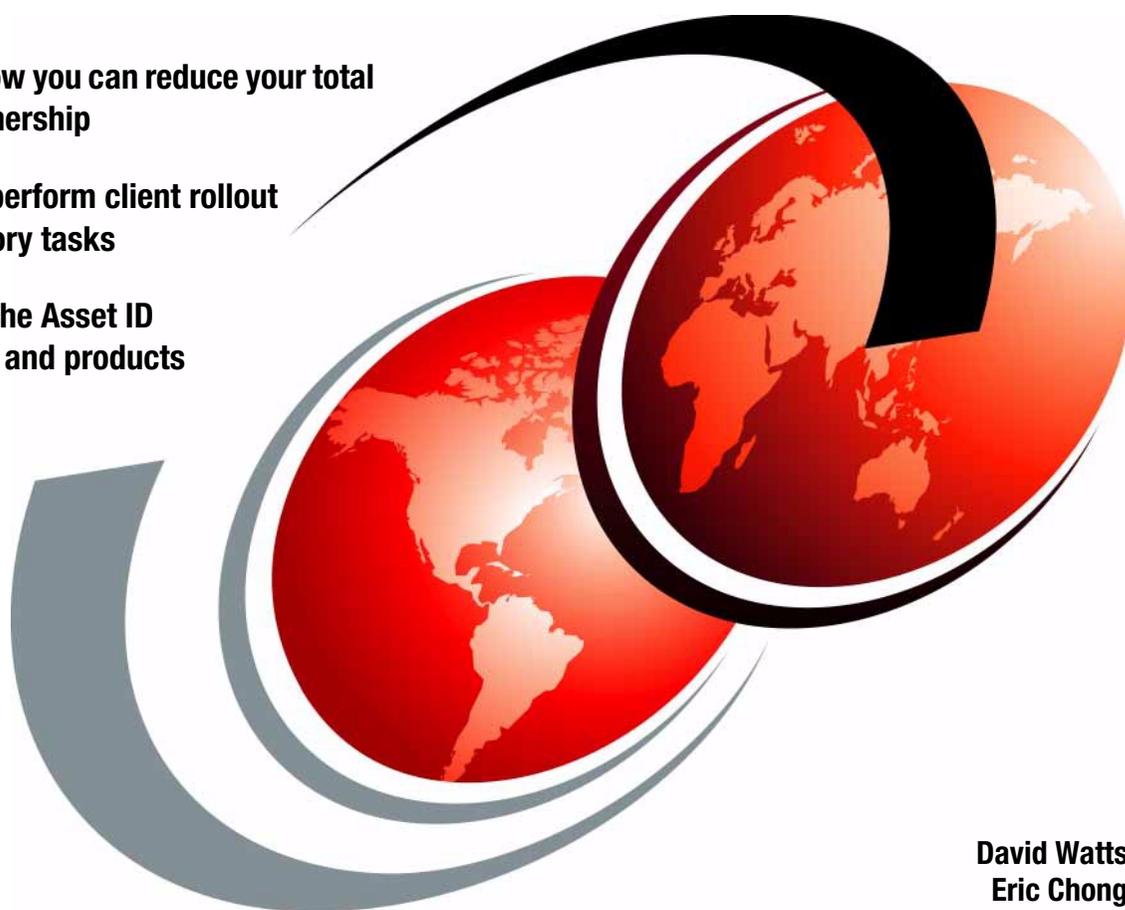# Implementing Asset ID

- Explains how you can reduce your total cost of ownership

- Helps you perform client rollout and inventory tasks
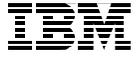
- Describes the Asset ID technology and products

David Watts
Eric Chong

Redbooks

ibm.com/redbooks

IBM International Technical Support Organization

Implementing Asset ID

February 2001

┌─ **Take Note!** ──┐

Before using this information and the product it supports, be sure to read the general information in Appendix A, "Special notices" on page 175.

└───┘

Contents

Preface

Asset ID is a radio-frequency identification technology that lets you read and write PC system data using RF devices such as handheld scanners. It can be considered the next generation of bar codes, but instead of actually having to find and scan the barcode then looking up a database to find the matching information, you simply hold the scanner near the system and all the system information is read in real-time, directly from the system.

Asset ID is available in recent models of the IBM PC 300PL, NetVista, and IntelliStation workstations, plus selected ThinkPad models.

Asset ID aids deployment by recording end-user information and software requirements on individual PCs without having to unpack them from the cardboard box. It also makes inventory reporting easier because you no longer have to open the system unit to determine what components are installed.

