



UM Services
User's Guide



UM Services
User's Guide

UM Services (12/2000)

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time. This publication was developed for products and services offered in the United States of America and the United Kingdom. It is possible that this publication may contain references to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM products, programming, or services in your country.

Requests for technical information about IBM products should be made to your IBM reseller or IBM marketing representative. No part of this publication may be reproduced or distributed in any form or by any means without prior permission in writing from the International Business Machines Corporation.

©Copyright International Business Machines Corporation 1999, 2000. All rights reserved.

Note to U.S. Government Users—Documentation related to restricted rights—Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corporation.

Trademarks

Alert on LAN, IBM, IntelliStation, Netfinity, Netfinity Manager, Netfinity Director, ThinkPad, and Wake on LAN are trademarks of IBM Corporation.

Microsoft, Windows, Windows NT, WIN32, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation.

Java and all Java-based trademarks or logos are trademarks of Sun Microsystems, Inc.

Intel, Pentium, and LANdesk are trademarks of Intel Corporation in the United States and other countries.

Other company, product, and service names mentioned in this document may be trademarks or servicemarks of others.

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Subject to IBM's valid intellectual property or other legally protectable rights, any functionally equivalent product, program, or service may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
N. Castle Drive
Armonk, NY 10504-1785
U.S.A.

Licensees of this program who wish to have information about it for the purpose of enabling: (1) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709, U.S.A. Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

Contents

Preface.....	ix
1. About UM Services	1
2. Preparing to Install UM Services	5
Preparing To Install UM Services.....	5
Supported System-Management Environments	6
UM Services Console	6
Tivoli Enterprise	6
Tivoli NetView	6
Microsoft SMS 1.2 or 2.0	7
CA Unicenter TNG Framework	7
LANDesk Management Suite.....	7
HP Openview.....	8
Installation Requirements.....	8
Hardware Requirements	8
Supported Operating Systems	8
Supported Browsers.....	9
Additional Installation Guidelines	9
3. Installing UM Services	13
Uninstalling UM Services.....	19
Starting the UM Services Console.....	19
Starting the UM Services Browser on a Local System	19
Starting UM Services Browser Remotely	20
Starting UM Services from Microsoft Management Console.....	20
Starting UM Services from a UIM Management Console.....	21
4. Using UM Services	23
Information Tab	24
Inventory Services.....	25

Basic System	26
Drives	28
Memory	31
Multimedia	33
Operating System	34
Ports	41
Monitor Services	42
Windows NT Event Log	42
Event Viewer	42
Notebook	46
System Health.....	49
Tasks Tab.....	52
Configuration	53
Alert on LAN.....	53
Asset ID	57
Date and Time	64
Network	65
SNMP	72
System Accounts.....	74
Users	74
Groups	75
UM Services Security	76
Security Levels	76
New User	78
User	80
Viewing User Properties.....	81
Tools.....	81
Remote Control	81
Shutdown	83
System Updates.....	84
5. Upward Integration Modules.....	87

Installing Upward Integration Modules	88
Tivoli Enterprise Plus Module Integration	89
Installing the Tivoli Enterprise Plus Module	89
Enabling Additional Functions.....	90
Using the Tivoli Enterprise Plus Module	95
Tivoli NetView 5.1.1 and 6.0 Integration	96
Installing the Tivoli NetView Upward Integration Module.....	96
Starting UM Services on NetView Clients	99
Using Tivoli NetView 5.1.1 and 6.0 to Obtain Inventory Data	99
Viewing UM Services SNMP Data from NetView	101
Forwarding SNMP Trap Information.....	102
Alert on LAN 2.0 Traps	103
Director Traps.....	104
MIB Browsing	104
CA Unicenter TNG Framework Integration	105
Configuring CA Unicenter TNG Framework	105
Installing the CA Unicenter TNG Framework Upward Integration Module	106
Reclassifying Existing Devices.....	108
Using CA Unicenter TNG Framework UIM.....	108
Launching UM Services with CA Unicenter TNG Framework UIM	109
Viewing UM Services Inventory from the 2D Map	109
Using AimIT to View Inventory	110
Viewing UM Services SNMP Alerts.....	110
Using ShipIT to Create a UM Services Software Package.....	111
Uninstalling the CA Unicenter TNG Framework Upward Integration Module	112
Intel LANDesk Management Suite Integration	112
Microsoft SMS Integration	113
Installing the Microsoft SMS Upward Integration Module	115
Customizing the SMS Installation.....	116
Modifying the SETUP.ISS File Manually	117
Uninstalling the Microsoft SMS Upward Integration Module.....	121

Using Microsoft SMS to View Client Computer Inventory	122
Microsoft SMS 1.2	122
Microsoft SMS 2.0	123
Installing Intel Alert on LAN Proxy	124
HP OpenView Integration Module	125
Installing UM Services Support on the OpenView Server	125
Accessing UM Services from the OpenView Console	127
Viewing UM Services Inventory Data from the OpenView Console.....	127
Adding UM Services Clients to the UM Services Submap	127
Populating the UM Services Submap	128
isUniversalService.....	128
isUMServicesCim	128
Launch HttpUM Services	128
Forwarding UM Services Events	129
Alert on Lan 2 Traps.....	130
Director Traps.....	131
MIB Browsing.....	131
Uninstalling OpenView Integration Support	131
Index	133

Preface

The *UM Services User's Guide* provides basic information for installing and using Universal Manageability (UM) Services on your system. It also provides information for installing and using UM Services Upward Integration Modules (UIMs) on systems running supported system-management applications.

Who Should Read This Guide

This guide is intended for the individuals who are responsible for installing and using UM Services (on their systems or on remote client systems in a network environment) and Upward Integration Modules (on supported system-management platforms). This guide assumes that you have extensive knowledge of server, mobile, and desktop system hardware; operating systems; Windows networking; desktop environments; system-management tasks; and the features and functionality that are provided by the supported system-management platforms.

What This Guide Contains

This guide contains the following chapters:

- “Chapter 1. About UM Services,” on page 1, provides an overview of UM Services.
- “Chapter 2. Preparing to Install UM Services,” on page 5, provides directions for starting UM Services on your IBM system.
- "Chapter 3. Installing UM Services", on page 13, guides you through the installation process for installing UM Services on supported operating systems.
- "Chapter 4. Using UM Services", on page 23, provides an overview of the UM Services console and includes brief descriptions of UM Services Information and Task functions.
- "Chapter 5. Upward Integration Modules", on page, provides information on installing and using UIMs with supported system-management applications.

Getting Help

UM Services includes an online troubleshooting guide that contains solutions for many common installation and usage issues. This troubleshooting guide is installed when you install UM Services, and it can be accessed from the **UM Services Troubleshooting** option in your **Start** menu.

Additional information and UM Services product updates, when available, can be obtained from the IBM Web site at:

<http://www.pc.ibm.com/ww/software/applications/ums>

1

About UM Services

IBM® Universal Manageability (UM) Services is a lightweight client that resides on managed computer systems. It provides a suite of graphical user interfaces (GUIs) that enhance the local or remote administration, monitoring, and maintenance of IBM systems, such as ThinkPad® computers, IntelliStation® computers, and Netfinity® servers.

With UM Services, a client-system user or remote system administrator can use a Web browser or the Microsoft® Management Console (MMC) and the UM Services console support to inventory, monitor, and troubleshoot IBM systems on which UM Services is installed.

This “point-to-point” system-management approach enhances support and enables a system administrator to effectively maintain IBM systems without having to install additional system-management software on the administrator console.

UM Services also includes support for Upward Integration Modules (UIMs). A system administrator who uses any supported system-management platform (such as Tivoli® Enterprise, CA Unicenter TNG Framework, Microsoft Systems Management Server) or HP OpenView can use UIMs to integrate portions of UM Services into the administrator console. Because it is designed to use industry-standard information-gathering technologies and messaging protocols (such as Common Information Model, Desktop Management Interface, and simple network management protocol), UM Services adds value to any of these supported workgroup or enterprise system-management platforms.

The following information describes the available components (services) that you can install on local UM Services client systems.

Basic Services

Basic Services includes a Java™ Virtual Machine, a Common Information Model (CIM) repository, a Desktop Management Interface (DMI) 2.0 compliant service provider, and basic instrumentation for gathering hardware inventory data. The inventory information that is provided by Basic Services can be viewed through a CIM browser such as Microsoft WBEMTEST. The IBM Managed Information Format (MIF) generator program (CIM2MIF) can also be used to generate inventory files that can be exported to system-management applications, such as Tivoli Enterprise, Microsoft Systems Management Server (SMS), or CA Unicenter TNG Framework. Basic Services must be installed on all UM Services clients in the network.

Director Support

IBM Director is an advanced Intel® processor-based workgroup hardware manager with centralized client and group-management console and server services. It includes object-oriented tools to provide flexibility and extendability, including Life Cycle Tools for added management over the entire life cycle of the asset. Installing this feature will enable the client system to be a part of this Universal Manageability process.

Web Based Access

Web Based Access offers a convenient Java-based tool for managing a client system and for viewing the CIM-based inventory data. If you install Web Based Access, a hypertext transfer protocol (HTTP) DAEMON will be installed and will require a user name and password to be typed during the installation. The user name and password will be used to limit access to the HTTP DAEMON. With Web Based Access installed on the client system, the client can be managed from any remote computer with a supported Web browser. No software other than a Web browser is needed on the remote computer.

Note: This component is selected for installation by default.

Web Based Remote Control

Using Web Based Remote Control, a system administrator can remotely take control of the client system desktop through a Web browser or MMC, enhancing the administrator's ability to diagnose system problems and troubleshoot the client system.

Note: You must install the Web Based Access component to install the Web Based Remote Control component.

System Health Monitoring

System Health Monitoring provides active monitoring of critical system functions, such as available disk space, system temperature, fan functionality, power supply voltage, and system cover removal. System Health Monitoring also provides software for enabling Alert on LAN functionality on systems that support this feature. With System Health Monitoring, you can detect system problems early, before system failures occur. The system administrator will be notified of a system problem by a CIM event, a simple network management protocol (SNMP) trap (SNMP traps are available only if SNMP access and trap forwarding are also enabled), or an SMS status message (Microsoft SMS 2.0 only). A critical problem also causes a message to be displayed on the monitor of the client system.

LANDesk Management Suite Integration

LANDesk® Management Suite Integration installs the Intel Common Base Agent on the client system. This enables the system administrator to use UM Services with LANDesk Management Suite.

Tivoli Management Agent

Tivoli Management Agent provides support on the client system that enables it to be managed by the Tivoli Enterprise system-management platform.

Simple Network Management Protocol (SNMP) Access and Trap Forwarding

This feature enables CIM information to be accessed from client systems that use SNMP. If System Health Monitoring is enabled, this option also enables System Health monitoring to

forward CIM events as SNMP traps. This component requires that you have the SNMP service (provided with your operating system) installed on the endpoint. If the SNMP service is not installed, you will be prompted to insert your operating system installation media and install SNMP during the UM Services installation.

DMI Support

When enabled, this feature maps Common Information Model (CIM) data and events from a managed client system to a Desktop Management Interface (DMI).

Online Help This option gives the system Administrator the flexibility to install UM Services with or without help documentation.

2

Preparing to Install UM Services

This section contains instructions for installing Universal Manageability Services (UM Services) on the client systems. Depending on your system-management environment, you can choose to install all of UM Services, or you can choose to install only selected portions of UM Services.

The UM Services installation program also includes support for installing Workgroup/Enterprise Integration on client systems running supported system-management platforms. Workgroup/Enterprise Integration adds an Upward Integration Module (UIM) to a supported system-management platform, such as CA Unicenter TNG Framework or Microsoft SMS. With UIMs, you can use your system-management software to manage clients running the UM Services client software. Workgroup/Enterprise Integration installation procedures are explained in "Chapter 5. Upward Integration Modules", page 87.

Preparing To Install UM Services

As noted in the previous chapter, UM Services includes a number of optional components that add value in a variety of system-management environments. Before you begin your installation, determine whether you will be using UM Services as a stand-alone client-based system-management solution, or whether you will be using UM Services to gather data for a supported system-management platform.

Also, UM Services require certain minimum hardware and software for installation. These requirements are listed on page 8.

Supported System-Management Environments

The UM Services components that you choose to install are largely determined by the system-management environment in which you are installing UM Services. Some components are of use to most system-management platforms, while others are of use only to specific platforms. The following sections offer example component selections based on the system-management platforms that are used to manage systems in the network.

UM Services Console

If you will be using a Web browser or MMC to manage UM Services client systems, install the following UM Services components on the client systems:

- Web Based Access
- System Health Monitoring
- Web Based Remote Control

Note: Systems using a Web browser or MMC to access UM Services locally require 64 MB of RAM to function properly.

Tivoli Enterprise

If you use Tivoli Enterprise to manage the client systems in your network, install the following UM Services components on the client systems:

- Web Based Access
- System Health Monitoring
- Tivoli Management Agent
- SNMP Access and Trap Forwarding

Tivoli NetView

If you use Tivoli NetView® to manage the client systems in your network, install the following UM Services components on the client systems:

- Web Based Access

-
- System Health Monitoring
 - Web Based Remote Control
 - SNMP Access and Trap Forwarding

Microsoft SMS 1.2 or 2.0

If you use Microsoft SMS 1.2 or 2.0 to manage the client systems in your network, install the following UM Services components on the client systems:

- Web Based Access
- System Health Monitoring
- SNMP Access and Trap Forwarding

Note: For SMS 1.2, the Upward Integration Module (UIM) must be installed on all primary site servers and management consoles. It does not need to be installed on the secondary servers.

For SMS 2.0, the UIM must be installed on all site servers and all management consoles.

CA Unicenter TNG Framework

If you use CA Unicenter TNG Framework to manage the client systems in your network, install the following UM Services components on the client systems:

- Web Based Access
- System Health Monitoring
- SNMP Access and Trap Forwarding

LANDesk Management Suite

If you use LANDesk Management Suite to manage the client systems in your network, install the following UM Services components on the client systems:

- Web Based Access
- System Health Monitoring
- LANDesk Management Suite Integration

HP Openview

If you use HP Openview to manage the client systems in your network, install the following UM Services components on the client systems:

- Web Based Access
- System Health Monitoring

Installation Requirements

Before you install UM Services, consider the following installation requirements:

- Hardware Requirements
- Supported Operating Systems
- Supported Browsers

Hardware Requirements

The UM Services Client in a Microsoft® Windows® operating system requires the following hardware, memory, and disk space:

- An IBM server, IBM desktop computer, IBM IntelliStation computer, or IBM ThinkPad mobile computer
Note: Client systems must support SMBIOS version 2.0 or later.
- An Intel Pentium 200 MHz or faster processor
- 75 MB of hard disk space on the client systems
- A minimum of 32 MB random access memory (RAM), or the recommended minimum for the operating system

Supported Operating Systems

The following operating systems support UM Services Client:

- Windows 2000—Server or Advanced Server
- Windows 2000 Professional
- Windows NT® Server 4.0 (with Service Pack 4 or later)
- Windows NT Workstation 4 (with Service Pack 4 or later)
- Windows 98

-
- Windows 95 (with original equipment manufacturer (OEM) Service Release 2 (OSR2) or later)
 - Windows Millennium

Supported Browsers

A World Wide Web browser is needed on the system from which you plan to manage remote UM Services client systems, and is required only if you are planning to install the UM Services Web Based Access or Web Based Remote Control options.

The following browsers support the UM Services console.

- Microsoft Internet Explorer 4.01 or later.

Notes:

- If you are using Internet Explorer 5.x, you must install the optional Java Virtual Machine (VM) support to access a client system running UM Services.
 - If you are using Internet Explorer and you reinstall Internet Explorer after installing UM Services, you must reapply the Microsoft VM update. The UM Services Client requires the Microsoft VM Build 3165 or later. Download the latest Microsoft VM from <http://www.microsoft.com/java>
 - The supported browser must have the file, URL, associated with opening the browser.
- Microsoft Management Console (MMC) 1.1 or later.
If you install UM Services before you install MMC, a Microsoft Management Console icon will not appear in the IBM Universal Manageability Services programs section of your **Start** menu.
 - Netscape Navigator or Netscape Communicator 4.51.
Note: Netscape Navigator 6.0 is not supported.

Additional Installation Guidelines

Before you install UM Services, consider these additional restrictions, requirements, and installation options:

- **Windows 95 installations**

Install DCOM95 before you install UM Services on systems running Windows 95. DCOM95 is included with Internet Explorer 4.0 or later and NetScape Navigator 4.5 or later. However, if one of these browsers is not installed on the system on which you are installing UM Services, you must install DCOM95 first.

To install DCOM95 and the Microsoft Virtual Machine (both of which are required by UM Services), run the program named **MSJAVX86.EXE** found in the directory to which you downloaded and decompressed the UM Services installation files. When this program finishes running, restart your system, delete (or rename) **MSJAVX86.EXE** from the installation directory, and then install UM Services.

If you are distributing UM Services remotely to systems running Windows 95, be sure to distribute and run the **MSJAVX86.EXE** program first. When running **MSJAVX86.EXE** remotely, use the following command:

```
MSJAVX86 /Q /R:N
```

Then, restart the remote system.

- **Default directory**

By default, the UM Services installation program installs the UM Services program files in **C:\Program Files\IBM\UMS**. If you do not want to install the program files in the default location, be prepared to provide an alternative installation drive and directory.

- **Microsoft Management Console (MMC) 1.1 or later**

You can use UM Services after installing MMC on systems running Windows 95, Windows 98, Windows 2000, Windows Millennium or Windows NT.

- **Running an unattended installation**

UM Services supports unattended installation. If you want to use your software distribution facility to install UM Services, you can set up an unattended installation for UM Services. UM Services can then be installed across your network from one central location. The format of the UM Services response file, named **SETUP.ISS**, is described in “Modifying the SETUP.ISS File

Manually” in the *Director User’s Guide* on the *Director with UM Services* CD.

■ **Using Microsoft Internet Information Server**

UM Services does not provide automatic integration with Microsoft Internet Information Server. The IIS configuration is a manual process. The configuration steps are as follows:

1. Disable the UMS HTTP Server.

Start the Services applet, found under **Administrative Tools**. Open the properties dialog for the UMS HTTPServ service. Stop the service and then change the startup type to Disabled. Delete the HTTPSERV Registry key from **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl Set\Services**.

2. Create an IBM UMS Web Site in IIS.

From Internet Services Manager, select your host computer and select create a New Web Site. This starts the Web Site Creation wizard. Name the site *IBM UMS*. If you will be accessing UMS only through IIS, assign port 411 to this site. If you will be configuring the UMS HTTPserv service to launch automatically at startup, you might want to assign a different port to the IIS site. The primary UMS provider should use port 411.

3. Assign the site’s home directory path to point to the UMS httpserv directory. If you choose the installations default, this is c:\Program Files\IBM\UMS\httpserv. Disallow anonymous access to the site by clearing the "Allow anonymous access to this Web site" check box.

4. Assign this directory read permissions only.

5. Enable **Server-Side Includes** for the IBM UMS site.

Display the IBM UMS sites properties and click the **Home Directory** tab. Click the configuration button that is in the middle right of the bottom section of the window. Make a new entry to start **ssinc.dll** from the **System32\inetrv** subdirectory of your **System** directory. You can specify that **ssinc.dll** will be started only on GET, POST actions.

6. Enable **Read Access** and **Script Execution**.

The Home Directory settings for the site must allow read access. Set **Execute Permissions** to **Scripts only**.

7. Disable **Anonymous Access**.

The UMS windows will not be displayed properly if **Anonymous Access** is enabled for the root. If you did not turn off anonymous access when creating the site, do so now. Display the IBM UMS sites properties and click the **Directory Security** tab. In the **Anonymous access and authentication** control section, click the **Edit** tab. Clear the **Anonymous Access** check box. Depending on your security requirements, you might also want to enable **Basic Authentication** for access from Netscape.

8. Enable CGI Script Execution for **cgi-bin**.

Expand the IBMUMS site tree and right click the Directory to display the Directory properties for the **cgi-bin** directory. In the middle of the window, remove read access. At the bottom of the sheet, change the **Execute Permissions** to **Scripts and Executables**.

9. Create an IBMUMSCGI account (optional).

At this point, users will not be able to view any UMS information under the following conditions:

- The user's account is not a member of the Administrative group.
- The browser is Internet Explorer.
- The browser system is not using Windows 2000 or the user is authenticated through the NT Challenge Response mechanism (NTLM) or Kerberos (Negotiate), not Basic Authentication (BASE64).

If you would like users to be able to view information, you must configure an account to access the WMI. Name the account IBMUMSCGI and set the password to ibmumscgiGuest.

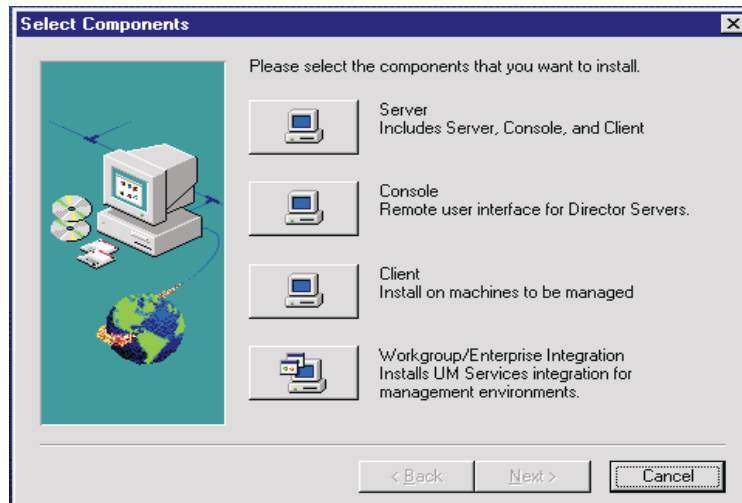
3

Installing UM Services

This section guides you through the installation process for installing UM Services on supported operating systems.

