. Also, there is no warning dialog will inform the user that changes have been made but not applied, as done in many applications.

### **Updating Set of Devices that use both Software Update and Download Manager**

When using Tootools for Hubs and Switches to update device firmware, if you select a set of devices that require the use of both the Software Update feature of Tootools and the older Download Manager utility, the user will have to execute a second step in the upgrade process. A page will be displayed listing the devices supported by the older Download Manager utility followed by a list of the devices supported by the Software Update feature. Following each list will be a link to launch either utility (Note that the older Download Manager did not support updating multiple devices that were not of the same type).

### **HP ProCurve Switch 100/200 port names all "ethernet\_csmacd"**

Under the Performance tab the user may select Traffic Data Collector Settings and configure whichever ports on any network device he wishes to collect statistical traffic information from. However, if the user has a Switch 100 or Switch 200, each port will be displayed as <device name> port ethernet\_csmacd. Since all ports will be named "ethernet\_csmacd", it will be impossible for the user to distinguish one port from the other and therefore it is recommended that the Switch 100 and 200 not be used for manually specifying the ports to monitor.

### **Cannot select HP AdvanceStack switching hubs for manual data collection**

The Switching hubs (J3200,J3202,J3204,J3210,J3212) will never be selectable in the Traffic Data Collector Settings window. Therefore, the user will never be able to specify monitoring on a port of the switching hubs.

### **Collecting Extended RMON data on too many ports can overload a system**

When configuring the traffic data collector to run in manual mode, care should be taken not to overload the system by specifying too many ports for Extended RMON analysis. Since the determination of overloading depends on the type of system and other applications running on the system and how much traffic is on the segments being monitored, a hard limit cannot be specified, but if the system seems to be running slowly after the traffic data collector is started then this could be the culprit

### **Inconsistent Port/Segment Naming when using Manual Mode for Traffic Data Collector**

Configuration of the Traffic Data Collector allows the user to choose which ports on a device should be monitored and, more specifically, whether those ports should be monitored via reading statistics or using Extended RMON. This is achieved by adding a device to a manually configured list and specifying which ports and which collection methods will be used for monitoring. However, the type of port information available for each device differs and therefore looks rather inconsistent in the display of monitoring devices. The user should refer to the specifications of each device to be sure which physical interfaces are available for monitoring.

Most devices have port numbers or friendly port names that represent each physical interface on the device. For example, if you have a switch named "UpperSwitch", you will see its ports named as "UpperSwitch port 1", "UpperSwitch port 2", etc. Or if there are slide in cards, the port names will be shown as "UpperSwitch port A1", "UpperSwitch port A2", etc.

Some devices have special ports that have a unique behavior normally not seen in that type of a device. Examples of this are an uplink port or a bridging port in a hub. Often, our applications will try to attach a friendly name to these ports so the user knows their function. In that case, a device named "UpperHub" may have three ports listed under its name called: "UpperHub port 1" (the hubbing port), "UpperHub port UpL" (the uplink port), and "UpperHub port Brg" (the bridging port).

### **Time Change**

If a time change has occurred on the Toptools Server (other than a change due to daylight savings time), the Toptools browser must be closed and restarted so that HP Toptools for Hubs and Switches Performance tools can recognize the change.

### **Utilization Reports**

When running the utilization reports in the Network Performance Advisor application, keep in mind that the historical utilization and utilization frequency graphs will not display when there is only one hour present on disk. These are line graphs that require more than one data point to display accurate graphs.

### **Network Performance Advisor will not generate reports when the traffic data collector is in manual mode**

Network Performance Advisor will not generate any suggestions for either of our optimization reports while the traffic data collector is running in manual mode. Network Performance Advisor's utilization report, however, will still be applicable in manual and in automatic mode.

[Return to Hubs & Switches Contents](#)

## **Support and More Information**

If you want to learn more about HP Toptools for Hubs & Switches and other HP networking products, the CD-ROM from which you loaded the system has a wealth of information, all accessible through your favorite web browser.

- If you are using the "HP Toptools for Hubs & Switches" CD, put the CD in your CD-ROM drive and click **Product Info** in the homepage, then click either **User's Guide** or **Hardware Product Manuals**
- If you are using the "HP Toptools" CD, put the CD in your CD-ROM drive and click the **HP TTHS Online Manual** or **HP Networking Product Manuals** icons in the Toptools for Hubs & Switches program group.

For the very latest information about Hewlett-Packard products, be sure to check out our Network City web page at <http://www.hp.com/go/procurve>

*Copyright © 1999-2000 Hewlett-Packard Company  
Hewlett-Packard Company*

*Workgroup Networks Division  
8000 Foothills Boulevard  
Roseville, California 95747-5551  
U.S.A.*

[Return to Hubs & Switches Contents](#)

[Return to Main Table of Contents](#)

Microsoft, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries. Pentium is a registered trademark of Intel Corporation. IBM and NetFinity are registered trademarks of International Business Machines Corporation. Compaq and Compaq Insight Manager are registered trademarks of Compaq Computer Corporation. Unicenter and TNG are registered trademarks of Computer Associates International, Inc. NetWare and Novell are registered trademarks of Novell, Inc. SCO Unix is a registered trademark of The Santa Cruz Operation, Inc.