This redbook describes how to implement Asset ID. We describe what the components are and how the technology works. We explain how to use Asset TraQ and the Asset ID Starter Kit, two Asset ID solutions from IBM Business Partner QueTel Corporation. We then take a look at how to implement Asset ID with the following management products: LANClient Control Manager (LCCM), Software Delivery Assistant (SDA), Netfinity Director, and the Tivoli FrameWork.

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, Raleigh Center.

David Watts is a Senior IT Specialist at the IBM ITSO Center in Raleigh. He manages residencies and produces redbooks on hardware and software topics related to xSeries systems and associated client platforms. He has authored over 20 redbooks; his most recent books include *Tuning Netfinity Servers for Performance* and *Migrating from Netfinity Manager to Netfinity Director*. He has a Bachelor of Engineering degree from the University of Queensland (Australia) and has worked for IBM for over 11 years. He is an IBM Professional Server Specialist and is an IBM Certified IT Specialist.

Eric Chong is a TCO IT Specialist and PC Institute instructor specializing in systems manageability in Canada. He specializes in promoting and implementing the IBM Personal System Group's lifecycle toolset. He holds a

Bachelor of Business Management degree from Ryerson Polytechnical Institute (now Ryerson University in Toronto, Canada). He is a Microsoft Certified Systems Engineer (MCSE), Chauncey Group Certified Technical Trainer and IBM Professional Server Expert. Six of his ten years of experience in the IT field have been with IBM.
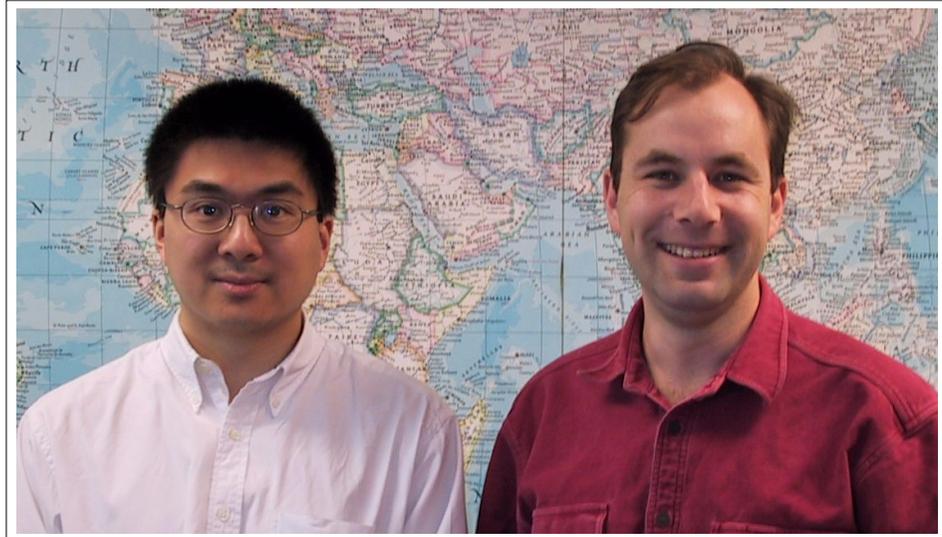
Figure 1. The authors (l-r): Eric and David

A special thanks goes to Steve Miller from QueTel Corporation for his invaluable contribution to this project.

Thanks also to the following IBM employees:

    Sulaiman Abdul-Mateen, NetVista Brand Launch Technician, Raleigh
    Drew Birnbaum, Advanced Technical Support, Gaithersburg, Maryland
    Sarah Brown, TCO IT Specialist, PSG, Markham, Ontario
    Ryan Catherman, Solutions Development - Asset ID Lead, Raleigh
    Ray Cook, Netfinity Director Product Engineering, Raleigh
    Brandon Ellison, Solutions Development and Education, Raleigh
    Brent Hanbury, TCO Manager, PSG, Markham, Ontario
    Kofi Kekessie, LCCM third-level support, Raleigh
    Marc-Andre Laniel, TCO IT Specialist, PSG, Montreal, Quebec
    George Mar, TCO IT Specialist, PSG, Markham, Ontario
    Morten Moeller, Tivoli Specialist, ITSO Austin
    Steve Murphrey, Cross Brand Systems Management, Raleigh
    Gary L Robinson, WW Product Marketing Manager, ThinkPad
    Richard Shryock, ThinkPad Technology Strategist, Raleigh

Michael Steinmetz, Development Engineer, Intellistation, Raleigh
Brian Teague, World Wide Solutions Product Manager, NetVista, Raleigh
Goran Wibran, Program Manager TCO Solutions, Raleigh

Comments welcome

Your comments are important to us!