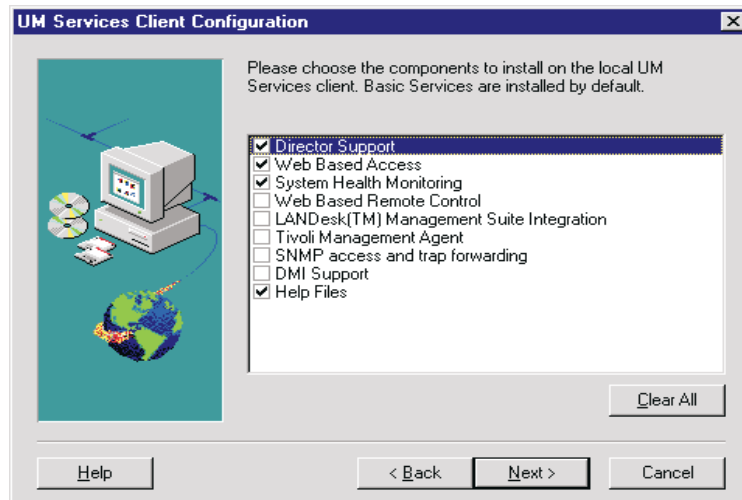
To install UM Services, use the following procedure:

1. Insert the *Director with UM Extensions* CD in the CD-ROM drive. The Director with UM Extensions window opens.
2. Click **Install Director**. The **Welcome** window opens.
3. Click **Next**. The License Agreement window opens. Click **Accept** to proceed. You must agree to the terms of the License Agreement to install UM Services. If you click **Decline**, the installation program will exit.
4. Click **Next**. The **Select Components** window opens. The installation choices are: Server, Console, Client and Workgroup/Enterprise Integration.



5. Click **Client**.

The **UM Services Client Configuration** window opens.



6. Select the check box beside any of the components that you want to install on the client system.

Note: The component **Basic Services**, is always selected. Basic Services installs a Java Virtual Machine, a Common Information Model (CIM) repository, and is the basic instrument for gathering hardware inventory data. The inventory information that is provided by Basic Services can be viewed through a CIM browser such as Microsoft WBEMTEST.

The following optional components are available. The components that are selected by default are indicated as such:

Director Support (default)

Director Support is an additional configuration option for the client installation only. IBM Director is an advanced Intel processor-based workgroup hardware manager, with centralized client and group management console and server services. Selecting this feature enables the client system to be managed in a Director environment by installing UM Services on this system.

Web Based Access (default)

Web Based Access offers a convenient Java-based tool for managing a client system and for viewing the CIM-based inventory data. If you install Web Based Access, a hypertext transport protocol (HTTP) DAEMON is installed and requires that a user name and password be typed during the installation. The user name and password limit access to the HTTP DAEMON. With Web-Based Access that is installed on the client system, the client system can be managed from any remote computer with a supported Web browser. The Web browser is the only software that is needed on the remote system.

System Health Monitoring (default)

System Health Monitoring provides active monitoring of critical system functions, such as disk space available, SMART drive alerts, system temperature, fan functionality, power supply voltage, and system cover removal (dependent upon the hardware options of a selected managed system). You can use System Health Monitoring to detect system problems early, before system

failures occur. System administrators are notified of a system problem by a CIM event, and SNMP trap (SNMP traps are available only if **SNMP access and trap forwarding** is also selected), or an SMS status message (Microsoft SMS 2.0 only). Critical problems also cause a message to be displayed on the monitor of the client system.

Web Based Remote Control

Web Based Remote Control enables a remote system administrator using a Web browser or MMC console to take control of the client system desktop, enhancing the administrator's ability to diagnose system problems and troubleshoot the system.

Note: You must install the Web Based Access component to install the Web Based Remote Control component.

LANDesk™ Management Suite Integration

LANDesk Management Suite Integration installs the Intel Common Base Agent on the client system. This enables the system administrator to use UM Services with LANDesk Management Suite.

Tivoli Management Agent

Tivoli Management Agent installs support on the client system that enables it to be managed by the Tivoli Enterprise system-management platform.

SNMP Access and trap forwarding (default)

This feature enables CIM information to be accessed from systems that use the simple network management protocol (SNMP). If System Health Monitoring is enabled, this option also enables System Health to forward CIM events as SNMP traps. This component requires that you have the SNMP service (provided with the operating system) installed on the endpoint. If the SNMP service is not installed, the system prompts you to insert the operating system installation media and install SNMP during the UM Services installation.

DMI Support

Selecting this component installs the Desktop Management Interface (DMI) compliant Service Provider. When enabled, this feature maps a managed system CIM data and events to DMI.

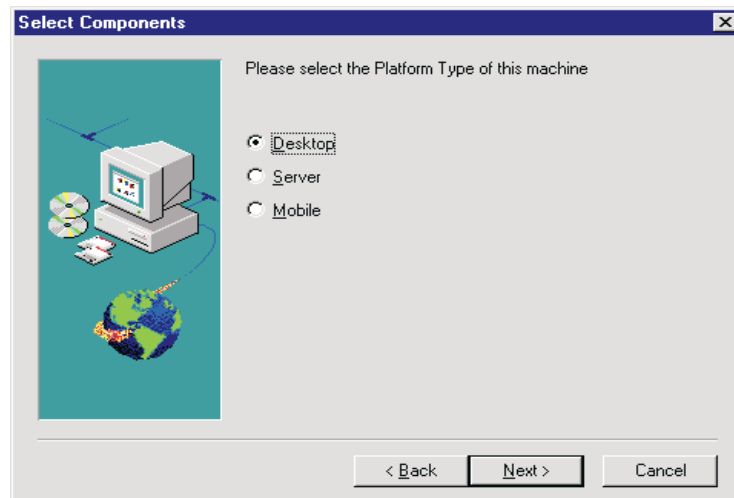
Help Files (default)

Selecting this component installs online documentation. Do not select this option if you are concerned about disk space or do not need online documentation installed on every client system.

7. Click **Next** to continue.

The **Choose Destination Location** window opens.

8. Click **Next** to accept the default directory (**c:\Program Files\UMS**), or click **Browse** to select a different directory.
9. If you did not select to install **DMI Support** in step 10, go to step 14. If you selected **DMI Support**, the **DMI Platform** window opens.



Select the type of platform that you are installing the DMI support to. Click **Next** to continue.

-
10. To use the UM Services console to manage this system, you must first provide a valid user ID and password before being allowed access to the system. In the **User ID** field, type the user ID. Then type the password in the **Password** field, and type the password again in the **Confirm Password** field.

Note: The user ID and password are case sensitive.

Then, select a TCP/IP port that is used to access the UM Services console. The default port is 411. If this port is not available, you can select port number 6411, 6500, 6600, or 6611. Make sure that other TCP/IP applications do not use the selected port.

11. Click **Next** to continue.
12. If you selected **SNMP access and trap forwarding** from the UM Services Client Configuration menu and do not have the SNMP network service installed, the UM Services installation program will prompt you with an SNMP installation query.
 - Click **No** to continue with the UM Services installation without installing the SNMP network service.
 - Click **Yes** to install the SNMP network service on the server. The **Installing SNMP** window and the **Network** window opens. Follow the instructions for installing SNMP. When the Windows operating system prompts you to restart the system, click **No**. In the **Installing SNMP** window, click **Next** to return to the UM Services installation program.
13. When the system asks you if you want to place a UM Services icon on the start menu, click **Yes** or **No**.
14. When the system asks you if you want to install files for remote control, click **Yes** or **No**.
15. When the system asks you if you require user authorization for remote control window access, click **Yes** or **No**.

The installation program begins installing the necessary files.
16. When the Director Installation Complete window opens, Click **Finish**.
17. Restart the computer now or later. If you click **Yes**, the system shuts down and restarts immediately. If you click **No** the UM

Services installation program closes. However, you must restart and log in to the system to begin using UM Services.

Uninstalling UM Services

You can uninstall UM Services through the Add/Remove Programs feature in the Windows Control Panel.

To uninstall UM Services, use the following procedure:

1. Click **Start** → **Settings** → **Control Panel**. The Control Panel opens.
2. Click the **Add/Remove Programs** icon. The **Add/Remove Programs Properties** window opens.
3. From the **Install/Uninstall** list, select **Director**, and then click **Add/Remove**.
4. Select Director, click the **Add/Remove** button.

The uninstallation process might take a while to complete.

Starting the UM Services Console

If the Web Based Access or Web Based Remote Control optional component is installed on a client system, you can use a Web browser or MMC to access and manage the client locally or remotely.

Note: IBM provides a Java class library (Swing/JFC with UM Services). Install this library on the Web browser before you access UM Services data. The first time you use a Web browser for UM Services, you will be asked to download the installation programs for this file. Click the HTML link to begin installation of the library. For Windows 95 and Windows 98, you will have to restart your UM Services Web browser for this Java library to take effect.

Starting the UM Services Browser on a Local System

During installation, if you clicked **Yes** to create icons on the Start menu, you can start UM Services locally from this menu.

Note: Systems using a Web browser or MMC to access UM Services locally require 64 MB of RAM to function properly.

To start UM Services, from the local system click

Start → **Programs** → **UM Services** → **UM Services Browser**.

The system starts the default Web browser and opens it to the Web address

http://localhost:tcpip_port

where *tcpip_port* is the TCPIP port that you selected during installation. You must type your user ID and password in the **UM Services User ID and Password** window.

Starting UM Services Browser Remotely

You can start UM Services remotely using a supported Web browser. In the address field of your browser, type

http://systemname:tcpip_port

where *systemname* is the TCP/IP address or the Internet Protocol (IP) address of the client and *tcpip_port* is the port number that is assigned for use by the UM Services console during UM Services client installation. Port number 411 is the default, but if this port is being used by another application, UM Services could also have been configured to use port number 6411, 6500, 6600, or 6611.

Starting UM Services from Microsoft Management Console

If you installed Microsoft Management Console (MMC) 1.1 and then installed UM Services on the client system, an icon is created on the Start menu from which you can start UM Services in the MMC.

To start UM Services, click **Start**→**Programs**→**UM Services**→**Microsoft Management Console**.

The Microsoft Management Console is available as part of the Windows NT Option Pack 4 or from:

<http://www.microsoft.com/MANAGEMENT/MMC>

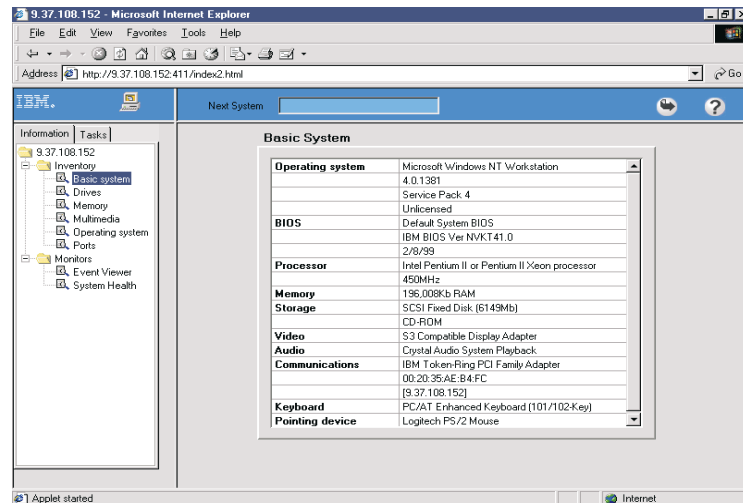
Starting UM Services from a UIM Management Console

If UM Services is integrated into Tivoli Enterprise 3.6, Tivoli NetView 5.1.1, SMS 1.2, SMS 2.0, CA Unicenter TNG 2.2 (Windows 95, Windows 98, Windows 2000 or Windows NT only), or HP OpenView, you can start UM Services directly from the management console. The management console starts either the default Web browser or the Microsoft Management Console (whichever is appropriate for the workgroup or enterprise environment). For more information, see “Chapter 6. Upward Integration Modules,” on page 151.

4

Using UM Services

When you have connected to a client system, the UM Services console opens in your Web browser or MMC. The console has two panes.



The Services pane is on the left side of the UM Services console and contains two tabs. Each tab contains a list of UM Services that are available on the client system. The following tabs are available from the Services pane:

- Information** — This tab contains a tree view of the UM Service that are used to gather hardware and software information from the client system.

-
- **Tasks** — This tab contains a tree view of the UM Services that are used to perform system-management and system-configuration tasks on the client system.

The Display pane is on the right side of the UM Services console and is a dynamic view that displays the interfaces and data that are associated with the service that is selected from the **Information** or **Tasks** tabs.

The following field and command icons also appear in the Display pane of the UM Services console:

Next System field

You can use the same browser window or MMC to access multiple UM Services client systems. In this field, type the TCP/IP address of another client running UM Services, and then press **Enter** to access another client system without opening another Web browser. This field is not available on MMC.

Export icon



With UM Services, you can create comma-separated-value (CSV) data files from the hardware and software data that is collected by many of the UM Services interfaces. These CSV files can be imported into many database programs so that you can create a centralized repository for data that is collected by UM Services. To create a CSV file, select a service from the Services pane. When UM Services has completed loading data, click the **Export** icon. If a CSV file can be created from the data that was collected, a new browser window opens, containing the CSV file data. You can then save this data by clicking **Save** from the **File** menu.

Help icon

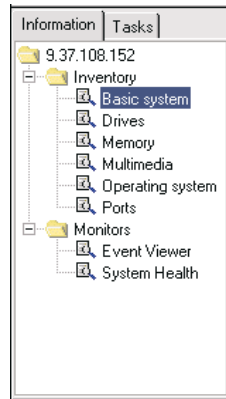


Online help is available for all UM Services. To access online help for a service, select the service from the Services pane and, when it has finished loading, click the **Help** icon.

Information Tab

The services that are available from the **Information** tab gather hardware information and software information from the client system. This data is gathered directly from the client system and represents the physical components of the system or the current, monitored state of the client system as reported by monitoring hardware and software in the client system. The data that is presented in the Information service

interface is static. A UM Services user cannot change or configure the data.



There are two categories in the **Information** tab:

- Inventory
- Monitors

The sections that follow describe each of the services that are available from the **Information** tab.

Inventory Services

Inventory Services gather information about the physical devices that make up the client system (such as disk drives, multimedia adapters, video adapters, and memory) or the operating system of the client system. The following Inventory Services are available:

- Basic system
- Drives
- Memory
- Multimedia
- Operating system
- Ports

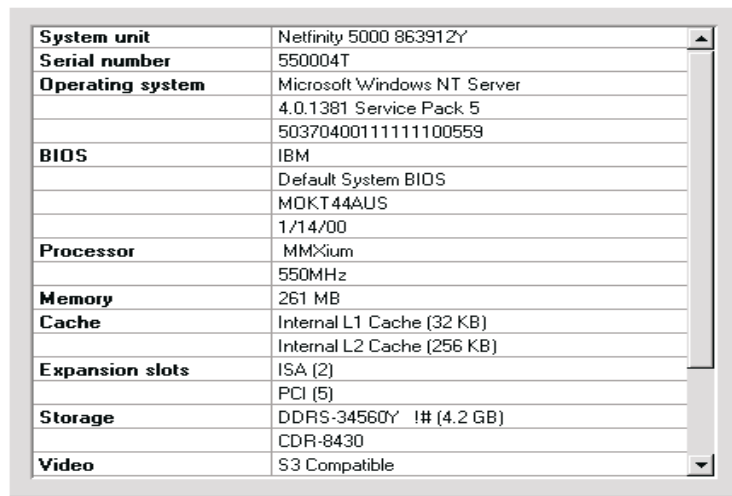
Descriptions of each of the Inventory services that you can select from the **Information** tab follow.

Basic System

The Basic System service gathers and displays general information about the client system hardware and operating system.

Note: Not all client systems have all of the items that can be displayed in the Basic System interface. If a client system does not have a particular item, the field that is associated with that item will not appear in the Basic System interface.

To start the Basic System service, click **Information**→**Inventory** →**Basic system** in the Services pane. The following interface opens in the Display pane.



The screenshot shows a window with a table of system information. The table has two columns: 'Item' and 'Description'. The items listed are System unit, Serial number, Operating system, BIOS, Processor, Memory, Cache, Expansion slots, Storage, and Video. The descriptions provide specific details for each item, such as 'Netfinity 5000 86391ZY' for the system unit and 'Microsoft Windows NT Server' for the operating system.

System unit	Netfinity 5000 86391ZY
Serial number	550004T
Operating system	Microsoft Windows NT Server 4.0.1381 Service Pack 5 50370400111111100559
BIOS	IBM Default System BIOS MOKT44AUS 1/14/00
Processor	MMXium 550MHz
Memory	261 MB
Cache	Internal L1 Cache (32 KB) Internal L2 Cache (256 KB)
Expansion slots	ISA (2) PCI (5)
Storage	DDRS-34560Y !# (4.2 GB) CDR-8430
Video	S3 Compatible

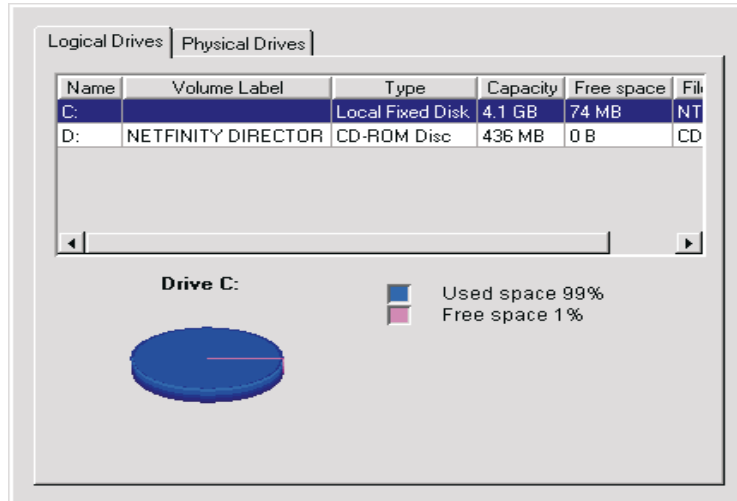
The Basic System interface provides information about the items that are described in the following table.

Item	Description
System unit	The manufacturer and model of the client system.

Item	Description
Serial number	The serial number of the client system.
Universal Manageability Services	The version and build number of Universal Manageability Services installed on the system.
Operating system	The name, version number, and service pack level (if applicable) of the operating system that is running on the client system.
BIOS	The version and completion date of the basic input/output system (BIOS) of the client system.
Processor	The type (for example, Pentium®, Pentium II, or Pentium III) and clock speed of the microprocessor that is installed on the system board of the client system.
Memory	The amount of random access memory (RAM) installed in the client system, in kilobytes (KB).
Cache	The amount of microprocessor memory cache that is available to the microprocessor of the client system.
Expansion slots	The number and type (for example, PCMCIA or PCI) of expansion slots in the client system.
Storage	The type and size, in megabytes (MB), of storage devices that are installed in the client system, such as hard disk drives, CD-ROM drives, or CD-RW (read/write) drives.
Video	The type of video adapter that is installed in the client system.
Communications	The network interface adapter or modem that is installed in the client system, the media access control MAC address of the adapter, and the internet protocol (IP) address of the client system.
Keyboard	The type of keyboard that is attached to the computer.
Pointing device	The type of pointing device, such as a mouse, trackball, or TrackPoint® that is attached to the client system.

Drives

The Drives service gathers and displays information about the physical and logical disk drives that are installed in the client system. To start the Drives service, click **Information** → **Inventory** → **Drives** in the Services pane. The following interface opens in the Display pane.



The Drives interface contains two tabs:

Logical Drives

Click the **Logical Drives** tab to display information about the logical drives that are configured on the client system.

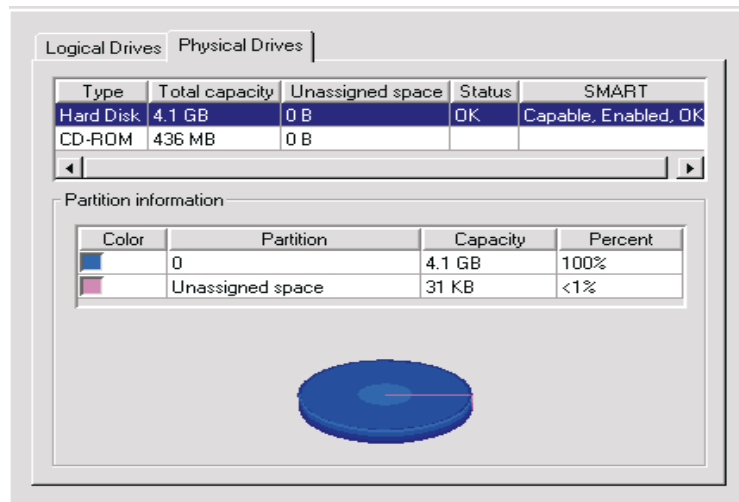
The **Logical Drives** interface is displayed by default. For additional information about each entry on the **Logical Drives** interface, click any disk row. The interface displays a pie chart that shows used space and free space on the selected logical drive. Used space contains the applications and files that are on the disk, and free space is available for adding files or applications.

The **Logical Drives** interface provides information about the items that are described in the following table.

Item	Description
Name	The drive letter that is assigned to the logical drive or partition.
Volume Label	The name or label of the storage volume.
Type	The type of logical drive, such as a removable drive.
Capacity	The size of each logical drive, measured in megabytes (MB) or gigabytes (GB).
Free Space	The amount of disk space available on the logical drive.
File System	The file system in use by the partition.

Physical Drives

Click the **Physical Drives** tab to display information about the physical drives installed in the client system. The **Physical Drives** tab displays the Physical Drives interface.



The **Physical Drives** interface shows the type; capacity; unassigned space; and self-monitoring, analysis, and reporting technology

(SMART) data of each physical drive that is installed in the client system. To see if a physical hard disk has partitions, click any disk row. If the selected disk has partitions, information about the partitions is displayed in the **Partition information** section of the **Physical Drives** interface.