We want our Redbooks to be as helpful as possible. Please send us your comments about this or other Redbooks in one of the following ways:

- Fax the evaluation form found in "IBM Redbooks review" on page 189 to the fax number shown on the form.

- Use the online evaluation form found at `ibm.com`/redbooks

- Send your comments in an Internet note to redbook@us.ibm.com

x Implementing Asset ID

Chapter 1. Introduction

Asset ID is radio frequency identification (RFID) technology from IBM that makes it easier for you to roll out new PCs and ThinkPads to users, to perform inventory, and to improve the security of your systems.

Recent models of IBM PC 300PL, NetVista, and IntelliStation workstations and ThinkPad notebooks have an electrically erasable programmable read-only memory (EEPROM) chip that can be read from or written to without having to open the system case or even unpack it from its shipping box.

Depending on the system and attached monitor, Asset ID gives you access to the following system information:

- System model and serial number
- CPU serial numbers
- Memory installed and DIMM serial numbers
- Hard disk sizes and serial numbers
- Attached monitor model and serial number

Without any additional hardware, you can do the following:

- Write user data to the EEPROM using tools such as IBM Director and LCCM, then read that data back later for analysis. The data will then be stored in the systems and can also be automatically uploaded to the company-wide asset database.

- Completely automate the rollout of new operating platforms specific to that user or system, using LCCM.

To take advantage of the RFID capabilities, you can add a handheld reader. This reader comprises three parts: a barcode reader from Symbol Technologies, an RF adapter from HID Corporation, and software that runs on the barcode reader and on a Windows PC.

With an RFID handheld reader and application software, you can:

- **Automate rollout of new systems**. You can read the serial number and MAC address of each system and write the name of the user to the EEPROM before the box is unpacked. Once the system is cabled up, you can then configure LCCM to remotely power up the system and install the operating system and user applications.

- **Perform inventory of existing systems, even if they are powered off**. You can read the system information in the EEPROM simply by holding the RFID scanner in front of the system, regardless of whether the

machine is powered on or not. You can then transfer this information into your inventory database for further analysis.

IBM has partnered with a number of hardware and application vendors to provide a complete Asset ID solution. In this redbook, we describe products from:

- Symbol Technologies, makers of a range of programmable handheld barcode scanners.

- HID Corporation, makers of the AMH100 handheld RF reader, which connects to the Symbol scanner.

- QueTel Corporation, makers of Asset ID software Asset TraQ and the Asset ID Starter Kit.

Chapter 2. Components

Asset ID is made up of components both internal to PCs and ThinkPads and external to system units. The Asset ID subsystem includes three components:

- An EEPROM non-volatile memory module, integrated on the system planar.

- A passive antenna, attached inside the system unit.

- A radio frequency (RF) reader, an external device. One implementation, as shown in Figure 2, uses the combination of a handheld programmable barcode scanner (known as a portable data terminal or PDT) and an RF reader. There are generally three types of reader: handheld, portal, and panel.

The EEPROM and antenna are collectively called the *tag*.
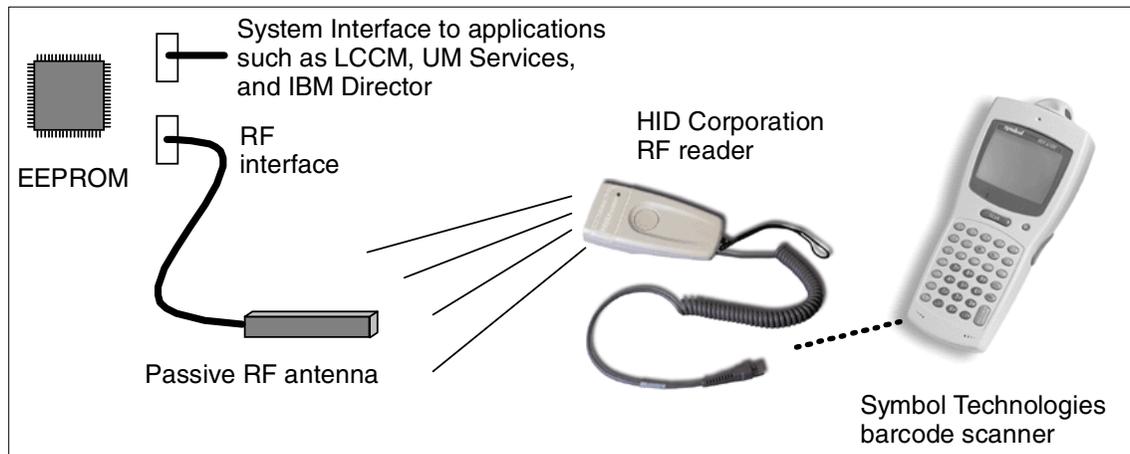
Figure 2. Asset ID EEPROM and passive antenna

Typically, the system interface of the EEPROM will be connected to a bus within the asset to allow access to the data from the system. Since the tag is integrated into the asset, this tag is called an *integrated tag*. If the tag has no system bus interface to the EEPROM, the tag is called a *non-integrated tag* and is also known as a *legacy tag*. These non-integrated tags are typically used to provide the RF capability for existing assets. All Asset ID implementations in IBM systems use integrated tags.

3

2.1 The Asset ID EEPROM

The Asset ID EEPROM is a non-volatile memory space. Information stored there remains intact even after a system power failure.

It can be read from and written to using either of two interfaces:

- The system bus interface is used by the system BIOS and application software running on the system to store and retrieve asset information on the EEPROM. LCCM, IBM Director and UM Services are three examples of an application that writes to the Asset ID EEPROM through the system bus interface. LCCM is discussed in 4.1, "LANClient Control Manager" on page 50.

- The RF interface connects to the antenna where the asset information can be read and written by an RF reader.

When the system is switched on, the EEPROM draws its power from the system power supply. When the system is not switched on, the EEPROM draws its power from the RF field generated by the RF reader. This allows you to access the tag even when the system is not connected to a power outlet, such as inside a shipping carton.

The EEPROM holds 1 KB of data broken up into three areas as listed in Table 1. The only area that the RF interface has write access to is the user area.

Table 1. EEPROM contents

Area	Size	Access via the RF interface	Access via the system interface
Serial	248 bytes	Read	Read/Write
User	248 bytes	Read/Write	Read/Write
Configuration	248 bytes	Read	Read/Write

2.1.1 Serial area

The serial area holds all the serial numbers of the system. This area can be written and read through the system interface but can only be read by the RF interface.

Serial numbers stored in this area are:

- System model and serial number
- CPUs
- Memory DIMMs

- CD-ROMs
- Power supplies
- Disk drives
- Diskette drive
- System planar
- Monitor model and serial number on supported monitors and systems

2.1.2 Configuration area

The configuration area contains details about the basic system configuration. It is updated automatically by the system BIOS during the initial power-on sequence when it detects a new component. The BIOS will compare the system state with the configuration area and make corrections if differences exist (for example, a new memory DIMM or CPU is added).

Data stored in this area is:

- System UUID
- MAC address of the integrated network controller
- CPU type and speed
- Memory: Number and sizes of installed DIMMs
- IDE devices: type and size
- PCI devices: location, vendor and device IDs, class and subclass
- Display size and resolution (ThinkPad LCD only)

2.1.3 User area

The user area consists mostly of personal data. This area is the only one that can be updated via the RF interface. The fields are separated into groups as follows:

- User information:

    - Name
    - Department
    - Location
    - Phone number
    - Position

- Lease information:

    - Start and end dates
    - Lease term
    - Lease amount
    - Lessor name

- Asset information:

    - Purchase date
    - Date of last inventory
    - Warranty end date
    - Warranty duration
    - Amount
    - Asset identification number

- LCCM image profile data:

    - Image name
    - Image date

- Network connection information:

    - System name
    - Login userID
    - Number of network cards
    - IP addresses
    - Default gateway
    - Subnet masks

- Five custom fields:

    - Label (for each field)
    - Data (for each field)

2.2 The RF antenna

The antenna is a passive RF receiver/transmitter and therefore does not have any power source of its own. It is designed to read data from the EEPROM and write data to the EEPROM using the energy generated by the RF field from the reader.

In operation, the reader initiates communications by generating a 125 kHz RF carrier signal modulated with information to be sent to the antenna and EEPROM (collectively called the *tag*). The reader then generates an unmodulated carrier and waits for a response from the tag. The tag uses backscatter modulation (BSM) to respond to the reader.

In this technique, the tag sends information to the reader by modulating the field generated by the reader and reflecting it back. The tag inside the PC is not capable of generating any RF signal on its own. It can only respond to the field generated by a reader designed for use with RFID.