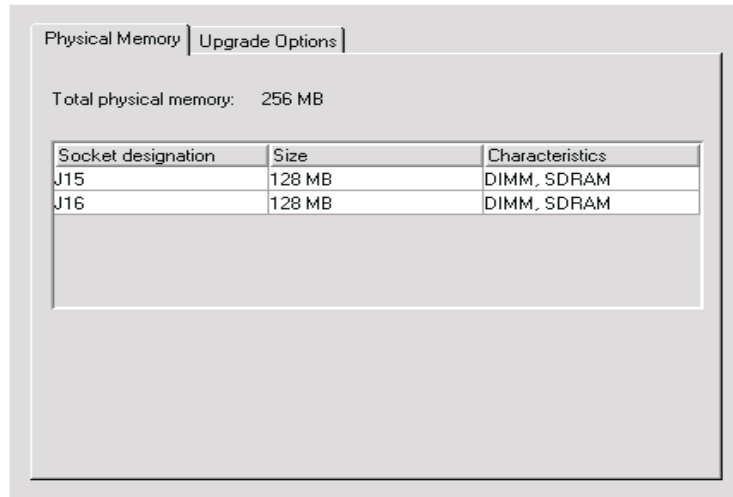
The partition information is displayed as a pie chart, showing the portion of the total physical disk that is used by each partition.

The Physical Drives interface provides information about the items described in the following table.

Item	Description
Type	The type of physical drive.
Total capacity	The total amount of data that can be stored by each physical drive, measured in KB, MB, or GB.
Unassigned space	The amount of space on a hard disk that is not used by logical partitions.
Status	The condition of the drive as reported by SMART.
SMART	Health alerts, generated by a status monitor, for a physical drive if potential failure exists.
Partition Information	
Color	The color of the partition being displayed on the graphic.
Partition	The drive letter that is mapped to the partition.
Capacity	The total amount of data that can be stored by each partition, measured in MB or GB.
Percent	Partition percentage of the entire drive.

Memory

The Memory service gathers information about the physical memory that is installed in the client system and provides information about memory upgrade options that are available for the client system. To start the Memory service, click **Information** → **Inventory** → **Memory** in the Services pane. The following interface opens in the Display pane.



The Memory interface contains two tabs:

Physical Memory

Click the **Physical Memory** tab to display information about the physical memory that is installed in the client system.

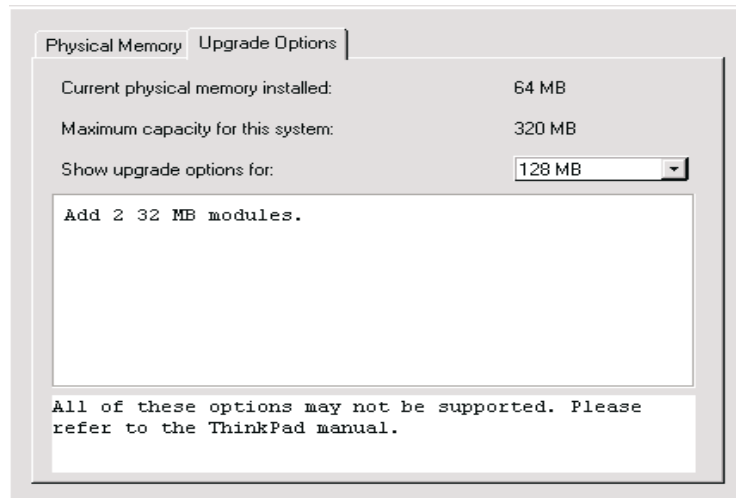
Upgrade Options

Click the **Upgrade Options** tab to display information about memory upgrade options for the client system.

The Physical Memory interface is displayed by default and provides information about the items that are described in the following table.

Item	Description
Socket Designation	The type and number assignment of memory sockets used to hold the memory modules.
Size	The size of the memory module currently installed in a given socket.
Characteristics	Details about the modules installed.

The Upgrade Options interface shows the current physical RAM that is installed in the computer, and the maximum capacity of the client system, which refers to the total RAM that can be installed in the computer. If you want to install additional memory in the client system, select the amount of memory that you want to install to display additional information on proper memory configuration.



The Upgrade Options interface provides information about the items that are described in the following table.

Item	Description
Current Physical Memory Installed	The amount of total physical random access memory (RAM) that is installed on the system board.
Maximum Capacity for this System	The number of the socket and the type of memory module the socket can hold. For example, DIMM-2 refers to a dual in-line memory module (DIMM) in socket 2, and SIMM-3 refers to a single in-line memory module (SIMM) in socket 3.
Show Upgrade Options for a total of:	The size (in MB) of the memory module that is currently installed in each socket.

Multimedia

The Multimedia service gathers information about the multimedia adapter that is installed in the client system. To start the Multimedia service, click **Information** → **Inventory** → **Multimedia** in the services pane. The following interface opens in the Display pane.

Audio	No audio device found
Video	
Adapter description:	S3 Compatible
Chip type:	S3 Trio64V2
RAM:	1 MB
Color bits/pixel:	8
Resolution:	1024x768
Refresh rate:	75

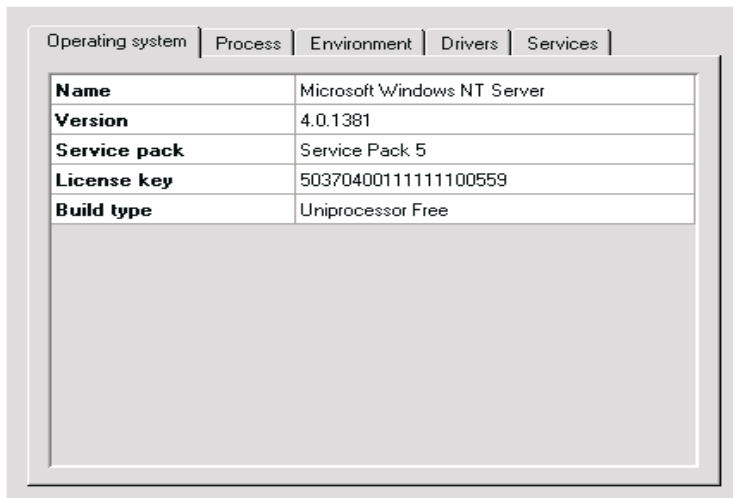
The Multimedia service has one interface that provides information about the system audio and video, described in the following table.

If an audio or video adapter is not installed in the client system or if information from the adapter is unavailable, the field that is associated with the missing data will not be shown in the interface.

Item	Description
Audio	The name of the audio adapter that is installed in the client.
Video	The name of the video adapter that is installed in the client.
Adapter description	The name of the video adapter installed on the computer.
Chip type	The type of video chip that is used by the video adapter.
DAC type	The type of digital to analog connector.
RAM	The amount of random access memory (RAM) available for use by the video subsystem.
Color bits/pixel	The number of color bits per picture element (pixel) that can be displayed by the video adapter.
Resolution	The picture element (pixel) resolution that is currently displayed by the video adapter (for example, 640 X 480 or 800 X 600).
Refresh rate	The frequency, in megahertz (MHZ), with which the monitor screen is cleared and redrawn.

Operating System

The Operating System service gathers information about the operating system that is installed and running on the client system. To start the Operating System service, click **Information** → **Inventory** → **Operating System** in the Services pane. The following interface opens in the Display pane.



The Operating System interface contains the following interfaces (the Services interface is displayed only for client systems running Windows NT):

Operating System

Click the **Operating System** tab to display general information about the operating system, including name, version, and service pack level.

Process

Click the **Process** tab to display information about the processes or tasks that are currently running on the client system.

Environment

Click the **Environment** tab to display information about the environment variables that are used by the client operating system.

Drivers

Click the **Drivers** tab to display information about the device drivers that are used by the client system.

Services

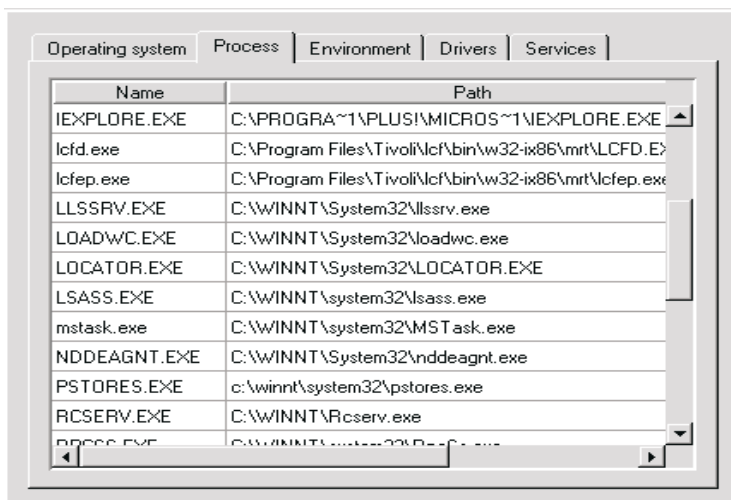
Click the **Services** tab to display information about the current state and start mode of services that are installed on the client

system. This interface is available only for client systems running Windows NT.

The Operating System interface is displayed by default and provides information about the items that are described in the following table.

Item	Description
Name	The name of the operating system.
Version	The version number of the operating system.
Service pack	The operating system service pack level installed on the system, if any.
License key	The license key number or code that was specified when the operating system was installed. Depending on the screen resolution, you might need to move the horizontal scroll bar to the right to view this item completely.
Build type	The operating system build type. Build type can refer to the processor configuration that the operating system is designed to run on (uniprocessor or multiprocessor), or to whether the build is a retail (or “Free”) version or debug (or “Checked”) version. Depending on the screen resolution, you might need to move the horizontal scroll bar to the right to view this item completely.

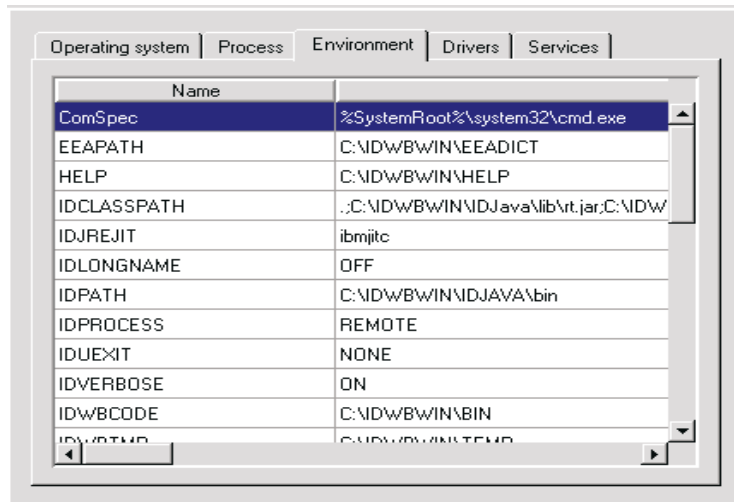
Click the **Process** tab to display the Process interface.



The Process interface provides information about the items that are described in the following table.

Item	Description
Name	The name of the executable process.
Path	The complete path to the executable file.
Kernel mode time	The amount of time that the computer processor spends in kernel mode because of this process. Depending on the screen resolution, you might need to move the horizontal scroll bar to the right to view this item completely. This item appears only for client systems running Windows NT.
Process ID	The identifying number that is assigned to the process by the system according to startup sequence. Depending on the screen resolution, you might need to move the horizontal scroll bar to the right to view this item completely.

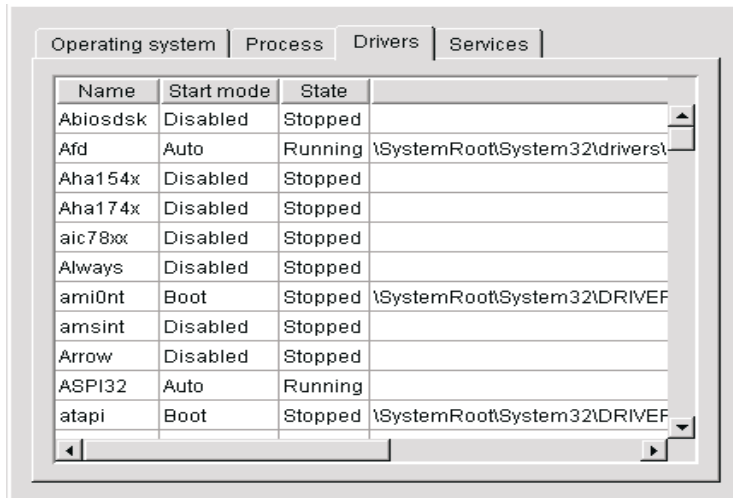
Click the **Environment** tab to display the Environment interface.



The Environment interface provides information about the item that is described in the following table.

Item	Description
Name	The name of the environment variables that are used by the client system.
Value	The settings information for each environment.
Detailed Value	An in-depth display of the name which includes the path.

Click the **Drivers** tab to display the Drivers interface. You must have administrator privileges to update the Driver Start mode and the Start/Stop options.

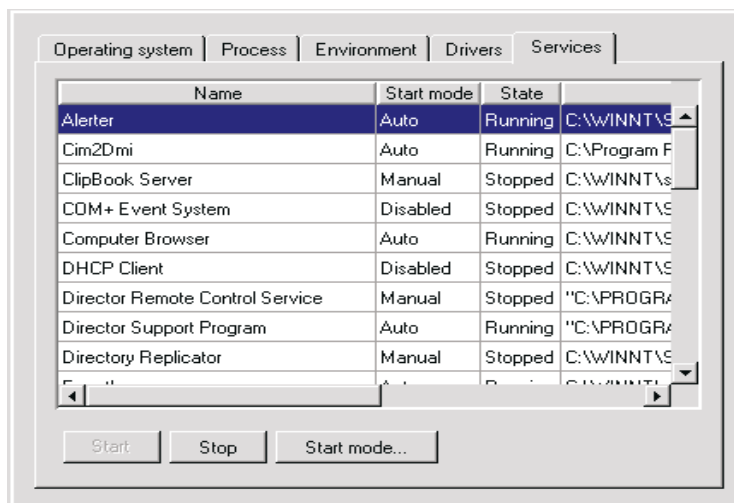


The Drivers interface provides information about the items that are described in the following table.

Item	Description
Name	The name of each device driver in the operating system directory.
Start mode	The start mode that is assigned to each device driver. Depending on which mode is selected, a device driver is incorporated or not incorporated into the operating environment. <i>Disabled</i> means that the device driver is not added to the operating environment. <i>Auto</i> means that the device driver is automatically started when the operating system is started. <i>Boot</i> means that the device driver is initialized during the operating system startup (boot) sequence. <i>Manual</i> means the user must start the driver. <i>System</i> means the system which occurs when the operating system starts the driver.
Start	To start a driver, highlight the driver and click the start button.
Stop	To stop a driver, highlight the driver and click the stop button.

Item	Description
State	The current run state of each device driver (Running or Stopped). This item applies only to client systems running Windows NT. State values are not displayed on client systems running Windows 95 or Windows 98.
Command line	The complete path to the device driver, such as C:\System Root \System32\adapti.sys . To view the complete command line, move the horizontal scroll bar to the right.

Click the **Services** tab to display the Services interface.



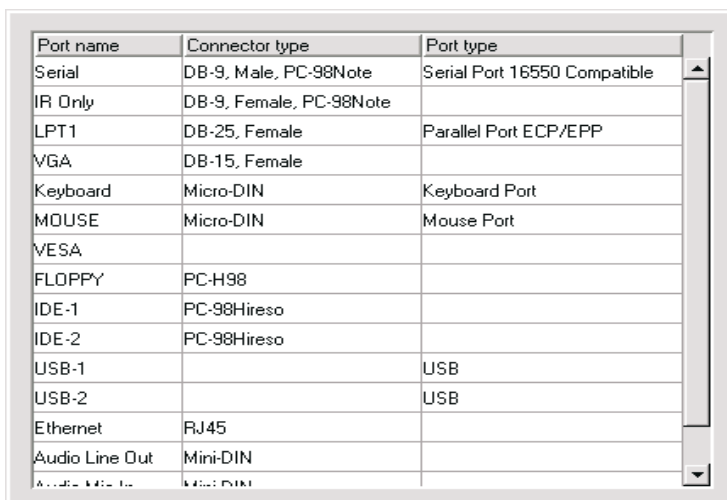
The Services interface provides information about the items that are described in the following table.

Item	Description
Name	The name of the service (for example, EventLog or Remote Control Service).
Start mode	The start mode of the service. For each service, the start mode can be Auto for automatic, Manual for manual start, or Disabled when the service is turned off or is unavailable.

Item	Description
State	The current run state of each service (Running or Stopped).
Start	To start a Service, highlight the name and click start.
Stop	To stop a Service, highlight the name and click stop.
Start Mode	Click to select service start mode. The modes are: auto, manual and disabled.
Command line	The complete path to the device driver, such as C:\System Root \System32\adapti.sys . To view the complete Command line, move the horizontal scroll bar to the right.

Ports

The Ports service gathers information about the input and the output ports and connectors on the client system. To start the Ports service, click **Information** → **Inventory** → **Ports** in the Services pane. The following interface opens in the Display pane.



Port name	Connector type	Port type
Serial	DB-9, Male, PC-98Note	Serial Port 16550 Compatible
IR Only	DB-9, Female, PC-98Note	
LPT1	DB-25, Female	Parallel Port ECP/EPP
VGA	DB-15, Female	
Keyboard	Micro-DIN	Keyboard Port
MOUSE	Micro-DIN	Mouse Port
VESA		
FLOPPY	PC-H98	
IDE-1	PC-98Hireso	
IDE-2	PC-98Hireso	
USB-1		USB
USB-2		USB
Ethernet	RJ45	
Audio Line Out	Mini-DIN	
Audio Line In	Mini-DIN	

The Ports service provides information about the items that are described in the following table.

Item	Description
Port name	The name of the input or output port (for example, LPT1, Keyboard, or Ethernet).
Connector type	The type of connector for each port (for example, DB-9 or DB-25 Female).
Port type	Type of port (for example, serial, parallel, or Universal Serial Bus).

Monitor Services

Monitor Services use system monitoring hardware and software that is included with the UM Services Client to gather data about the current operational state of the client system, such as temperature, battery time remaining, and contents of the Windows NT Event Log on the client system. The three Monitor Services are as follows:

- Event Viewer
- Notebook (available only if you are using UM Services on an IBM ThinkPad model 560, 570, 600, or 770)
- System Health

Windows NT Event Log

Applications, device drives, operating systems, and UM Services record hardware events and software events in the NT Event Log. The UM Services Event Viewer displays these events.

Event Viewer

The Event Viewer service shows the contents of the Windows NT Event Log. To start the Event Viewer service, click **Information** → **Monitors** → **Event Viewer** in the Services pane. The following interface opens in the Display pane.

Type	Date	Time	Event	Source	Category	User
information	28-Jun-00	3:28:53 PM	0	lcfd	0	
error	28-Jun-00	2:59:27 PM	10	WinMgmt	0	
error	28-Jun-00	2:59:27 PM	10	WinMgmt	0	
error	28-Jun-00	2:59:27 PM	10	WinMgmt	0	
information	28-Jun-00	2:54:32 PM	0	lcfd	0	
information	27-Jun-00	4:37:27 PM	0	lcfd	0	
information	27-Jun-00	3:39:41 PM	0	lcfd	0	
information	20-Mar-00	7:37:49 PM	0	lcfd	0	
information	20-Mar-00	6:58:51 PM	0	lcfd	0	
information	20-Mar-00	6:50:42 PM	0	lcfd	0	
information	20-Mar-00	6:13:53 PM	0	lcfd	0	
error	20-Mar-00	6:10:49 PM	101	TWGServer	2	
information	15-Mar-00	2:20:30 PM	0	lcfd	0	
.....	14-Mar-00	5:00:15 PM	10	WinMgmt	0	

Information Warning Error
 Success Audit Failure Audit

The Event Viewer interface provides information about the items that are described in the following table.

Item	Description
Type	The log category (information, warning, error, success audit, or failure audit).
Date	The date when the event took place, in mm/dd/yy format.
Time	The time when the event occurred, in hh:mm:ss format for a.m. or p.m.
Event	The identification number that is automatically given to an event, with related events getting the same number. For example, Service Control Manager has 7001 and 7002 event numbers, regardless of the time of the event.

Item	Description
Source	The program, application, system, or security problem that led to the event (for example, WinMgmt, DCOM, Simple Network Management Protocol (SNMP), AOLAgent, or UM Services).
Category	A number that identifies the category that the event falls into. This is used to organize the events. To view this field, move the scroll bar to the right.
User	The ID of the user. To view this field, move the horizontal scroll bar to the right.

The Event Log can contain a large number of entries. With the Event Viewer service, you can filter the contents of the Event Log before viewing the entries. Before Event Viewer loads the contents of the Event Log, you must select a log category. These broad categories help limit the number of Event Log entries that will be loaded into the Event Viewer. From the **Log** menu, select an Event Log category that corresponds to the Event Log entries you want to view, or click **Load All Events** to display all log entries.

Note: The Event Log can contain thousands of individual entries. Clicking **Load All Events** can result in significant delays while the contents are loaded into the Event Viewer.

The available selections are as follows:

Application

Displays the 30 most recent log entries that result from software issues or application issues, faults, and problems.

System

Displays the 30 most recent log entries that result from system issues or hardware issues, faults, and problems.

Security

Displays the 30 most recent log entries that result from security problems, such as invalid user ID or password entries and other attempted security violations.

Use the check boxes at the bottom of the **Event Viewer** window to filter the contents of the Event Viewer by event type. The event type provides a general description of the severity of the event. The following event-type check boxes are available:

Information

Displays rows of informational entries that are related to the Application, System, or Security Event Log category that you selected.

Warning

Displays rows of warning entries that indicate a severe problem to resolve for an Application, System, or Security problem.

Error

Displays logs that result from security issues, such as password or user ID failures or other access problems, or attempted security violations.

Success Audit

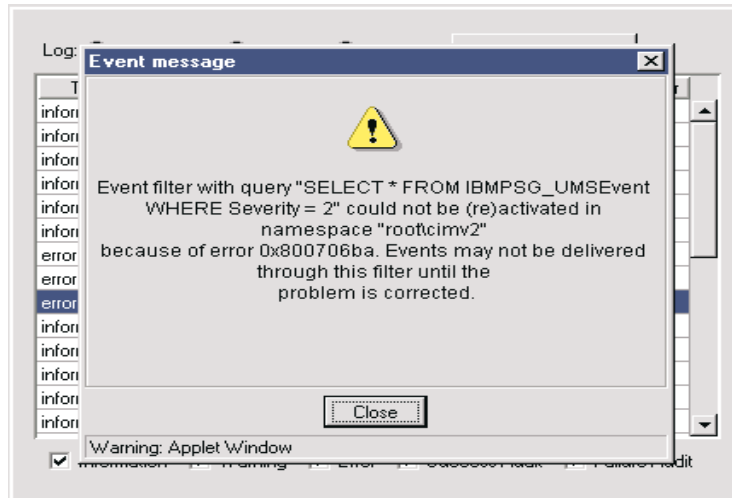
Displays event information on successful events.

Failure Audit

Displays event information on unsuccessful events.

Only entries that correspond to a selected check box will be displayed in the Event Viewer. For example, if you want to view only entries that are the results of a system error, select the **Error** check box and leave the other selections cleared. If you select an event-type check box and no information is displayed, it means that there are no Event Log entries that correspond to the selected event type.

You can use Event Viewer to display additional information about any entry that appears in the window. To display additional information about any entry, click the entry to highlight it, and then double-click the entry. A window opens, containing additional information about the event.



Notebook

The Notebook service is available only if UM Services is running on an IBM ThinkPad model 560, 570, 600, or 770 system. If the client system is not one of these supported models, this service is not displayed when you click **Information**→**Monitors**.

The Notebook service gathers and displays information about ThinkPad computers. To start the Notebook service, click **Information** → **Monitors** → **Notebook** in the Services pane. The following interface opens in the Display pane.

Battery	
Battery	Main
Status	Fully Charged
Estimated run time (mins)	N/A
Remaining charge (%)	100
Full charge time (mins)	N/A
Battery type	Lithium-ion

The Notebook service interface contains two categories. The Battery interface is displayed by default.

Battery

Click the **Battery** tab to display information about the ThinkPad battery power supply.

Enclosure status

Click the **Enclosure status** tab to display information about the power supply that is currently being used by the computer and for information about whether the computer is currently docked in a docking station.

The Battery interface provides information about the items that are described in the following table.

Item	Description
Battery	The battery that is being used by the ThinkPad computer (Main or Backup).
Status	The charge status of the battery (Fully Charged, Partial, High, Low, Critical, Charging, Charging High, Charging Low, Charging Critical, Unknown).

Item	Description
Estimated Run Time (minutes)	<p>The number of minutes of run time that are left on the battery.</p> <p>If the ThinkPad computer is plugged into an electrical outlet by using an adapter, the Estimated Run Time will show N/A.</p>
Remaining Charge (%)	<p>The approximate percentage of battery charge remaining, running from 100% to 0%.</p> <p>If the ThinkPad computer is plugged into an electrical outlet using an adapter, the Remaining Charge will continue to show the percentage of battery life that remained at the time the system was plugged in.</p>
Full Charge Time (minutes)	<p>The amount of time that is needed to charge the battery to full capacity. If the battery is fully charged, the Full Charge Time will show N/A.</p>
Battery Type	<p>The type of battery. The ThinkPad computer uses a lithium-ion battery.</p>

Click the **Enclosure status** tab to display the **Enclosure Status** interface. The **Enclosure Status** interface provides information about the items that are described in the following table.

Item	Description
Power Source	<p>The current power source being used by the ThinkPad computer (Battery or On-Line).</p>
Docking Station	<p>The current docking status of the ThinkPad computer (Docked or Not Docked).</p>

System Health

UM Services automatically monitors the client systems for changes in a variety of system-environment factors, including temperature and voltage. Each monitored value has a System Health normal range. If the monitored value stays within normal range, the assumption is that the System Health is normal. However, if any of these monitored values falls outside of acceptable System Health parameters, UM Services can automatically generate five forms of output to alert the system administrator of this state change. The following alert output can be generated by UM Services:

- **System Health** graphical user interface (GUI) window in UM Services
- Alert messages
- Alert messages that are sent as simple network management protocol (SNMP) traps
- Alert messages that are sent as System Management Server (SMS) status messages
- Common Information Model (CIM) events

You can use the System Health service to check the status of all health monitors that are supported by the client system. To start the System Health service, click **Information** → **Monitors** → **System Health** in the Services pane. The following interface opens in the Display pane.

Health	Description	Date & Time
Normal	\\.\physicaldrive0	30-Nov-00 12:27:06 PM
Normal	disk space c:	30-Nov-00 12:27:59 PM

The System Health interface provides information about the items that are described in the following table.

Item	Description
Health	The current state of the monitored device (Normal, Warning, or Critical).
Description	A description of the monitored device.
Date & Time	The date and time stamp applied to for the health event. The format is DD/MM/YY hh:mm:ss (AM or PM).

Health reports are gathered from a variety of system devices. One of these devices is the LM Sensor which performs environmental monitoring. The health reports that are available on a client system are dependent on the availability of components that contribute to health reports. The following are some examples of potential System Health event messages and the circumstances that cause them:

Chassis Intrusion

If the system chassis has been opened, a Warning System Health event is generated, regardless of the reason.

Fan Failure

If the system cooling fan fails, a Critical System Health event is generated. This might be the only prediction of a temperature-related event.

LAN Leash

LAN Leash detects if a client system is disconnected from the LAN, even when the computer is off. A Critical System Health event is generated if a client system is disconnected from the LAN.

Low Disk Space

If free disk space is low, a Warning or Critical System Health event is generated.

Processor Removed

If the microprocessor is removed from the client system, a Warning System Health event is generated.

Temperature Out of Specification

If the microprocessor temperature is out of the specified range, a Warning System Health event is generated.

Voltage Out of Specification

If there is a dramatic change in the voltage of the power that is supplied to any part of the client system, a Warning or Critical System Health event is generated.

Predicted Failure Alert (PFA)

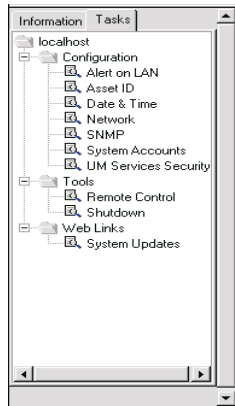
SMART-drive enabled systems generate events if operational thresholds on the hard disk drive are exceeded.

Redundant NIC

If the redundant network interface card is configured for automatic failover, a Warning or Critical System Health event is generated. The Redundant NIC feature is supported only on Windows NT and Windows 2000.

Tasks Tab

The services that are available from the **Tasks** tab help the system administrator manage the client systems. Users with less than system-administrator authority can view the available screens, but only system administrators can change or update system configurations and use the available tools.



UM Services displays only the tasks that are associated with the components that are installed on a client system. For example, if the Web Based Remote Control feature is not installed on a client system, the task Remote Control (under Tools) is not displayed for that system. Requirements and optional installations are noted under each task heading. Certain security levels are required so that users can view or edit selected features in the UM Services program. See "User Security " on page 76 for additional information.

There are three main categories in Tasks services:

- Configuration (beginning on page 53)
- Tools (beginning on page 81)
- Web Links (beginning on page 84)

The sections that follow describe each of the services that are available from the **Tasks** tab.

Configuration

There are seven setup options that are associated with the Configuration task.

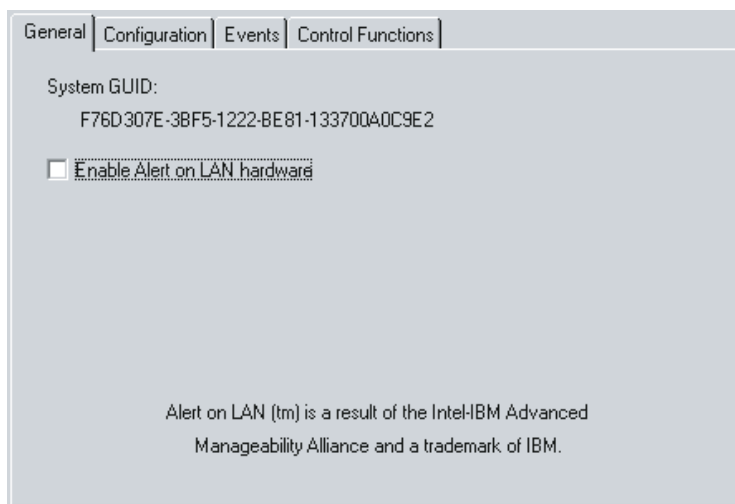
- Alert on LAN
- Asset ID
- Date and Time
- Network
- SNMP
- UM Services Security
- System Accounts

Alert on LAN

Note: Alert on LAN is displayed in the task list only for IBM PC 300@PL, PC 300, PC300GL computers, IBM ThinkPad A20x, A21X, T20 and T21 and NetVista model systems on which Alert on LAN hardware is installed.

A user with administrative security status can use the Alert on LAN task to set the options that are related to network system alerts.

To start the Alert on LAN service, click **Tasks** → **Configuration** → **Alert on LAN**. The following interface opens in the Display pane.



The Alert on LAN interface provides information about the items that are described in the following table. Each section in the table denotes a tabbed window within the Alert on LAN task.

Item	Description
General Tab	
System GUID	A Globally Unique ID (GUID) is assigned to each system board for system-management purposes. The GUID is stored in the BIOS on the system board.
Enable Alert on LAN hardware	This option determines whether the system alerts are on or off. Select the check box to enable system alerts.
Configuration Tab	
Proxy server (IP address port)	The internet protocol address for the server you use to communicate with the client systems. The IP address is assigned by the system administrator. (default port is 5500.)

Item	Description
Heartbeat timer period	<p>The Alert on LAN proxy computer verifies that the client system is running. This is the number of seconds between system checks. The default value is 32.</p> <p>The enabled heartbeat timer period values range from 43 to 5461 seconds and can be set in intervals of 43 seconds.</p>
Watchdog Timer Period	<p>If the watchdog timer indicates that a client system has stopped, the watchdog timer automatically sends a message to the proxy computer. This is the period between polls for the watchdog timer (measured in seconds). The default value is 43.</p> <p>The watchdog timer period values range from 86 to 5461 seconds and can be set in intervals of 86 seconds.</p>
Transmission attempts	The number of retries for transmission after the client system stops. The default value is 3.
Event Polling Period	The polling period for software problems. The default value is 30.
Events Tab	
Cover Tamper	If the cover of the managed system has been opened or removed, an event message is generated.
LAN Leash Tamper	LAN Leash detects if a client system is disconnected from the LAN, even when the computer is off. If a client system is disconnected from the LAN, an event message is generated.
Temperature Out of Specification	If the microprocessor temperature is out of the specified range, an event message is generated.

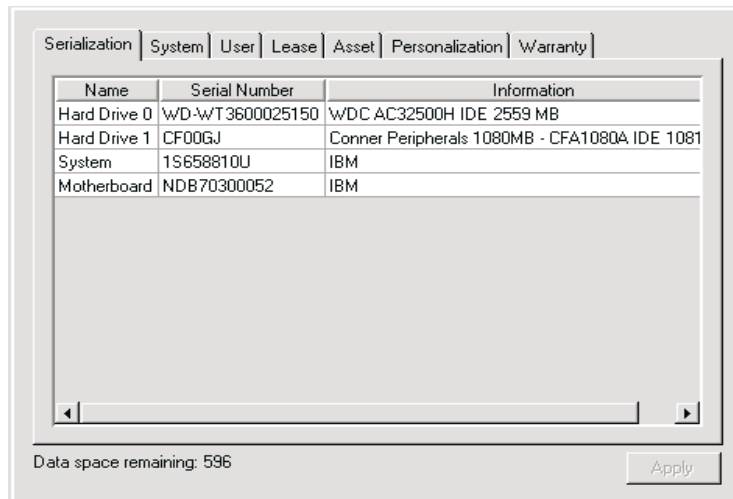
Item	Description
Watchdog	If the operating system of the managed system is not functioning, or is in a suspended state, an event message is generated.
Voltage Out Specification	If there is a dramatic change in the voltage of the power supplied to any part of the client system an event message is generated.
Processor 0	Click to enable the notification of a watchdog.
Processor 1	Click to enable the notification of a processor missing sensor report.
Auto-clear events	If this option is enabled, the client system sends an alert each time the condition is present (multiple alerts). If this option is disabled, the system sends an alert for a condition only once (no reminder alerts).
Clear All Events	Select this option and click Apply , to clear the events log.
Control Functions Tab	
Power Down	Click to power down the system. You will receive this message as a system state report.
Power Up	Click to restart power up system. You will receive this message as a system state report.
Reboot	Click to restart your system. You will receive this message as a system state report.
Presence Ping	Returns the message that the system is not on but is still connected to the network.

If you make changes to any of the Alert on LAN default user options, click **Apply** to save the changes and return to the UM Services main window.

Asset ID

The Asset ID service contains the hardware information for the client system. To start the Asset ID service, click

Tasks→**Configuration**→**Asset ID**. The Asset ID interface contains the following interfaces:



Serialization

Click the **Serialization** tab to display serial numbers for the client system hardware.

System

Click the **System** tab to display the current client system characteristics: system name, MAC address, user login name, operating system, GUID address, IBM LAN Client Control Manager (LCCM) Profile.

User

Click the **User** tab to display the user profile: user name, telephone number, work location, department, and professional position.

Lease

Click the **Lease** tab to display the information on the lease agreement for the client system hardware.

Asset

Click the **Asset** tab to display the inventory factors that are related to the client system.

Personalization

Click the **Personalization** tab to display the free-form window where you can add information on your systems, users, or computers.

Warranty

Click the **Warranty** tab to display the information on the warranty agreement for the client system hardware.

When you click **Asset ID** from the UM Services task list, the Serialization window opens. To access any of the other Asset ID windows, click the appropriate tab.

Serialization

Click the **Serialization** tab to display the Serialization interface. The Serialization interface displays the serial numbers for the various components in the client system.

The Serialization interface provides information about the items that are described in the following table.

Item	Description
Name	The hardware component name.
Serial Number	The serial number for the hardware component.
Information	Descriptive information for the hardware component.

System

Click the **System** tab to display the System interface. The System interface displays information about the client system.

Serialization | System | User | Lease | Asset | Personalization | Warranty

System Name PRIMMDDOM

MAC Address 00:20:35:31:CC:72

Login Name PRIMM_DOM\Administrator

Operating System Microsoft Windows NT Server

System GUID <empty>

LCCM Profile YY

Data space remaining: 1017

Apply

The System interface provides information about the items that are described in the following table.

Item	Description
System Name	The NetBEUI name of the client system (the computer name as it appears under Network Properties). NetBEUI is NetBIOS extended user interface, and NetBIOS is network basic input/output system.
MAC Address	The unique hexadecimal character string that identifies the network adapter in the client system.
Login Name	The user ID that the system administrator assigned at installation.
Operating System	The operating system (for the management server or for the computer where UM Services resides).

Item	Description
System GUID	The client system Global Unique Identifier (GUID). This is your BIOS unique ID number.
LCCM Profile	The profile name of the IBM LAN Client Control Manager (LCCM), if applicable.

User

Click the **User** tab to display the User interface. The User interface displays information about the logged-in user.

The screenshot shows a web interface with a navigation bar at the top containing tabs: 'Serialization', 'System', 'User', 'Lease', 'Asset', 'Personalization', and 'Warranty'. The 'User' tab is currently selected. Below the navigation bar is a form with five input fields, each with a label to its left: 'Name', 'Phone', 'Location', 'Department', and 'Position'. At the bottom left of the form area, there is a red text message: 'Data space remaining: -21'. At the bottom right, there is a button labeled 'Apply'.

The User interface provides information about the items that are described in the following table.

Item	Description
Name	The user login name.
Phone	The user phone number.
Location	The user office location.

Item	Description
Department	The user department name or number.
Position	The user job title.

Lease

Click the **Lease** tab to display the Lease interface. The Lease interface displays lease information for the client system.

The screenshot shows a software interface with several tabs: 'Serialization', 'System', 'User', 'Lease', 'Asset', 'Personalization', and 'Warranty'. The 'Lease' tab is selected. Below the tabs are five input fields: 'Start Date' (with a dropdown for 'September', a spinner for '27', and a spinner for '2000'), 'End Date' (with a dropdown for 'September', a spinner for '27', and a spinner for '2000'), 'Term (Months)' (with a text input field containing '0'), 'Amount' (with an empty text input field), and 'Lessor' (with an empty text input field). At the bottom left, it says 'Data space remaining: 975'. At the bottom right, there is an 'Apply' button.

The Lease interface provides information about the items that are described in the following table.

Item	Description
Start Date (mm/dd/yy)	The date that the lease agreement began.
End Date (mm/dd/yy)	The date that the lease agreement ends.
Term (months)	The number of months for which the client system is leased. In this field, you may enter 0 to 255 characters.

Item	Description
Amount	The total price of the lease agreement. In this field, you may enter 20 characters or less.
Lessor	The name of the company that leased the client system. In this field, you may enter 64 characters or less.

Asset

Click the **Asset** tab to display the Asset interface. The Asset interface displays inventory information about the client system.

The screenshot shows a software interface with several tabs: 'Serialization', 'System', 'User', 'Lease', 'Asset', 'Personalization', and 'Warranty'. The 'Asset' tab is selected. Below the tabs, there are two date pickers: 'Purchase Date' and 'Last Inventoried', both set to 'January 1, 1999'. Below these are two text input fields: 'Asset Number' and 'RF-ID'. At the bottom left, there is a red text message: 'Data space remaining: -21'. At the bottom right, there is an 'Apply' button.

The Asset interface provides information about the items that are described in the following table.

Item	Description
Purchase Date (mm/dd/yy)	The date the client system was purchased.
Last Inventoried (mm/dd/yy)	The date of the last inventory check.

Item	Description
Asset Number	A unique number that is assigned to the client system for inventory purposes. In this field, you may enter 64 characters or less.
RF-ID	The radio-frequency identification (RF-ID) number that was encoded in the client system by the manufacturer. Not all computers have RF-ID capabilities. This is a fixed field and cannot be changed.

Personalization

Click the **Personalization** tab to display the Personalization interface.

The Personalization interface is a free-form window where you can type information about your users, system, or computer. There is a 64-character maximum for each of these fields.

The screenshot shows a software interface with a tabbed menu at the top containing: Serialization, System, User, Lease, Asset, Personalization (selected), and Warranty. Below the tabs is a table with two columns: 'Label' and 'Value'. There are five rows of empty text input fields in each column. At the bottom left of the table area, it says 'Data space remaining: -21'. At the bottom right, there is an 'Apply' button.

Warranty

Click the **Warranty** tab to display the Warranty interface. The Warranty interface displays information about the warranty on the client system.

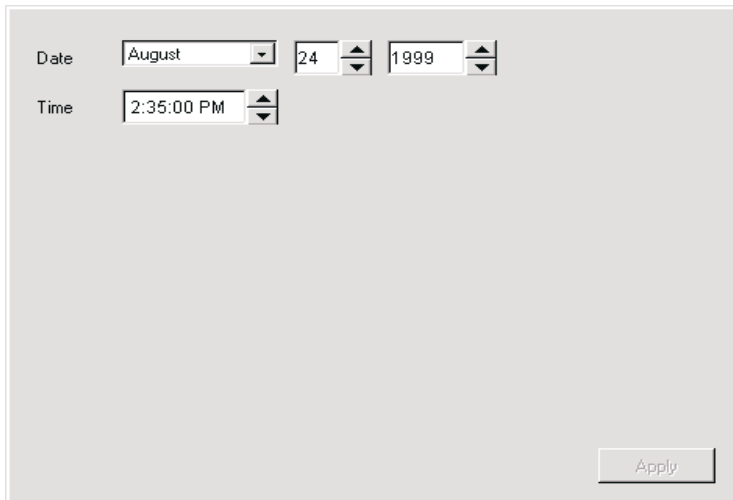
The Warranty interface provides information about the fields that are described in the following table.

Item	Description
Duration (months)	The duration of the warranty agreement. There is a 255 character maximum for this field.
Cost	The total cost of the warranty. There is a 20 character maximum for this field.
End Date (mm/dd/yy)	The date that the warranty ends.

Date and Time

Use the Date and Time service to set the date and time that are displayed on the client system. For the date, you have separate fields for month, day, and year. For the time, you have a field for the local time.

To start the Date and Time service, click **Tasks** → **Configuration** → **Date and Time** in the Services pane. The following interface opens in the Display pane.



A screenshot of a dialog box for setting the date and time. The 'Date' section has a dropdown menu set to 'August', a spinner box set to '24', and another spinner box set to '1999'. The 'Time' section has a spinner box set to '2:35:00 PM'. An 'Apply' button is located in the bottom right corner of the dialog box.

Network

The Network service provides information about your network. The following tabs are available under **Network**:

IP Address

Provides routing information for your network.

DNS

Provides information on the distributed database system that is used to map domain names to IP addresses.

WINS

Provides information about the WINS server.

Domain/Workgroup

Provides information about the domain or workgroup for the client.

Modem

Provides a list of modems installed on the client system.

When you click **Network** from the UM Services **Tasks** tab, the **IP Address** tab interface opens. Click the **DNS** tab or the **Modem** tab to view those windows.

IP Address Tab

The IP Address interface provides routing information for your network. Click **Tasks** → **Configuration** → **Network** to display the IP Address interface.

IP Address | DNS | WINS | Domain/Workgroup

Adapter
IBM Shared RAM Token-Ring Adapter

Use DHCP for automatic configuration
 Configure manually

IP Address: . . .
Subnet Mask: . . .
Default Gateway: . . .
MAC Address: 00:06:29:F0:11:FB

Apply

The IP Address interface provides information about the items that are described in the following table.