2.3 The RF reader/writer

The RF reader/writer is an external device that communicates with the Asset ID tag via the RF antenna. A reader is required to read or write data using the RF interface. The three types of reader are: handheld, portal, and panel.

- A handheld reader is a reader that is battery operated and designed for portable use. These devices are typically designed to be lightweight with an antenna that is easily positioned within close proximity to a tag. Applications for these readers include deployment or inventory of assets throughout the enterprise.

  An example is the combination of the Symbol Corporation Portable Data Terminal (PDT) and HID Corporation AMH100 handheld reader as discussed below. This portable combination lets you read from and write to the Asset ID tag plus upload that data to a PC-based application via the PDT's serial interface.

  The PDT is completely programmable via the serial interface. Typically, the PDT software is downloaded during the installation of the asset software on the PC it is connected to.

- Panel readers are usually mounted on a wall or placed on a counter near a protected area. This type of reader is primarily used in a paperless, property pass application.

- Portal readers are devices that have a more permanent installation, typically located at a doorway or portal to a protected area. Portal readers are positioned so as to require the asset to be carried through the reader field to exit or enter the area.

Regardless of the reader type, since power for the EEPROM is obtained from the RF signal generated by the reader, it is possible to read and write the EEPROM with the asset still in the shipping box.

2.3.1 Symbol Technologies Portable Data Terminal

The Symbol PDT is a handheld programmable terminal with built-in barcode scanner. RFID applications such as QueTel Asset TraQ and the Asset ID Starter Kit work with both the Symbol 6100 and the 8-line Symbol 3100 PDTs.

Product information about these devices can be found at:

```
http://www.symbol.com/products/mobile_computers/mobile_kb_pdt_3100.html
http://www.symbol.com/products/mobile_computers/mobile_kb_pdt_6100.html
```

Symbol 6100   Symbol 3100

Figure 3. Symbol PDTs (6100 and 3100)

These PDTs are available with a variety of installed memory from 640 KB to 7.2 MB. The extra memory lets you store more Asset ID data from clients without having to upload to a PC.

Using the following values, you can determine how many systems you can record in the available RAM:

- QueTel application: 500 KB
- Each Asset ID record: 550 bytes

This means, for example, the 640 KB model of the 3100 can hold data for up to 254 systems:

```
640 KB - 500 KB = 140 KB / 550 bytes = 254 systems
```

The Symbol cradle, power supply and 25-9 pin null modem cable shown in Figure 4 is part of the QueTel Asset ID Starter Kit as described in 3.1, "QueTel Asset ID Starter Kit" on page 16. You can also order each item separately.

This combination provides the following functions:

❶ Recharger and cradle to store the PDT
❷ Connectivity to the host PC for data transfer and programming of the PDT
❸ Space to recharge an optional second battery

Figure 4. Recharger and host connection cradle

Also available is a cable and power supply combination, as shown in Figure 5, that performs the same functions, but without the bulk of the cradle. These components are ordered separately.

Figure 5. Recharger and host connection kit

2.3.2 HID Corporation AMH100 RF Reader

Figure 6. HID Corporation AMH100 RF Reader

The AMH100 plugs into the Symbol PDT to provide a read/write interface to the Asset ID tag. The connector provides an RS-232 interface.

Using a converter the AMH100 can be connected directly to a desktop PC or ThinkPad via the serial port. This does, however, also require an AC adapter for the AMH100 as the PC serial port cannot power the unit directly.

Product information about this device can be found at:

`http://www.proxtrak.com/products/handrdr.html`

2.4 Supported systems

Selected IBM desktop PCs have both the Asset ID EEPROM and the RF antenna installed inside the system unit. In most instances, the RF antenna is located behind the front bezel of the system unit (see Figure 8 on page 13). Some systems (for example, some ThinkPad models) only have the EEPROM installed as standard, but the antenna is available as an option.

The location of the antenna is also indicated by an Asset ID "bull's-eye" sticker on the outside of the packing box in which the desktop system was shipped:
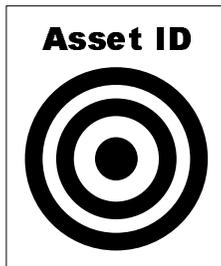
Figure 7. Asset ID sticker on packing box

The purpose of the sticker, as well as showing you that the system is enabled for Asset ID, is that it indicates the location of the RF antenna and where you should point the RF reader to communicate with the Asset ID subsystem.