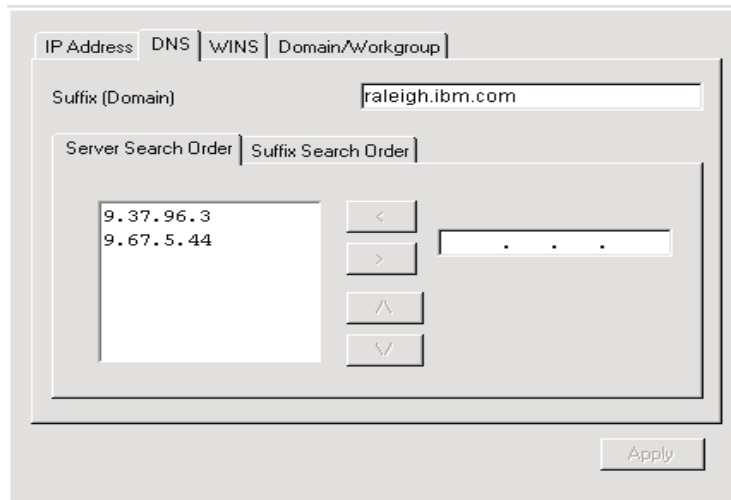
Item	Description
Network Adapter	Select the appropriate network adapter from the list.
Use DHCP for automatic configuration	Select this option to configure IP addresses automatically.
Configure manually	Select this option to configure IP addresses manually. When this option is selected, the remaining entry fields are enabled.

Item	Description
IP Address	The IP address of the client system. If you do not use DHCP to obtain an IP address, you must type the values into the IP Address and Subnet Mask fields manually.
Subnet Mask	<p>A bit mask that is used to identify which bits in an IP address correspond to the network address and which bits correspond to the subnet portions of the address.</p> <p>The address mask has ones in positions corresponding to the network and subnet numbers and zeros in the host-number positions.</p>
Default Gateway	The IP address for the default gateway server that you are using to communicate with other networks.
MAC Address	The unique hexadecimal number that identifies the network adapter in the client system.

DNS Tab

Domain Name System (DNS) is the distributed database system that is used to map domain names to IP addresses.

From the UM Services task list, click **Tasks** → **Configuration** → **Network** → **DNS** tab to display the interface.



The DNS interface displays the following items.

Item	Description
Servers	The alphabetic identifier for your server with the network domain (IP address).
Suffixes	The text strings for the domain.
Apply	Changes are not saved until you click the Apply button.

Note: The up arrow button is enabled when an item is selected in the list box and is not the topmost entry. The down arrow button is enabled when an item is selected in the list box and is not the bottom entry. Clicking the up arrow or down arrow button moves the selected entry up or down one position in the list.

The **Remove** (>) button is enabled only when an item is selected in the list box. Removing an item from the list box removes the item from the list box and puts it into the text field.

WINS

The **Windows Internet Naming Service (WINS)** interface provides information about NetBIOS names and their corresponding IP addresses.

From the UM Services Task list, click **Tasks**→ **Configuration**→ **Network**→ **WINS** tab to display the interface.

The WINS interface provides information about the items that are described in the following table.

Item	Description
WINS Servers	Registered NetBios name with the associated IP address.
Primary	The address for the primary server.
Secondary	The address for the secondary server.
Apply	Click Apply to save changes.

Domain/Workgroup

The Domain/Workgroup interface lists the client system with its associated domain or workgroup.

From the UM Services task list, click

Tasks→**Configuration**→**Network**→ **Domain/Workgroup** tab to display the interface.

The screenshot shows a configuration window with four tabs: IP Address, DNS, WINS, and Domain/Workgroup. The Domain/Workgroup tab is active. It contains the following fields and controls:

- Computer Name:** A text box containing the value "PRIMMDOM".
- Member of:** A section with two radio buttons: "Domain" (which is selected) and "Workgroup".
- Domain:** A text box containing the value "PRIMM_DOM" (visible only when the "Domain" radio button is selected).
- Workgroup:** An empty text box (visible only when the "Workgroup" radio button is selected).
- Create a Computer Account in the Domain:** An unchecked checkbox.
- User Name:** An empty text box (visible only if the checkbox is checked).
- Password:** An empty text box (visible only if the checkbox is checked).
- Apply:** A button at the bottom right.

The Domain/Workgroup interface provides information about the items that are described in the following table.

Item	Description
Computer Name	The name given to the client system. This naming scheme enables identification of the computer.
Domain	The client is a member of the domain. A domain requires that user's validate their account before they can log on to the network.

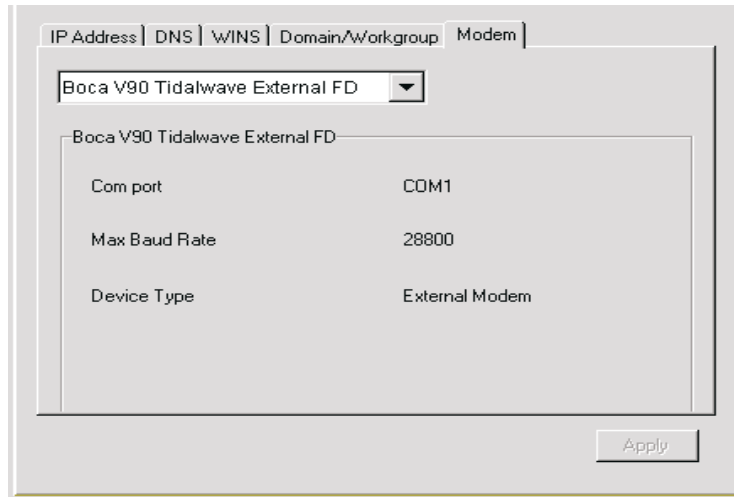
Item	Description
Workgroup	The client is a member of a workgroup. The workgroup is a collection of clients and servers with no centralized logon validation.
Apply	Changes are not saved until the Apply button is pushed.

MODEM

The Modem interface provides information about the modem type, speed, connector and device.

From the UM Services task list, click

Tasks→**Configuration**→**Network**→**Modem** tab to display the interface.



The modem interface provides information about the items that are described in the following table.

Item	Description
Modem	The drop-down list provides the name of the modem. Only installed modems are listed.
Comport	Lists the specific port that the modem is using.
Max Baud Rate	The maximum rate at which the modem operates.
Device Type	Describes the type of modem (internal or external).

SNMP

Note: The SNMP task appears on the task list only if the SNMP service is installed on the operating system.

The SNMP task provides the ability to work with community strings that are used in network communication and to set trap destination addresses.

Click **Tasks** → **Configuration** → **Network** → **SNMP** to display the SNMP interface.

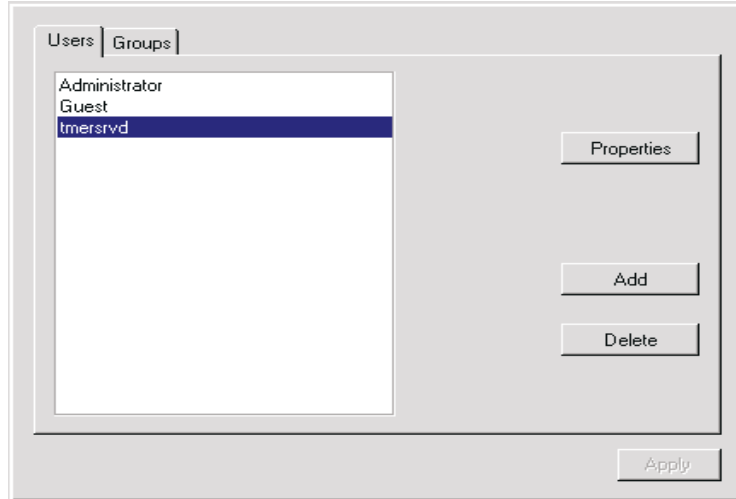
The screenshot shows the SNMP configuration window. At the top, there is a 'Community Name' dropdown menu currently set to 'community'. Below it are 'Add...' and 'Remove' buttons. The 'Trap Destination' section contains a list box with two entries: '9.37.88.123' and '2.44.36.4', with the second entry selected. Below the list box are 'Add...', 'Edit...', and 'Remove' buttons. An 'Apply' button is located at the bottom right of the window.

The **SNMP** screen displays the following the items.

Item	Description
Community name	A unique character string that identifies the community. The community name enables your network-management system (NMS) to verify that a server is authorized to take a specific action. If the server community name matches the community name that is assigned to the requested information or action, the NMS provides the information or action to the server. You can add or remove a unique community name.
Trap Destination	A list of network management system IP addresses to which the server can send alerts. You can add, remove, or edit a trap destination. To modify a trap destination, select an IP address and click Edit .

System Accounts

The System Accounts task provides remote administration of user security and group security within a Windows operating system. To start the System Account service, click **Tasks** → **Configuration** → **System Accounts** in the Configuration pane.



Users

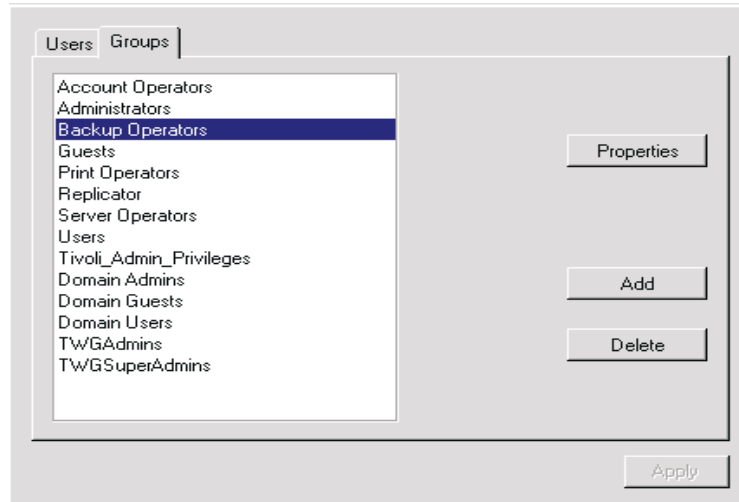
The Users tab interface provides information about the items that are described in the following table.

Item	Description
Properties	Edit or view user properties
Add	Click the Add button to add a new user.
Delete	Click the Delete button, to delete a user.

Groups

The Groups interface enables the administrator to review and edit members within the group. Click the **Groups** tab to display a list of all groups.

Note: The **Properties** and **Delete** buttons are initially disabled. They become enabled when a group is selected in the list box.



The **Groups** interface provides information about the items that are described in the following table.

Item	Description
Groups	List of global groups.
Properties	Edit or view group properties.
Add	Click the Add button to add a new group.
Delete	Click the delete button to delete a group.

UM Services Security

The UM Services Security displays user names, provides the ability to add and remove user names, and sets the security level and password options for each user name.

Security Levels

The security level that is assigned to a user affects that user's ability to access the UM Services program and the ability to view, manipulate, and access selected features in the program. The following security levels are associated with UM Services:

Disabled A disabled user is not permitted to log in (usually a temporary state). The disabled state is not technically a security level but is included here because users with Administrator privileges can use it to override other security levels and temporarily prevent access to the UM Services program.

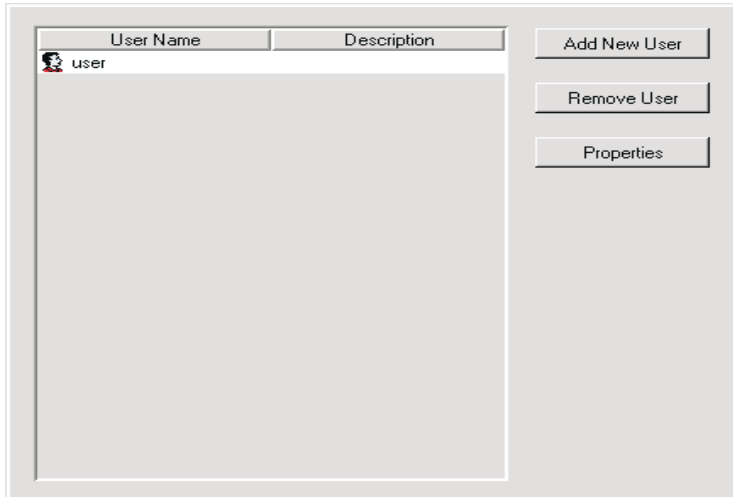
Browse, User, and Power User

Users with Browse, User, or Power User privileges can access much of the UM Services program. They cannot change settings or save typed information. In this release of the UM Services program, there are no practical differences between the Browse, User, and Power User privileges.

Administrator

Users with Administrator privileges have full control over the UM Services program. In addition to having full read and write access to the UM Services program, they can add new users, assign and change passwords, and assign security levels.

Click **Tasks** → **Configuration** → **User Services Security** to display the following interface.



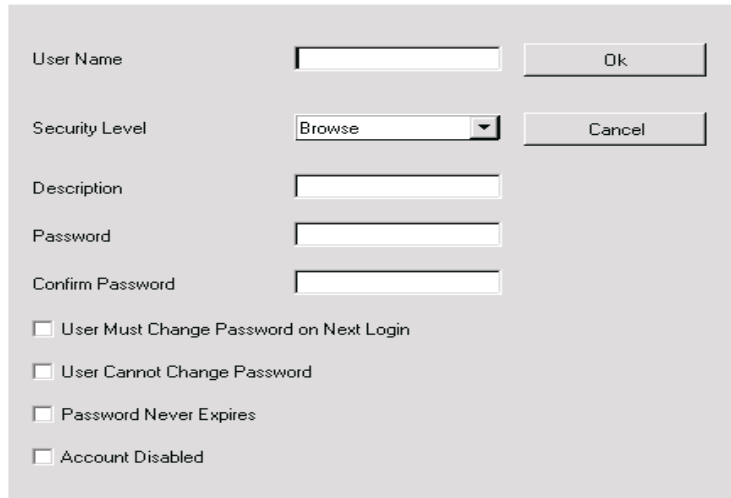
The UM Services Security interface provides information about the items that are described in the following table.

Item	Description
Add New User	To add a new user, highlight user name and click Add New User .
Remove User	To remove a user, highlight the user name and click Remove User .
Properties	To view or edit user properties, highlight the user and click Properties .

New User

Use the Add New User interface to add new UM Services users with the appropriate security levels and password options.

To display the Add New User interface, from the UM Services Security interface, click **Add New User**.



The Add New User interface contains the following items.

Item	Description
User Name	A unique character string that identifies the user (32 characters maximum).
Security Level	The level of system access authority the user is granted. From the list, select the security level that is appropriate for the user that you are adding.

Item	Description
Description	Information about the user, such as title, department, or reason for granting access to the UM Services program (32 character maximum).
Password	The user password (32 character maximum, case sensitive). There are no restrictions on the characters that can be used in passwords.
Confirm Password	This field must contain the same character string as the Password field (32 character maximum, case sensitive).
User Must Change Password on Next Logon	Select this check box if you want to force the user to change the password the next time the user accesses the UM Services program.
User Cannot Change Password	Select this check box if you want to prevent the user from changing the password. If this check box is selected, only someone with Administrator privileges can change the password.
Password Never Expires	Select this check box if you do not require the password to be changed at regularly scheduled intervals.
Account Disabled	Select this check box if you want to temporarily disable this user's access to the UM Services program. As a system administrator, you cannot disable your own account. This ensures that at least one account with Administrator privileges remains active.

The following table lists the user security levels.

Item	Description
User	Limited read/write
Power User	Limited read/write
Administrator	Read/write, lock/unlock, assign security levels, add new users and passwords

Note:

- Disabled users cannot access the UM Services program. Administrators can use the disabled state to override other security levels and temporarily prevent access to the UM Services program.
- Users with Browse, User, or Power User privilege have similar privileges in this release of the product. Though these users can access much of the UM Services program, they cannot change settings to save typed information.
- Users with Administrator privileges have the highest degree of control over the UM Services program. They can add new users, assign and change passwords, lock and unlock selected features, and assign security levels.

User

You can use the User Services Security interface to remove a user from UM Services. To remove a user, use the following procedure:

1. From the User Security interface, highlight the user that you want to remove.
2. Click **Remove User**. The following message is displayed:
Are you sure you want to remove user?
3. Click **Yes**. The user is removed.

Viewing User Properties

You can use the UM Services Security interface to review or edit user properties such as description, security level, and password options. To view or edit user properties, use the following procedure:

1. From the **UM Services Security** interface, highlight the user that you want to view or edit.
2. Click **Properties**. The **User Properties** interface opens.

You can view or edit the properties that are listed in this interface.

Tools

On the UM Services task list there are two items under Tools:

- **Remote Control** —Provides a way to control one computer to from another computer.
- **Shutdown** — Provides three shutdown options.

Note: Administrator level of security is required to use Tools functions.

Remote Control

Notes:

- The Remote Control service appears on the task list only if the Remote Control option is installed on the client system. If you did not select Web Based Remote Control during the UM Services installation, the Remote Control option is not displayed.
- Remote Control is not supported when you use a Web browser or MMC to manage the client systems.

You can use the Remote Control interface to set configuration options for remote-control sessions.

Click **Tasks** → **Tools** → **Remote Control** to display the Remote Control interface.

The screenshot shows a dialog box for configuring remote control settings. It includes the following fields and options:

- Access type:** A dropdown menu set to "Monitor".
- Grace period:** A dropdown menu set to "0".
- Proceed if timeout:** Radio buttons for "Yes" (selected) and "No".
- Change state on Target:** Radio buttons for "Yes" and "No" (selected).
- Desktop optimization:** Radio buttons for "Yes" (selected) and "No".
- Color reduction:** Radio buttons for "16", "256", and "Nothing" (selected).
- Enable compression:** Radio buttons for "Yes" (selected) and "No".
- Refresh rate:** A text input field containing "100".

At the bottom, there are three buttons: "Start session", "Default", "Cancel", and "Apply".

The Remote Control interface displays the following items.

Item	Description
Access type	The access type (Monitor or Active) determines whether you will monitor the client system or actively control it.
Grace period	Number of seconds before the management server takes active control of the client system. This is the number of seconds between the warning and the actual active control. If you are having trouble with the management server timing out, increase the grace period.
Proceed if timeout	This timeout option is associated with the grace period. If you click Yes , the management server automatically takes control of the client system if the grace period times out before you get a response from the client system.

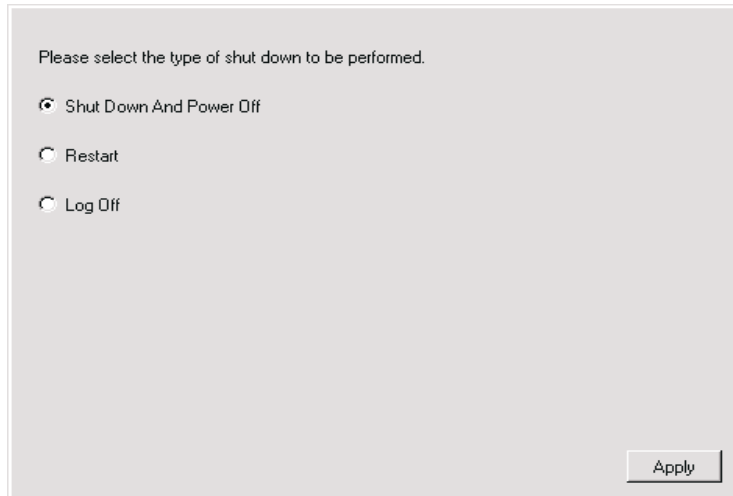
Item	Description
Change state on Target	Click Yes , the client system can take back control from the remote computer.
Desktop optimization	Click Yes , you can disable the background wallpaper of the client system for faster transmission between computers.
Color reduction	For faster transmission between computers, you can compress the display on the client system. This number (16, 256, or Nothing) represents the number of pixels to which the display will be compressed.
Enable compression	Click Yes , the system compresses data for faster transmission between computers, but the user must wait for the compressed data to be decompress after the transfer. If you are having difficulty transferring the data, enable compression.
Refresh rate	A numeric value that represents the delay time between the controlling computer and the client system. The default is 100 milliseconds.

Shutdown

The Shutdown service provides three options for shutting down your system:

- **Shutdown and Power Off** — Shut down and turn off the computer.
Note: Shutdown, and Power Off is available only on systems that support and have enabled Advanced Power Management.
- **Restart** — Shut down and restart your computer without turning it off.
- **Log Off** — Log off your operating system without shutting down the computer.

Click **Tasks** → **Tools** → **Shutdown** from the UM Services task list to display the following interface.



System Updates

Use the **System Updates** option to connect to an IBM Web site that provides updated information for your specific system. This option works only if you have the ability to connect to the Internet.

Click **Tasks** → **Tools** → **System Updates** from the UM Services task list. The System Updates interface opens.

Model	IBM 86391ZY
Serial number	550004T
Operating system	Microsoft Windows NT Server
Version	4.0.1381

When you make a choice below, the above information will be sent to IBM to assist in finding the correct information for your computer system.

Get the Latest Drivers and News about Your System

Get immediate access to the latest device drivers, FAQs, and News about your system. This information will be shown in a new window.

Build a Custom Online Profile with IBM for your System

Now you can be automatically notified when there is new information about your system, including new versions of any device drivers, system software

Check for updates to your Operating System

The following items are available from the System Updates screen.

Item	Description
Table of machine information	The client system model number, serial number, operating system, and version number.
Get the latest drivers and news about your system	Immediate access to the latest device drivers, technical information, and news about the client system.
Build a custom online profile with IBM for your system	Be notified automatically when there is new information about the client system.
OS	The operating system.

5

Upward Integration Modules

This chapter provides information on installing and using Upward Integration Modules (UIMs) on supported system-management platforms.

UIMs enable workgroup- and enterprise-level system-management products to interpret and display data that is provided by client systems running UM Services. The modules provide enhancements on the management server that enable the system administrator to start UM Services from within the system-management platform, collect UM Services inventory data, and view UM Services alerts. UIMs are provided for the following system-management platforms:

- Tivoli Enterprise, including Tivoli Framework 3.6, Tivoli Software Distribution 3.6, and Tivoli Enterprise Console 3.6
- Tivoli NetView 5.1.1 and 6.0 for Windows NT
- CA Unicenter TNG Framework for WIN32 Version 2.2, AIM IT Version 3.0, Asset Management Option 3.0, SHIP IT Version 2.0, Software Distribution Option 2.0
- Intel LANDesk Management Suite 6.3
- Microsoft SMS 1.2; Microsoft SMS 2.0
- HP OpenView Network Node Manager

You can use the UM Services installation program to install the Alert on LAN proxy agent on your system-management platform. The Alert on LAN proxy is not a UM Services UIM, but this proxy agent must be

installed on your system-management platform to receive Alert on LAN messages from Alert on LAN-enabled client systems.

Installing Upward Integration Modules

The method that is used to install an Upward Integration Module depends on the system-management platform for which you are installing support.

- If you are installing the Tivoli Enterprise Plus Module, see “Installing the Tivoli Enterprise Plus Module” on page 89.
- If you are installing Intel LANDesk Management suite integration, see “Intel LANDesk Management Suite Integration” on page 112.
- If you are installing an Upward Integration Module for any other supported system-management platform or are installing the Alert on LAN proxy agent, use the UM Services installation program to install the UIM on the system-management platform. Copy the UM Services installation files to a directory on the system-management system and then go to the same platform-specific section of this chapter for additional installation instructions and usage information.

Systems Management Platform	Additional Information
Tivoli NetView	“Tivoli NetView 5.1.1 and 6.0 Integration” on page 96
CA Unicenter TNG	“CA Unicenter TNG Framework Integration” on page 105
Microsoft SMS	“Microsoft SMS Integration” on page 113
HP OpenView Network Node Manager	“HP OpenView Integration” on page 125

- If you are installing the Intel Alert on LAN proxy on your system-management platform, see “Installing Intel Alert on LAN Proxy” on page 124.

-
- If you are installing UM Services Support on the HP OpenView Server, see page 125

Tivoli Enterprise Plus Module Integration

Tivoli Enterprise is part of Tivoli Management Environment (TME)10. The Tivoli Enterprise UIM adds a module that enables a system administrator using Tivoli Enterprise to manage client systems that have UM Services installed. For example, the system administrator can shut down, restart, and wake up any selected client system that has UM Services installed.

Installing the Tivoli Enterprise Plus Module

Follow these steps to install the Tivoli Enterprise Plus Module:

1. Copy the Tivoli Enterprise Plus Module to a temporary directory on the system that is running Tivoli Enterprise.
You can download the Tivoli Enterprise Plus Module from <http://www.pc.ibm.comwww/software/applications/ums>
2. Select **Download and Support**.
3. From the Select Product drop-down list, highlight UM Services Plus-Tivoli and click **Submit**.
4. Use a file decompression program that supports the TAR file compression format to extract the contents of the file to a temporary directory, for this example, UM Services Plus for Tivoli.
5. Use the Tivoli Desktop to install the Tivoli Enterprise Plus Module.
 - a. From the Tivoli Desktop menu, click **Install** → **Install Product**.
 - b. Select your host and directory. Choose the temporary directory **UM Services Plus for Tivoli**, which contains the Tivoli Enterprise Plus Module files.
 - c. Click **Set Media** → **Close**.

-
- d. Install the Plus Module Support link binaries first, and then install the UM Services Plus module for Tivoli. You must install the Plus Module on the Tivoli Management Region (TMR) and on any other managed nodes from which the Plus Module will be used.

Notes:

- Because of a limitation in Tivoli Enterprise 3.6, the only administrator roles that can install the Plus Module are root (for systems running UNIX) and administrators (for systems running Windows NT).
- When installing the Tivoli Enterprise Plus Module, the administrator must use a fully qualified Tivoli login name (in *name@domain* format).

Enabling Additional Functions

After you install the Tivoli Enterprise Plus Module, use the following information to enable additional functionality.

■ Enabling Wake on LAN® support

To use the Wake on LAN component, you must have a Java Virtual Machine installed on the computer on which the Tivoli Enterprise Plus Module is installed. Also, you must install the Inventory module and collect inventory from the client endpoints, before you attempt a wake up.

■ Enabling Software Distribution support

To enable Software Distribution support, install the Software Distribution Gateway from the Software Distribution CD onto a managed node before installing the UM Services Plus Module so that Tivoli endpoints can be targeted. Additionally, you must install the Software Distribution product on any managed node where the Tivoli Plus Module is installed.

1. Before you can distribute UM Services software, you need a source computer and a source directory that contains the UM Services installation files. This is your staging location for distributing software. You also need a destination drive and location (for example, **C:\temp**) on the target systems where

the installation files will be copied. This destination drive and directory must exist on all client systems before you distribute the software.

Notes:

- The source path of the UM Services FilePack profile designates the root directory as the beginning of the installation. If you have changed or added to the installation file path

/Win32/Install/en

you must edit the correct path in the file **ums_fp_after.bat**.

For example, if you mount the *IBM Director* with UM Services CD on a system running Unix with a mount point of /cdrom, you add the change directory command of

```
CD CDROM
```

before the other change directory commands. The edited section of the batch file will look like this:

```
REM Next line is Unix CDROM mount
```

```
CD CDROM
```

```
CD Win32
```

```
CD Install
```

```
CD en
```

- This destination differs from the final destination for the UM Services software (for example, **C:\program files\ibm\ums**, which must be configured with the **SETUP.ISS** file. For more information on editing the **SETUP.ISS** file, see “Modifying the SETUP.ISS File Manually” on page 117.
2. Before doing any software distribution, run the **Prepare for UM Services Install** service to configure a UM Services file package. Take the following steps:

-
- a. Double-click the icon, **Prepare for UM Services Install**.
 - b. In the **Source Host** field, type the machine name of the system where the installation files are located.
 - c. In the **Source Path** field, type the directory path where the installation files are located.
 - d. In the **Destination Path**, type the directory path of the managed system where the files are to be distributed.
 - e. Click **Set and Close**.
 - f. Right-click the **Install UM Services icon**. In the pop-up menu, click **Distribute**.
3. You can distribute UM Services to any supported Windows operating system (Windows 95, Windows 98, or Windows NT 4.0 or later). A log file (named **umsinst.log**) records the results of the software distribution. The file is located in **%DBDIR%\.\tmp**.

Note: DCOM95 must be installed before you install UM Services on systems running Windows 95. DCOM95 is included with Internet Explorer 4.0 or later and NetScape Navigator 4.5 or later. However, if one of these browsers is not installed on the system on which you are installing UM Services, you must install DCOM95 first.

To install DCOM95 and the Microsoft Virtual Machine (both of which are used by UM Services), run the program named **msjavx86.exe**, included in the UM Services installation files. When this program finishes running, restart the system, delete (or rename) **msjavx86.exe** from the installation directory, and then install UM Services.

If you are distributing UM Services remotely to systems running Windows 95, be sure to distribute and install the **msjavx86.exe** program first. When running **msjavx86.exe** remotely, use the following command:

MSJAVX86 /Q /R:N

Then, restart the client system, delete (or rename) **msjavx86.exe** from the installation directory, and install UM Services.

- Installing the Inventory Gateway product

Install the Inventory Gateway product from the Tivoli Enterprise Inventory CD onto a managed node before you install the Plus Module. The Inventory Gateway product must be installed on a managed node where the Plus Module is installed.

- Enabling distributed monitors

Distributed monitors are not supported on Windows 95 or Windows 98 endpoints. To enable distributed monitors on systems running Windows NT, install the distributed monitor package on a managed node where the Plus Module is installed.

UM Services monitors the UM Services HTTP DAEMON and the SNMP subagent processes.

- Activating Tivoli Enterprise Console (TEC) integration

To activate TEC integration, run the Setup TEC Event Server for the UM Services task on the TEC server.

- TEC events from UM Services Monitors

The UM Services SNMPCheck and HTTPCheck monitors send TEC events when the UM Services SNMP subagent or HTTP DAEMON processes stop. The Events register, with the corresponding TEC indicator, changes its temperature icon depending on the severity of the event. Additionally, the events appear in the TEC console as members of the UM_Services_Plus Event Group.

Note: The default configuration for each monitor is for critical responses only.

To change the default settings in the **Edit Monitor** window, you first must select the critical response level. Otherwise, you will create a new configuration rather than change the existing one.

-
- Automated actions in response to events sent by UM Services Monitors

When the **httpserv.exe** and **snmp.exe** processes stop, the TEC server responds by restarting them automatically.

- Starting UM Services

UM Services provides a Web browser-based console that you can use on any system that supports Netscape 4.5 or later, Internet Explorer 4.01 or later, and Java 1.1.7b or later. This includes UNIX-based Tier 1 nodes. However, because the Tivoli application does not import system-wide environment variables on UNIX platforms, such as CLASSPATH, that are needed by UM Services, you must add the CLASSPATH environment variable to the Tivoli **setup_env.sh** or **setup_env.csh** scripts to enable UM Services startup support. Also, under AIX, the MOZILLA_HOME variable that Netscape uses must be included in the **setup_env.sh** or **setup_env.csh** scripts. After you set these variables, run **setup_env.sh** to enable the startup support for UM Services in the Plus Module.

- Adding Plus Module icons

The Plus Module installation automatically places startup icons in the collection window for every managed node in the TMR that has the Plus Module installed. The launch functionality for a specific managed node works only when you double-click the startup icon for that managed node (for example, Launch UM Services@hostname.)

- Managing large numbers of managed nodes

For TMRs with a large number of managed nodes running the Plus Module, the number of startup icons in the Plus Module collection window can become excessive. You can remove some of these icons from the collection window by clicking an icon to highlight it and choosing **Remove** from the **Edit** menu. Alternatively, you can create a separate collection just for the startup icons by clicking **Create** → **Collection**, and then dragging and dropping the individual icons into the new collection.

Note: In this case, the icons still must be removed from the original view.

- Deploying endpoints with UM Services

Deploying endpoints with a preconfigured gateway helps ensure their successful initial login. You can specify the gateway for a particular endpoint in the silent installation script **tmasetup.iss** that is included in the UM Services installation package. Open the file and scroll to:

```
[SdShowDlgEdit3-0]
```

```
szEdit1=9494
```

```
szEdit2=9494
```

```
szEdit3=-d1
```

```
Result=1
```

The key

```
szEdit1
```

specifies the port through which the gateway communicates. It is 9494 by default. The key

```
szEdit2
```

specifies the port through which the endpoint communicates, also 9494 by default. The key

```
szEdit3
```

specifies any command lines to pass to the install action program. Use this key with the following flags to specify a gateway:

```
szEdit3=-d1 -g gateway host+ gateway listening port
```

Using the Tivoli Enterprise Plus Module

You can use Tivoli Enterprise Plus Module to perform the following additional system-management tasks from the system where UM Services is installed:

- Configure UM Services for all platforms
- Conduct UM Services queries
- Obtain UM Services inventory on a client computer

-
- Use the UM Services indicators for monitors

You can also select a remote system and perform any of the following tasks remotely:

- Restart (shut down and restart) a UM Services client system
- Shut down a UM Services client system
- Wake up a UM Services client system

To use the Plus Module to manage client systems, use the following procedure:

1. From the Tivoli Management Framework window, double-click the Plus Module icon (in the upper-right corner of the window). The **Plus Module** window opens.

Note: The items that appear on the **Plus Module** window depend on what you have installed on the computer that you are managing.

2. To be able to restart, shut down, or wake up a client computer, you must first select the client computer from a list of subscribers. Click the **UMS Subscribers** icon on the **Plus Module** window.

Tivoli NetView 5.1.1 and 6.0 Integration

Tivoli NetView can be used to manage clients running UM Services. To enable this functionality, you must use the UM Services installation program to install the UM Services NetView Upward Integration Module on the system that is running NetView Server.

Installing the Tivoli NetView Upward Integration Module

To install the Tivoli NetView UIM, use the following procedure:

1. Establish an appropriate remote access policy.

The NetView system administrator must have access privileges on every remote client system so that UM Services inventory data can be obtained for each client system. The easiest way to do this is to create a Windows NT domain in which every client is a member. The system administrator should be a member of the Domain

Admins group. This enables the system administrator to access all the computers in the domain (and any trusted domains) without requiring further authentication.

2. Install UM Services on the client computers.

You must install the Web Based Access component on UM Services client computers to classify client systems as UM Services-capable. It is important to do this before installing the NetView UIM on the NetView server. For more information on installing UM Services on client systems, see “Chapter 2. Preparing to Install UM Services,” on page 5.

3. Use **dcomcnfg.exe** to enable DCOM connections on client systems running Windows 95 and Windows 98.

You can download **dcomcnfg.exe** from

<http://www.microsoft.com/com/tech/DCOM.asp>

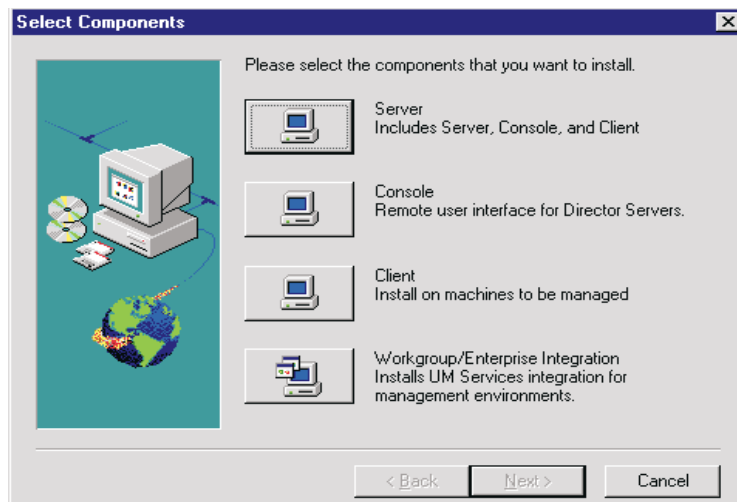
Ensure that **CONNECT** level authentication and **IMPERSONATE** level impersonation are selected.

4. Stop the NetView server. Click **Programs**→**NetView**→**Administrator**→**Stop Server**.
5. Start the UM Services installation program on the NetView server, insert the Director with UM Server Extensions CD. The Director window opens.
6. Click **Install Director**.
7. Click **Next**.

The **License Agreement** window opens. Click **Accept** to proceed.

Note: You must agree to the terms of the License Agreement to install UM Services. If you click **Decline**, the installation program will close.

The Select Components window opens.



8. From the **Setup Options** window, click the **Workgroup/Enterprise Integration — Installs UM Services integration for management environments** button.
The Intergration Selection window opens.
9. Click **Tivoli NetView Upward Integration**, and then click **Next**.
The installation program adds the UM Services SmartSet, loads UM Services MIB files, adds trap filters for UM Services SNMP traps, and adds menu items for starting and inventory collection into the NetView Tools menu.



10. When the installation is finished, restart the server.
The integration setup program configures **nvsniffer.exe** to run after the system is restarted and has populated the UM Services SmartSet.

Starting UM Services on NetView Clients

NetView clients with the UM Services Web Based Access component installed can be targets for starting UM Services. To start UM Services on NetView clients, use the following procedure:

1. Open the UM Services SmartSet and then select a client system.
2. From the **Tools** menu, click **Universal Manageability Services**.

This selection will be disabled and unavailable if the client system you selected does not have the Web Based Access component installed.

UM Services starts on the selected client, using the management system default Web browser. A valid UM Services user ID and password are required to use UM Services to manage a remote client system.

Using Tivoli NetView 5.1.1 and 6.0 to Obtain Inventory Data

NetView clients with the UMSCIM Object capability can be targets for collecting UM Services WBEM-based inventory. Inventory data from UM Services clients can be collected in one of the following ways:

- From the command prompt
 1. Create a new NetView sniffer configuration file.
Open the file **nvsniffer.conf**.
 2. Replace the line, `wbem_discovery.conf` with `ums_wbem.conf`
 3. Save the file as **ums_wbem_discovery.conf**.
 4. While logged into the NetView server host with an account that is a member of the Domain Admins group, run `nvsniffer.exe` interactively from the command prompt:

```
nvsniffer.exe -c
/usr/ov/conf/ums_wbem_discovery.conf
```
- From the NT Schedule service
Use the NT Schedule service to run **nvsniffer.exe**.

By default, NetView configures the Schedule service to run **nvsniffer.exe** daily at 1:00 a.m. However, because UM Services inventory collection relies on a remote DCOM connection to the client computer to access its WBEM repository, you must reconfigure the Schedule service to log in as a user with remote access privileges on the client system.

To reconfigure the NT Schedule service, use the following procedure:

1. Select the **Control Panel** → **Services**.
 2. Select the Schedule service.
 3. Click **Startup** and configure the service to **Log On As a user** to join the Domain Admins group.
- From the NetView Console
1. Open the NetView console.
 2. Open the SmartSets submap.
 3. Open the UM Services SmartSet.
 4. Select a system in the submap for which to collect inventory information.
 5. Open the **Tools** menu and select the **UM Services Inventory** item.

A menu displays the different categories of WBEM-based inventory information that is provided by UM Services on the client system.

6. Click **Demand Poll** to have the data collected from each client in the NetView database.
7. To see the database-logged UM Services inventory data from a particular system, from the command prompt, type:

```
ovobjprint -s <hostname>
```

Note: If the client system that you selected does not have a UMSCIM Object capability (there is no remote access policy to the computer from the NetView server), the UM Services Inventory item will be disabled.

Viewing UM Services SNMP Data from NetView

During the installation of UM Services NetView integration support, trap filters for UM Services SNMP traps are added to the NetView **trapd.conf** file. Thus, when an SNMP trap is sent from a UM Services client system, it can be viewed in the NetView Event Browser. Only traps of critical severity are filtered, and the default action is to change the icon color of the source computer from green to red. Traps indicate an abnormal environment condition on the UM Services client, such as chassis intrusion, a removed processor, or temperature out of range.

To configure the NetView console to display advanced menu items, use the following procedure:

1. Click **Options** → **Advanced** to configure the NetView console to display advanced menu items and query this data.
2. Shut down and reopen the NetView console.
3. Open the UM Services SmartSet and select a system from which to view SNMP data.
4. To start the NetView SNMP browser, open the **Tools** menu and click **MIB** → **Browser**. Ensure that the selected system node name is displayed in the **Node Name** or **Address** field, and click **Get Values**.

Note: To view specific Alert on LAN SNMP traps, you must use the SNMP V2 browser. Click **MIB** → **SNMP V2** → **Browser**.

5. The NetView SNMP collection DAEMON will contact the UM Services SNMP subagent on the client system and query it for the data published in the UM Services MIB files.

Because SNMP support is an optional component of UM Services, and not a required component, not all systems in the UM Services SmartSet will have the UM Services SNMP subagent installed. Those that have the subagent installed will have UMSSnmp Object capability. The **is UMSSnmp** test is not enabled by default in **nvsniffer.conf**, but it can be enabled by opening the **nvsniffer.conf** and removing the comment symbol from the line that begins with **is UMSSnmp**.

Forwarding SNMP Trap Information

UM Services forwards SNMP trap alerts to the NetView administrator for critical IBM system environmental conditions, low disk space, a failing hard disk drive, and a system being removed from a LAN. During the installation of the UM Services upward integration support for NetView, these traps are added to the NetView **trapd.conf** file with their Trap Properties configured using the **addtrap.exe** utility.

UM Services forwards the following SNMP traps to the NetView server workstation:

- iBMPSG_TemperatureEvent
- iBMPSG_VoltageEvent
- iBMPSG_ChassisEvent
- iBMPSG_FanEvent
- iBMPSG_StorageEvent
- iBMPSG_SMARTEvent
- iBMPSG_LANLeashEvent

The following list describes the default properties that are configured for UM Services SNMP traps:

Enterprise: ibm

Trap type: Specific <Last field of NOTIFICATION-TYPE OID>

Trap name: <Label of NOTIFICATION-TYPE>

Display the trap category as:

Status Events

With severity:

Critical

From this source:

Load MIB

Object status for specific traps:

Critical/Down

Event description:

<Event> condition critical

Run this command when the trap is received:

“”

Run as: Hidden Application

The MIB file describing the traps is named **umsevent.mib** and is installed in the

%NV_DRIVE%\USR\OV\SNMP_MIBS

directory. Client systems must have SNMP support installed and the UMSSnmp Object Property before they can forward UM Services SNMP traps.

Additionally, the installation program adds placeholders for the following traps, which will be implemented by UM Services in the future:

- iBMPSG_ProcessorEvent
- iBMPSG_AssetEvent
- iBMPSG_POSTEvent
- iBMPSG_ConfigChangeEvent
- iBMPSG_LeaseExpiration
- iBMPSG_WarrantyExpiration

Note: SNMP on agent must be set to forward traps to the server.

Alert on LAN 2.0 Traps

The Alert on LAN 2.0 networking hardware that is present on certain IBM systems, such as the IBM PC300 PL, also has the ability to send alerts when it detects abnormal environmental conditions or system tampering. These alerts are sent to the AOL 2 Proxy tool that can be installed from the UM Services install program by clicking **Workgroup/Enterprise Integration** and then **AOL Proxy**. (For more information, see “Installing Intel Alert on LAN Proxy” on page 124.)

After the tool is installed, the administrator can configure AOL 2 clients to forward their alerts to the system with the AOL 2 Proxy tool. After the alerts reach the AOL 2 Proxy system, they are converted to SNMP traps and can be forwarded to the NetView Event Browser.

The traps that are forwarded by AOL 2 Proxy are defined in the **aolntrap.mib** and **aolnpet.mib** files. The files are loaded into NetView SNMP MIB loader when the UM Services upward integration support for NetView is installed. Both MIB files describe the same traps except in different formats. Therefore, it is recommended that one of the MIB files should be unloaded. Specifically, **aolntrap.mib** defines traps whose packets are formatted in the traditional way and **aolnpet.mib** defines traps whose packets are formatted in a way that complies with the newer Intel pET standard.

The traps that are defined in both MIB files are added to **trapd.conf**. To view the traps, use the following procedure:

1. From the NetView console, click **Trap Settings**.
2. For **aolntrap.mib** traps, select **Enterprise Intel, ID 1.3.6.1.4.1.343**.
For **aolnpet.mib** traps, select **Enterprise Intel, ID 1.3.6.1.4.1.3183**.
3. Click **Event Details**.

Director Traps

During the installation of the UM Services upward integration support for NetView, a trap filter for IBM Director is added to **trapd.conf**. This filter enables administrators to view SNMP traps that are forwarded from the IBM Director Management Server and that were received from an IBM Director agent. IBM Director supports only one trap type.

To view the details of the trap, including the description, severity, and origin, do the following use the following procedure:

1. From the NetView console, click **Trap Settings**.
2. Select **Enterprise IBM, ID 1.3.6.1.4.1.2.6.146**.
3. Click **Event Details**.

MIB Browsing

By default, the UM Services upward integration support for NetView installation program loads the UM Services MIBs using the

loadmib.exe utility. These MIBs comply with the SMIV1 standard, and therefore the SNMP MIB Browser must be used when browsing UM Services systems. In addition, target systems must be installed with the UM Services SNMP Support installation option. See the "Installing UM Services" on page 13 for more information.

To uninstall, click **Start**→**Programs**→**NetView**→**UM Services**. Run the uninstall program. NetView 5.1.1-6.0 must unload SNMP version 2 mibs.

CA Unicenter TNG Framework Integration

You can use CA Unicenter TNG Framework to manage client computers that have UM Services. The UM Services integration for Unicenter TNG Framework supports the generation of custom MIF files for the AimIT or Asset Management Option repositories. You can also discover IBM client systems running UM Services, start IBM UM Services, and create an IBM UM Services software distribution package for installing on client computers.

Configuring CA Unicenter TNG Framework

To receive SNMP traps from UM Services, you first must configure the SNMP trap server to receive UMS Service alerts (critical only) from IBM computers that have UM Services installed. To activate the SNMP trap service, perform the following steps:

1. Click **Start** → **Programs** → **Unicenter TNG Enterprise Management** (or **Unicenter TNG Framework**). Then click **Enterprise Managers**. A window with a **Windows NT** computer icon opens.
2. Double-click the **Windows NT** icon.
3. Double-click the **Configuration** icon. The **Settings** window opens.
4. Double-click the **Settings** icon. The **Settings** window, with tabs, a table, and a list of items, opens.

-
5. Click the **Component Activation Flag** at the bottom, click the **Client Preferences** tab on the right, and then scroll to the row with **SNMP Trap Server Activated** in the **Description** field.
 6. In the **Settings** column, the value should be **YES**. If it is not, select the **Setting** check box. Click the **YES** option.
 7. Click the **Server Preferences** tab, and scroll to the row with **SNMP Trap Server Activated** in the **Description** column.
 8. In the **Settings** column, the value should be **YES**. If it is not, select the **Setting** check box. Click the **YES** option.
 9. Set the Windows NT SNMP Trap service to Manual by using the following procedure:
 - a. Click **Start** → **Settings** → **Control Panel**.
 - b. Double-click **Services**.
 - c. Double-click **SNMP Trap Service**.
 - d. Set the startup type to **Manual**.
 10. Start all CA Unicenter TNG Enterprise Management services. Open a command prompt window, and type:
`UNICNTRL START ALL`
 11. Close any Unicenter TNG Framework applications that are running.
 12. If you have not restarted the computer since the CA Unicenter TNG Framework was installed, do so now.

Installing the CA Unicenter TNG Framework Upward Integration Module

To install the CA Unicenter Upward Integration Module, use the following procedure:

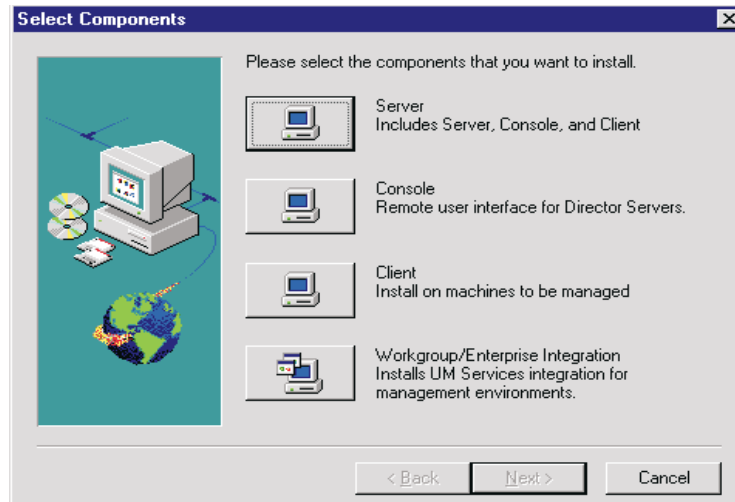
1. Start the UM Services installation program on the CA Unicenter server.
The **Director** window opens.
2. Click **Install Director**.
The **Welcome** window opens.

3. Click **Next**.

The **License Agreement** window opens. Click **Accept** to proceed.

Note: You must agree to the terms of the license agreement to install UM Services. If you click **Decline**, the installation program will close.

The Select Component window opens.



4. From the **Setup Options** window, click the **Workgroup/Enterprise Integration — Installs UM Services integration for management environments** button.

The Integration Selection window opens.

5. Click **CA Unicenter Upward Integration**, and then click **Next**.

The installation program adds the UM Services UIM for CA Unicenter to the Unicenter server. A command window opens.

6. Click **Next**. A **Unicenter TNG Framework** window opens, prompting you to select a repository. Use the down-arrow or the **Find** button to locate a repository, and then click **OK**. You are prompted for a user ID and a password. If a Unicenter TNG Framework session has been initiated before you installed UIM, use that logon procedure.

-
7. A notification is displayed and informs you that the installation is complete. Click **OK** to close this notification window.
 8. You must restart the system to activate the CA Unicenter TNG Framework UIM. A window opens and prompts you to restart the system. Click **Yes** to restart the system immediately, or click **No** to restart your system later and click **Finish**.

Reclassifying Existing Devices

After installation, the Unicenter TNG Framework discovery process runs automatically and identifies IBM systems running UM Services, reclassifying them in Unicenter TNG Framework. However, there can be many existing computers that need to be reclassified. To reclassify existing devices, use the following procedure:

1. Run the Reclassify utility by clicking **Start** → **Programs** → **IBM Integration with Unicenter TNG** → **Reclassify Systems in Unicenter TNG**.

A Unicenter TNG Framework window opens, prompting you to select a repository.

2. Select the repository that you defined during setup. Click **OK** to start the Reclassify utility. A command prompt window opens and displays a message showing that it is finding existing computers running Windows 95, Windows 98, or Windows NT that might have UM Services installed on them.

The process reclassifies existing objects into UM Services objects. These computers can receive UM Services inventory requests and can send SNMP traps.

If there are many systems to reclassify, the reclassification process can take several minutes to complete. When the reclassification process is finished, the command prompt window closes. You should have to run the **Reclassify** utility only once.

Using CA Unicenter TNG Framework UIM

You can use the CA Unicenter TNG Framework UIM to do any of the following tasks:

-
- Launch UM Services from the CA Unicenter TNG Framework 2D or 3D Map
 - View UM Services inventory from the 2D Map
 - Use AimIT to obtain inventory data from client systems
 - View SNMP alerts sent by UM Services clients
 - Use ShipIT to create a UM Services software package

Launching UM Services with CA Unicenter TNG Framework UIM

To launch UM Services from the CA Unicenter 2D or 3D map, use the following procedure:

1. Click **Start** → **Programs** → **Unicenter TNG Framework** → **2D Map** (or **3D Map**). Select the repository that is defined in setup. The Unicenter TNG Framework Map opens with the **Managed Objects** window opened.
2. In the **Managed Objects** window, double-click the **UM_Services** icon. The **Computers** window opens.
3. Right-click the computer of your choice, and then select **UM Services** from the menu. The UM Services console opens.

Viewing UM Services Inventory from the 2D Map

When AimIT is integrated with CA Unicenter, it enables you to obtain inventory information on CA Unicenter clients. To use AimIT from the 2D Map to view inventory data on UM Services client inventory data, use the following procedure:

1. From the **Managed Objects** window, double-click the **UM Services** icon.
2. Double-click the client system for which you want information.
3. Right-click the **Inventory** icon, and then click **View** from the menu to open the **AimIT Domain** window.
4. Click the **Additional** bar at the bottom of the window. An additional inventory list window opens.

-
5. Click **UM Services Inventory**, and then select any inventory option. The inventory information appears on the right side of the window.

Using AimIT to View Inventory

AimIT can be used to view inventory. To start AimIT, use the following procedure:

1. Click **Start** → **Programs** → **AimIt Workgroup Edition** → **Admin Console**. After you type the CA Unicenter password, the **AimIT Domain** window opens.
2. Double-click **Domain**. A window that contains a list of available domains and computers opens.
3. Click the **Computer** icon, and then double-click a single computer for which you want to display the inventory. The inventory for the selected computer is displayed.
4. Scroll to the **Inventory** icon in the list, and click it to display primary inventory.
5. Click the **Inventory Browser** icon in the toolbar. The **Inventory** window opens.
6. Click the **Additional** bar at the bottom of the window to open the window that displays the complete inventory list. You can view the inventory of UM Services by selecting an item under this category in the inventory directory.

Viewing UM Services SNMP Alerts

When an SNMP alert occurs, a banner scrolls at the top of the window to notify you of the alert. To view all UM Services SNMP Alerts that have been received by the CA Unicenter Framework, use the following procedure:

1. Click **Start** → **Programs** → **Unicenter TNG Enterprise Management** (or **Unicenter TNG Framework**). Then click **Enterprise Managers** to open a window with a **Windows NT** icon.
2. Double-click the **Windows NT** icon. A window with three options, **Calendar**, **Configuration**, and **Event**, opens.

-
3. Double-click the **Event** icon. A window with three options, Console Logs, Messages, and Messages Action, opens.
 4. Double-click the **Console Logs** icon.

The **Console Log** window opens. The top of the window shows held messages. Held messages are deleted from the **Console Log** window after you reply to them.

Using ShipIT to Create a UM Services Software Package

You can use ShipIT to create a UM Services installation package, which can then be used to install UM Services onto CA Unicenter TNG Framework client systems.

Note: DCOM95 must be installed before you install UM Services on systems running Windows 95. DCOM95 is included with Internet Explorer 4.0 or later and NetScape Navigator 4.5 or later. However, if one of these browsers is not installed on the system on which you are installing UM Services, you must install DCOM95 first.

To install DCOM95 and the Microsoft Virtual Machine (both of which are used by UM Services), run the program named **msjavx86.exe**, included in the UM Services installation files. When this program finishes running, restart the system, delete (or rename) **msjavx86.exe** from your installation directory, and then install UM Services.

If you are distributing UM Services remotely to the system running Windows 95, be sure to distribute and install the **msjavx86.exe** program first. When running **msjavx86.exe** remotely, use the following command:

```
MSJAVX86 /Q /R:N
```

Then, restart the client system, delete (or rename) **msjavx86.exe** from the installation directory, and install UM Services.

To create and distribute an installation package, use the following procedure:

-
1. Set up a software package to distribute UM Services from the server to client computers by manually *copying* all of the UM Services installation files into the directory **c:\TNGFW\IBMSW_Distribution**
 2. Manually run **rr_swdistrib.bat**, to set up the UM Services package into ShipIT Enterprise ED, WkgrpEd, or Software Delivery Option (SDO), so that you can install it onto remote client systems.
 3. To use this ShipIT software, click **Start → Programs → ShipIt → SD Explorer**.
 4. Using SDO, drag and drop the package onto the client systems.

Uninstalling the CA Unicenter TNG Framework Upward Integration Module

To remove the UM Services UIM from the Unicenter TNG Framework server, click **Start → Programs → IBM Integration with Unicenter TNG → IBM Integration with Unicenter TNG → Uninstall IBM Integration with Unicenter TNG**. After the uninstallation program finishes uninstalling the UIM, remove the modifications made to **umclient.bat**.

Intel LANDesk Management Suite Integration

Unlike other UM Services Upward Integration Modules, LANDesk Management Suite integration requires that an additional component be installed on each UM Services client system. When installing UM Services on your client systems, be sure to select the LANDesk Management Suite Integration component from the **Select Components** window.

Important: Do *not* select Web Based Remote Control when installing UM Services on client systems that you will manage using LANDesk Management Suite. LANDesk Management Suite includes a remote control service that is not compatible with the Web Based Remote Control service that is included with UM Services.

For more information, see “Supported System-Management Environments” on page 6 and “Installing UM Services” on page 13

Note: You can install UM Services on client system with the LANDesk integration option enabled, even if you have not yet installed LANDesk Management Suite on your network.

You do not need to install additional software to your LANDesk Management Suite administration system to manage UM Services clients that have the LANDesk Management Suite component installed. To integrate UM Services clients into your LANDesk Management Suite environment, configure the batch file **ldinv.bat** to run periodically on each UM Services client. **ldinv.bat** generates custom MIF files that can be used by the LANDesk Management Suite inventory functions. Be sure to run **ldinv.bat** before **ldiscn32.exe** inventory collection. One method that you can use to accomplish this task is described in the following procedure:

1. From a login script, run **ldinv.bat**, and then run **ldiscn32.exe**.
2. Create a login script that connects the system to the \LDLOGON share of the LDMS server.
3. Copy the contents of the `%UMS_HOME%\inventory\ldinv.bat` file into the script.
4. Remove the comment symbols from the command line for **ldiscn32.exe** that is included in the batch file and configure it with the name of the inventory server and its network address and any other desired settings. With this line active, whenever a user logs in, the login script generates an MIF file, outputs it to `c:\dmi\dos\mifs` (by default), and trigger an inventory scan that will update the LDMS inventory database.
5. Use the LANDesk scheduler to run **ldinv.bat** on each client at a predefined time.
6. Run **ldinv.bat** from the **Startup** folder of each client system. Ensure that **ldiscn32.exe** runs from **ldinv.bat** and that no other copies of **ldiscn32.exe** are run from the **Startup** folder.

Microsoft SMS Integration

Microsoft SMS can be used to manage client systems running UM Services. To enable it, use the UM Services installation program to

install the UM Services Microsoft SMS Upward Integration Module on the Microsoft SMS server.

Notes:

- After you have installed the Microsoft SMS UIM on the Microsoft SMS 1.2 or Microsoft SMS 2.0 Server or Console, you can use the SMS Software Distribution function to distribute UM Services to your SMS 1.2 or 2.0 client systems. A special installation program designed to facilitate this process, named **umsw32un.exe**, can be downloaded from the Web at

<http://www.pc.ibm.com/ww/software/applications/ums>

- DCOM95 must be installed before you install UM Services on systems running Windows 95. DCOM95 is included with Internet Explorer 4.0 or later and NetScape Navigator 4.5 or later. However, if one of these browsers is not installed on the system on which you are installing UM Services, you must install DCOM95 first.

To install DCOM95 and the Microsoft Virtual Machine (both of which are used by UM Services), run the program named **msjavx86.exe**, included in the UM Services installation files. When this program finishes running, restart the system, delete (or rename) **msjavx86.exe** from your installation directory, and then install UM Services.

If you are distributing UM Services remotely to systems running Windows 95, be sure to distribute and install the **msjavx86.exe** program first. When running **msjavx86.exe** remotely, use the following command:

```
MSJAVX86 /Q /R:N
```

Then, restart the client system, delete (or rename) **msjavx86.exe** from the installation directory, and install UM Services.

Installing the Microsoft SMS Upward Integration Module

Installing UIM on the SMS 1.2 server adds a resource file (**ibmsmsresdll**) and bitmaps for IBM features, and provides an **.atd** file that is used by **smsaddin.exe** to add features to the **Tools** menu of the SMS console.

During installation of the UIM on the SMS 2.0 server, the SMS console is configured with the queries, collections, and tools specific to UMS. Also, the installation provides a Microsoft Management Console (MMC) snap-in module that adds a context to the client systems. The UM Services specific menu items appear only on systems that have UM Services installed.

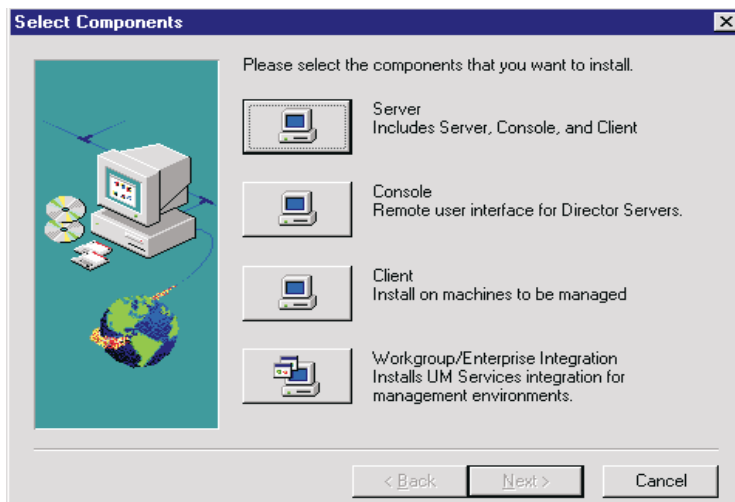
1. Start the UM Services installation program on the Microsoft SMS Console or Server.
2. Insert the Director with UM Server Extensions CD into the CD-ROM
The Director with UM Server Extensions window opens.
3. Click **Next**.

The **License Agreement** window opens. Click **Accept** to proceed.

Note: You must agree to the terms of the License Agreement to install UM Services. If you click **Decline**, the installation program will close.

The Select Components window opens.

4. From the Select Components window, click **Workgroup/Enterprise Integration — Installs UM Services integration for management environments**.
The Integration Selection window opens.
5. Click **Microsoft SMS Upward Integration** and then click **Next**.



6. Select the version of Microsoft SMS for which you are installing support, and then click **Next**. The installation program adds the UM Services UIM to your Microsoft SMS system.

Customizing the SMS Installation

Use the following procedure to modify the UM Services installation routine and to create a new UM Services installation executable file. This procedure requires a compatible compression utility program, such as WinZip, to decompress the original file and to create a new executable file with preset command-line instructions.

Note: To customize the UM Services installation file (**UMSW32UN.EXE**) properly, the compression utility must meet the following basic requirements:

- Has the ability to extract files into a temporary directory
- Enables the user to edit and delete compressed files
- Contains a self-extracting process that creates a user defined installation executable file, with the ability to set up specific startup commands

To create a new UM Services installation file, use the following procedure:

1. Use Windows Explorer to locate the file **UMSW32UN.EXE**.
 2. Using the compatible compression utility program, extract the component files of **UMSW32UN.EXE** into a temporary directory.
 3. Edit the extracted file, **SETUP.ISS**, to select the installation components to install for your particular configuration.
See “Modifying the SETUP.ISS File Manually” for more information.
 4. To reduce the size of the new package, delete **Tivoli.z** or **Netfin.z** from the temporary directory if they are not required for downloads.
 5. Select all the extracted files, including **SETUP.ISS**, and create a new compressed file with the file name **UMSW32UN**.
 6. Open your self-extracting executable file program using the compressed **UMSW32UN** file.
 7. Label the new file **UMSW32UN.EXE**.
 8. In the **Command To Issue** field (after the self-extraction operation is completed), type

```
en/um_setup.exe REBOOT-S-SMS
```

Note: To have the client system restart after installation type

```
en/um_setup.exe REBOOT-S-SMS
```
 9. In the **Wait For** field, type

```
_ISDEL
```
 10. Click **OK** to save the new file.
- A customized UM Services installation executable file is created.

Modifying the SETUP.ISS File Manually

This section describes the contents of the UM Services response file, **SETUP.ISS**, which can be used for the silent installation of UM Services on client systems. You can use this response file for software distribution from the Upward Integration Module environments and other silent installation scenarios.

Note: You must install the UIM before using this process.

The response file is a text file that includes a number of variables that specify installation selections, such as which components are installed or the drive and directory to which the program files will be copied, that would ordinarily be selected during an attended installation. Some portions of the response file must not be changed by the user; making changes to these sections will cause the installation program to fail. All portions of the **SETUP.ISS** file, including sections that the user should not change, are described in the following pages.

This first four sections of the **SETUP.ISS** response file provide information about the installation process to the installation program. These entries must not be changed by the user:

```
[InstallShield Silent]
```

```
Version=v3.00.000
```

```
File=Response File
```

```
[Application]
```

```
Name=UMS
```

```
Version=2.2
```

```
Company=IBM
```

```
[DlgOrder]
```

```
Dlg1=SdAskOptions-0
```

```
Dlg2=AskDestPath-0
```

```
Dlg3=AskSecurInfo-0
```

```
Count=3
```

```
[SdOptionsButtons-0]
```

```
Result=103
```

```
[SdOptionsButtons-1]
```

```
Result = 101
```

The next section of the **SETUP.ISS** response file *can* be customized by the user. This section determines the UM Services components that will be installed on the client system.

To change these options, change the value of Component-count to the total number of components that you want to install, and list the components in sequential order, starting at Component-0.

UMS detected on system. Would you like to upgrade? Yes or No.

1=Yes

0=No

[UpgradeYesNo]

Result=1

The following is the list of components that you can install. If your **SETUP.ISS** file contains all of these examples as shown, all selectable UM Services components will be installed on the client system. Include only the components that you want to install. X is the total number of components to be installed.

Component-x=0 Director Support

Component-x=1 Web Based Access

Component-x=2 System Health & Monitoring

Component-x=3 Web Based Remote Control

Component-x=4 LANDesk (TM) Management Suite Integration

Component-x=5 Tivoli Management Agent

Component-x=6 SNMP access and trap forwarding

Component-x=7 DMI Support

Component-x=8 Help Files

Add components below if desired. Recommended defaults are already set below:

[SdAskOptions-0}

Component-type=string

Component-count=4

Component-0=1

Component-1=2

Component-2=6

```
Component-3=8
```

```
Result=1
```

The next section of the response file displays the path where you want to install UM Services. The default path is shown. You can change the installation path if necessary.

```
[AskDestPath-0]
```

```
szPath="C:\Program Files\IBM\UMS"
```

```
Result=1
```

The next section of the response file configures the security information. In this section of the file, type your user ID and password; both items are case-sensitive. Type your password again in the `svConfirm` line. You can also use this section to specify the TCPIP port number that will be used by UM Services.

```
[AskSecurInfo-0]
```

```
svUser=ums
```

```
svPassword=ums
```

```
svConfirm=ums
```

```
svPort=411
```

```
Result=1
```

The default port number is 411. You can change this default port if necessary. Other valid port numbers are 6411, 6500, 6600, and 6611.

The last two sections of the **SETUP.ISS** response file provide information about the installation process to the installation program. These entries must not be changed by the user.

```
DMI machine type
```

```
Options:1=Desktop
```

```
          2=Mobile
```

```
          3=Server
```

```
[DMI]
```

```
DMIType=1
```

```
Do you want icons on the start menu?
```

```
[icons]
```

```
Result=0
If you installed Director support, would you like Director
Remote Control?
[NFDRemote]
Result=1
Do you want to require authorization for Director remote
Control?
[NfDreqAuth]
Result=1
AutoReboot machine when install is finished?
[AutoReboot]
Result=0
Terminal services installation question.
Setup could not detect if system is in install mode. Are
you sure the system is in install mode?
Continue with install.
        1=YES
        0=NO
[TerminalServices]
Result=0
Use IIS as web server for UMS?
Setup detected IIS installation. Do you want to use IIS as
web server for UMS?
        1=YES
        0=NO
[Use IIS]
Result=0
```

Uninstalling the Microsoft SMS Upward Integration Module

To remove UM Services from a SMS 1.2 server, use the following procedure:

-
1. Delete the files from the `%UMS_HOME%` directory and remove the directory.
 2. Remove the environment variable `UMS_HOME`
 3. Remove the Registry key
`HKEY_LOCAL_MACHINE\SOFTWARE\IBM\UMS`
 4. Remove the Registry
key `HKEY_CURRENT_USER\Software\Microsoft\SMS\Applications\IBM - PCCo`

To remove UM Services from a SMS 2.0 Server or Console, use the following procedure:

1. Run `REGSVR32 - U UMSCONS.DLL`
2. Run `REGSVR32 - U UMSSMSE1.DLL`
3. Run `REGSVR32 - U UMSSMSE2.DLL`
4. Run `UMSCOLL . \UMSCOLL.INI YourSMSSiteServer -D`
where *YOURSMSSiteServer* is the name of the SMS server.
5. Delete the files from the `%UMS_HOME%` directory and remove the directory.
6. Remove the environment variable `UMS_HOME`
7. Remove the Registry key `HKLM\SOFTWARE\IBM\UMS`

Using Microsoft SMS to View Client Computer Inventory

You can use Microsoft SMS 1.2 or 2.0 to view UM Services client inventory data.

Microsoft SMS 1.2

To view UM Services inventory data or start the UM Services console from the Microsoft SMS 1.2 Console, use the following procedure:

- Start the SMS Console, and then double-click a client system to open the **Personal Computer Properties** window.

-
- Start the SMS Console, and then click **Issue Wake on Lan Request** → **UM Services Help** → **UM Services Management Tools** → **Update UM Services Client Inventory**.

SMS 1.2 UIM uses a static MIF file to provide inventory data to the SMS server. An MIF file is created for each inventory query file in the UM Services inventory directory. To refresh the client inventory data, select **Update Client Inventory** from the **SMS Tools** menu for the currently selected client system.

The Microsoft SMS 1.2 UIM also enables the SMS server to receive UM Services alerts (such as System Health messages) as SNMP traps.

Microsoft SMS 2.0

The Microsoft SMS 2.0 UIM enables the SMS server to gather inventory data directly from the CIM agent on client systems running Windows 95, Windows 98, or Windows NT clients. It also enables SMS to gather inventory data using the static MIF file method used by Microsoft SMS 1.2.

The Microsoft SMS 2.0 UIM extends the SMS 2.0 **Collections** tree in the SMS 2.0 console to include UM Services clients. The SMS 2.0 UIM also extends the **Queries** tree, so that it can retrieve UM Services-specific inventory data. The **Tools** tree is extended as well, so that you can start the UM Services console on a client system.

SMS 2.0 does not support SNMP trap listening. However, the Microsoft SMS 2.0 UIM translates CIM notifications that are generated by UM Services into SMS 2.0 status messages.

To view the UM Services inventory data from the SMS 2.0 Console, click the **Collections** tree, and then use following procedure:

1. Click **All Systems with UM Services Agent**
2. Right-click a client system in the window on the right side.
3. Click **All Tasks** → **Start Resource Explorer**.
4. Click the **Hardware** node. The UM Services inventory data is under **IBM UM Services**.

Installing Intel Alert on LAN Proxy

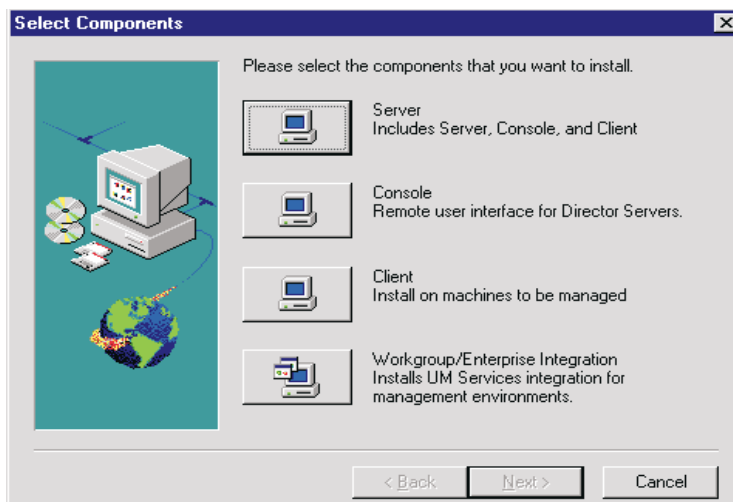
To install the Intel Alert on LAN Proxy on your system-management system, use the following procedure:

1. Start the UM Services installation program on the system-management system that will receive Alert on LAN messages.
2. Insert the Director with UM Server Extensions CD in the CD-ROM
The Director with UM Server Extensions window opens.
3. Click **Install Director**.
4. Click **Next**.

The **License Agreement** window opens. Click **Accept** to proceed.

Note: You must agree to the terms of the License Agreement to install UM Services. If you click **Decline**, the installation program closes.

The Select Components window opens.



5. From the Select Components window, click the **Workgroup/Enterprise Integration — Installs UM Services integration for management environments** button.

The Integration Selection window opens.

6. Click **Intel Alert on LAN Proxy** and then click **Next**.
7. Select a TCPIP port for use by the Alert on LAN Proxy. Then, click **Next** to finish the installation process.

HP OpenView Integration Module

UM Services provides the following integration with HP OpenView Network Node Manager:

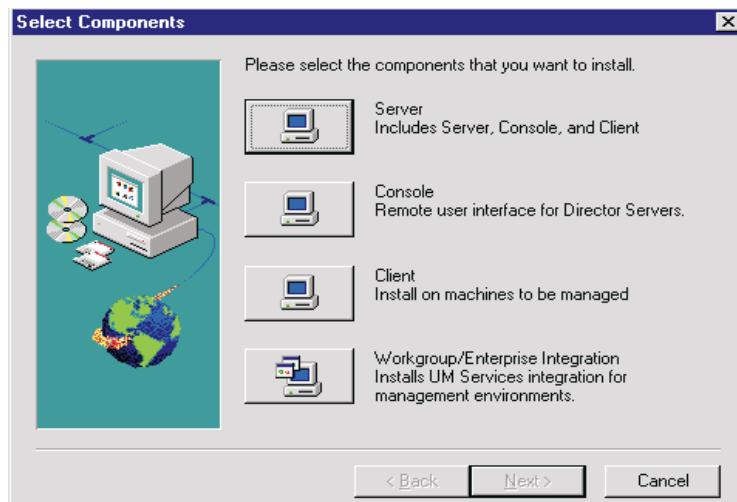
- Visibility of UM Services Inventory data from the OpenView Console
- Availability of a current UM_Services submap
- Accessibility of UM Services from the OpenView Console

Installing UM Services Support on the OpenView Server

From the **Enterprise** option, the installation program automatically installs the files necessary for UM Services installation for OpenView.

1. Insert the Director with UM Server Extensions CD into the CD-ROM.
The Director with UM Server Extensions window opens.
2. Click **Install Director**.
The Welcome window opens.
3. Click **Add New Program** → **UM Services**.
4. Click **Next**.
The License Agreement window opens. Click **Accept** to proceed. You must agree to the terms of the License Agreement to install UM Services. If you click **Decline**, the installation program will close.

The Select Components window opens.



5. From the Select Components window, click the **Workgroup/Enterprise Integration** to install UM Services integration for management environments. The Integration Selection window opens.
6. Click **HP Openview Integration** and then click **Next**. The installation program installs the files necessary for UM Services for HP OpenView.

The following events are associated with UM Services installation to Openview:

1. Install `\openview\snmp_mibs*.mib` (SNMP MID files for UM Services client systems).
2. Add lines to `\openview>alerts\umstraps.conf` (configures UM Services events in to HP OpenView)
3. Install `\openview\registration\c\ums*.reg` (adds map files).
4. Install `\openview\registration\c\rrrov_reg` (adds tools menu options)
5. Install `\openview\registratoin\c\umstrap.reg` (loads UM Services events into the event configuration window)
6. Install `\openview\bin*` (adds map support for UM Services)

7. Install `\openview\bitmaps\c\universal_service*` (bitmaps for UM Services icons in OpenView Console)
8. Install `\openview\fields\c\universal_service` (fields for UM Services in OpenView Console)

Accessing UM Services from the OpenView Console

You can access UM Services from the OpenView Server by using either Microsoft Internet Explorer (Version 4.01 or later) or Netscape (Version 4.51 or later).

1. Select a client node in the OpenView Console.
2. Open the **Tools** menu.
3. Click **Universal Manageability Services**.

Viewing UM Services Inventory Data from the OpenView Console

To view UM Services Inventory Data from the HP OpenView Console:

1. Select a client node in the OpenView Console.
2. Open the **Tools** menu.
3. Click an option under **UM Services Inventory**.

Adding UM Services Clients to the UM Services Submap

When the `hpovums.exe` program detects client systems that have UM Services installed.

- UM Services clients become members of the UM Services Submap.
- The **OpenView Console Tools** menu is expanded to include items enabling access Universal Manageability Services inventory options.

Populating the UM Services Submap

The UM Services upward integration module for OpenView defines three attributes that **hpovums.exe** checks before creating UM Services: `isUniversalService`, `isUmServicesCim`, and `LaunchHttpUmServices`.

isUniversalService

An SNMP Get() operation is performed against the Enterprise OID 1.3.6.1.4.1.2.6.159 on a remote system. This OID is owned by IBM UM Services, and a valid return value will add the UM ServicesSnmp Object Capability to the system properties and add the system to the `UM_Services` Submap.

isUMServicesCim

A WMI ConnectServer() call is performed against a remote system **winmgt.exe** process in the **root\cim\2 namespace**. If the user who is invoking the connection has remote access privileges on the system, the UM Services HTTP port is queried, the `UMServicesCim` Object Capability is added to the system properties, and the system is added to the `UM_Services` Submap. The `isUMServicesCim` test requires WMI on the client system (installed automatically by UM Services) and remote access privileges for the OpenView administrator. Note that a system must have the `UMServicesCim` capability to retrieve UM Services-specific inventory information, because Windows Management instrumentation supplies this data.

Launch HttpUM Services

After the client systems with UM Services are found, **hpovums.exe** checks whether each client system supports starting of web-based UM Services by sending an SNMP request on the HTTP port. If a valid HTTP port is returned, this attribute is enabled, if not, this attribute is disabled.

Based on this attribute, **Tools** menu option **Universal Manageability Service**, which is used to start HTTP-based UM Services, is enabled or disabled.

Forwarding UM Services Events

UM Services forwards the following SNMP traps to the OpenView server workstation:

- iBMPSG_TemperatureEvent
- iBMPSG_VoltageEvent
- iBMPSG_ChassisEvent
- iBMPSG_FanEvent
- iBMPSG_StorageEvent
- iBMPSG_SMARTEVENT and
- iBMPSG_LANLeashEvent
- iBMPSGRedundantNetworkAdapterEvent
- iBMPSGRedundantNetworkAdapterSwitchoverEvent
- iBMPSGRedundantNetworkAdapterSwitchbackEvent

These traps alert the OpenView administrator to critical environmental conditions in IBM systems, low disk space, a failing hard disk drive, and a system being removed from a LAN. During the installation of the UM Services upward integration support for OpenView, these traps are added to OpenView **trapd.conf** file with their trap properties configured using the **addtrap.exe** utility. In addition, the installation program adds placeholders for the following traps, which will be implemented by future versions of UM Services:

- iBMPSG_ProcessorEvent
- iBMPSG-AssetEvent
- iBMPSG_POSTEvent
- iBMPSG_ConfigChangeEvent
- iBMPSG_LeaseExpiration
- iBMPSG_WarrantyExpiration

The following list describes the default properties that are configured for UM Services SNMP traps:

- Enterprise: ibm

-
- Trap-Type: Specific <Last field of NOTIFICATION - TYPE OID>
 - Trap Name: <Label of NoTIFICATION - Type>
 - Display the Trap Category as: Status Events
 - With Severity: Critical
 - From this Source: Load MIB
 - Object Status for Specific Traps: Critical/Down
 - Event Description: <Event> condition critical
 - Run this command when the trap is received: " "
 - Run as: Hidden Application

The MIB file describing the traps is named **umsevent.mib** and installed in the **%OV_DRIVE%\openview\snmp_mibs** directory. Client systems must have SNMP support installed before they can forward UM Services SNMP traps.

Alert on Lan 2 Traps

The Alert on LAN 2 networking hardware which is present on certain IBM systems, such as the PC300 PL, also has the ability to send alerts when it detects abnormal environment conditions or system tampering. These alerts are sent to the AOL 2 Proxy tool that can be installed from the UM Services installation program by selecting **Workgroup/Enterprise Integration** and **AOL Proxy**. After the tool is installed, the administrator can configure AOL 2 client systems to forward their alerts to the system with the AOL 2 Proxy tool. After the alerts reach the AOL 2 Proxy system, they are converted to SNMP traps and can be forwarded to OpenView Event Browser.

The traps that are forwarded by AOL 2 Proxy are defined in the **aoltrap.mib** and **aolpet.mib** files, which are loaded into OpenView SNMP MIB loader when the UM Services upward integration support for OpenView is installed. Because the MIB files describe the same traps, just in different formats, one of the MIB files should be unloaded. Specifically, **aolntrap.mib** defines traps whose packets are formatted in the traditional way, and **aoimpet.mib** defines traps whose packets are

formatted in a way that complies with the newer pET standard from Intel.

The traps that are defined in both MIB files are added to **trapd.conf** and can be viewed by opening the Trap Settings dialog and scrolling to **Enterprise intel, ID 1.3.6.1.4.1.343** of the **aintrap.mib** traps and **ID 1.3.6.1.4.1.3183** for the **ainpet.mib** traps.

Director Traps

During the installation of the UM Services upward integration support for OpenView, a trap filter for the IBM Director product is added to **trapd.conf**. This filter enables Administrators to view SNMP traps forwarded from the IBM Director management server on behalf of a IBM Director agent. IBM Director supports only one trap type, so to view the details of the trap, including the description, severity, and origin, select the trap and open its Event Details. The trap settings for the Director_Trap type can be viewed by opening the **Trap Settings** dialog and scrolling to **Enterprise ibm, ID 1.3.6.1.4.1.2.6.146**.

MIB Browsing

By default, the UM Services upward integration support for the HP OpenView Network Node Managed install program loads Management Information Bases (MIBs) using the **loadmib.exe** utility. These MIBs comply with the SMIv1 standard, and therefore, the SNMP MIB Browser must be used when browsing UM Services systems. In addition, target systems must be installed with the UM Services SNMP Support installation option. See Chapter 4 of the UM Services User Guide for more information.

Uninstalling OpenView Integration Support

To Uninstall OpenView integration support, from the HP Openview console click **Start**→**Programs**→**HP OpenView**→**UMServices Integration** and run Uninstall UM Services. You must unload SNMPVS mibs.

Index

A

- activate TEC integration 93
- adding plus module icons 94
- Agent Polling Period 27
- AimIT 109
 - view inventory with 110
- Alert on LAN 53
- Alert on LAN Proxy
 - installing 124
- Asset ID 57
 - Asset tab 62
 - Lease tab 61
 - Personalization tab 63
 - Serialization tab 58
 - System tab 58
 - User tab 60
 - Warranty tab 63
- Asset tab 62

B

- basic services, IBM Director 14
- Basic System service 26
- browsers
 - Internet Explorer 9
 - MMC 9, 10
 - Netscape 9

C

- CA Unicenter TNG
 - 2D or 3D map 109
 - configuring 105
 - installing 106

- integrating 105
- reclassifying 108
- uninstalling 112
- using 108
- Capacity 30
- Color bits/pixel 34
- Common Information Model 1
- component selection suggestions
 - for CA Unicenter 7
 - for LANDesk Management Suite 7
 - for Microsoft SMS 1.2 or 2.0 7
 - for Tivoli Enterprise 6
 - for Tivoli Netview 6
- configuration tasks 53
 - Alert on LAN 53
 - Asset ID 57
 - Date and Time 64
 - Network 65
 - SNMP 72
 - User Security 76

D

- Date and Time task 64
- default directory, installing 10
- distributed monitors 93
- DMI Mapper 17
- DNS Tab 67
- DNS tab 67
- Domain/Workgroup 70
- Drivers page 38
- Drives Service
 - logical drives 28
 - physical drives 29

E

- Event Viewer 42
- Expansion slot 27

H

hardware requirements, UM Services Client 8
Hardware Version 27

I

Information tab 24
installation rules 9
installing UIMs 88
Internet Explorer 9
inventory data with Tivoli NetView 5.1.1 99
Inventory Gateway 93
IP Address tab 66

K

Keyboard 27

L

LANdesk Management Suite
 integrating 112
 integrating UM Services clients 113
LANdesk Management Suite Integration 3, 16
launching UM Services 94
Lease tab 61
Logical Drives tab 28

M

managing many managed nodes 94
Memory service 31
 physical memory 31
 upgrade options 31
Microsoft Management Console 9, 10

Microsoft SMS
 using to view client inventory 122

Microsoft SMS UIM
 installing 115
 integration 113
 uninstalling 121

Monitor services
 Event Viewer 42

Monitor services 42
Multimedia service 33

 Audio tab 33
 Video tab 33

N

Netscape 9
Network
 DNS tab 67
 IP Address tab 66
Network task 65
Notebook service 46
 Battery tab 47
 Enclosure status tab 47

O

Operating System service 34
 Drivers tab 35
 Process tab 35
 Services tab 35

P

Partition 30
Personalization tab 63
Physical Drives 29
Physical Drives tab 29
Pointing Device 27

Ports service 41
Process page 37

R

RAM 34
redirected installation 10
Remote Control 81
 rules for running 81
Resolution 34
rules for installation 9

S

security level, user 76
Serialization tab 58
server files
 basic services 14
Services page 40
ShipIT 111
Shutdown task 83
Simple Network Management Protocol 1
SMS 1, 2
SNMP 1
SNMP access and trap forwarding 3, 16
SNMP alerts
 viewing 110
SNMP data, viewing through NetView 101
SNMP task 72
software distribution support 90
starting the UM Services console
 from a UIM management console 21
 from MMC 20
 on your local system 19
 remotely 20
Storage 27
System Health 49
 LAN Leash 51
 low disk space 51
 processor removed 51

 temperature out of specification 51, 55
 voltage out of specification 51, 56
System Health Monitoring 3, 15
System tab 58
System Updates 84
Systems Management Server 1, 2

T

tasks
 Asset ID
 Asset tab 62
 Lease tab 61
 Personalization tab 63
 Serialization tab 58
 System tab 58
 User tab 60
 Warranty tab 63
 configuration tasks 53
 Network
 DNS tab 67
 IP Address tab 66
 Remote Control task 81
 Shutdown task 83
 System Update 84
Tasks menu 52
tasks menu
 Web Links 84
ThinkPad 1
Tivoli Enterprise Plus Module
 activate TEC integration support 93
 distributed monitors support 93
 enabling added function 90
 installing 89
 integrating 89
 Inventory Gateway support 93
 launching UM Services support 94
 managing many managed nodes 94
 Plus module icon support 94
 software distribution support 90
 using 95

- Wake on LAN support 90
- Tivoli Management Agent 3, 16
- Tivoli NetView 5.1.1
 - installing 96
 - integration 96
 - using to obtain inventory data 99
 - viewing SNMP data 101
- tools
 - Remote Control task 81
 - Shutdown task 83
- Type 30

U

- UIMs
 - CA Unicenter TNG 105
 - Intel Alert on LAN Proxy 124
 - LANDesk Management Suite 112
 - Microsoft SMS 113, 115
 - Tivoli NetView 5.1.1 96
- UM Services
 - installing 5
 - introducing 1
 - using 23
- UM Services Client, supported systems 8
- UM Services components 5, 6
- Upgrade Options 32
- Upward Integration Modules, installing 88
- User Security task 76
- User tab 60

V

- Video Adapter Description 34
- viewing client inventory through Microsoft SMS 122

W

- Wake on LAN support 90
- Warranty tab 63
- Watchdog Timer Period 27
- Web Links 84
 - System Updates 84
- Web-based Access 2, 15
- Web-based Remote Control 3, 16
- Windows User Management 74
- WINS 69



Part Number: CT7UMSG
File Number:

CT7UMSG