Tip: If you are having problems scanning a system while it's still in its shipping carton, try the following:

- Rotate the AMH100 RF Reader 90°. If the system is a mini-tower instead of a desktop, the antenna will be in a different orientation.
- Move the RF Reader closer or further away from the box.
- Try the area around the bull's-eye sticker, not just on the sticker.

ThinkPad systems have the EEPROM installed on the system planar but typically, the RF antenna is an easily installable option. This means that you cannot use the RF interface of the EEPROM until you install the option. You can use the system interface with tools such as LCCM, however.

The following systems have Asset ID capabilities. This means that, except where noted, they have both the EEPROM and the RF antenna installed:

IBM PC 300PL:

- Model 6862
- Model 6892
- Model 6584
- Model 6594
- Model 6565

IntelliStation:

- M Pro Model 6889
- E Pro Model 6893
- Z Pro Model 6865

NetVista:

- A40p Model 6649
- A40p Model 6579
- A40p Model 6841
- S40p Model 6646

ThinkPad:

- T20, Models 2647 and 2648 (requires RF Antenna option 08K6064)
- A20 Models 2628 and 2633 (requires RF Antenna option 08K6064)

The list of the latest supported systems can be found at:

http://www.pc.ibm.com/ww/assetid/systems.html

You can also get details about the level of Asset ID support from spec sheets at one of the following addresses:

http://www.pc.ibm.com/us/netvista/library.html
http://www.pc.ibm.com/us/thinkpad/tech_library.html
http://www.pc.ibm.com/us/intellistation/tech_library.html

In some other desktop systems (for example, NetVista A40 and S40 systems), the Asset ID EEPROM is installed but there is no option for an antenna and thus it cannot be RFID enabled in the future. This means you can use tools such as LCCM and UM Services to read and write to the EEPROM but you cannot use a handheld reader to access Asset ID data via the RF interface.

The antenna option for the ThinkPads, once installed, should not normally be removed. In some systems, such as ThinkPad T20s, the antenna cannot physically be removed once it is installed. On the ThinkPad A20 systems, if you do decide to remove the antenna, make sure you disable antenna detection (using the RFID Security menu accessible from the Config menu in the System BIOS) before you remove the antenna. If you do not, you will get a POST error 0193 which will prevent the system from starting until the antenna is reinstalled.

The Asset ID antenna is in different locations depending on the system, as indicated in Figure 8. You should hold the AMH100 RF Reader about 3-5 inches (8-13 cm) in front of these areas to get proper communication with the antenna.

Note: The face of the AMH100 RF Reader should be parallel to the antenna to get a proper reading. If the reader is 90° out, for example, you may not be able to establish communications with the antenna. If you are scanning

systems while they are still in their packing boxes, you should determine, from Figure 8, what the antenna orientation is.

Figure 8. Asset ID antenna locations on various IBM systems

2.5 Software

There are a number of software products that work with Asset ID. These include:

- LANClient Control Manager (LCCM) is an IBM product that is used to remotely install software on client machines. On Asset ID-enabled client machines, LCCM can read user information from the EEPROM to make a rollout totally automatic. LCCM can also write information to the EEPROM for use by other applications. See 4.1, "LANClient Control Manager" on page 50 and the LCCM Web page:

    `http://www.pc.ibm.com/us/desktop/lccm`

- Software Delivery Assistant (SDA) is an IBM product that lets you easily roll out sets of applications to a particular business groups. See 4.2, "Integrating Software Delivery Assistant with Asset ID" on page 87 and the SDA Web page:

    `http://www.pc.ibm.com/ww/software/applications/sda`

- UM Services, Netfinity Director 2.12 and IBM Director 2.2. These IBM management products can also read from and write to the EEPROM and queries can be made against that data from a large group of systems for

analysis. See Chapter 5, "Integrating with IBM Director" on page 111 and the UM Services and Netfinity Director/IBM Director Web pages:

```
http://www.pc.ibm.com/ww/software/applications/ums/index.html
http://www.pc.ibm.com/ww/eserver/xseries/systems_management/
```

- Tivoli products, with the use of the Universal Manageability Services plus module for Tivoli Framework, allow you to access the Asset ID data from your Tivoli console. See Chapter 6, "Integrating Asset ID with Tivoli Inventory" on page 127.

- The Asset ID Starter Kit from QueTel, an IBM Business Partner, is a combination of a handheld RF reader/writer plus software to access the Asset ID data via the RF interface into the EEPROM. The Asset ID Starter Kit is an excellent entry-product for inventory and rollout tasks. See 3.1, "QueTel Asset ID Starter Kit" on page 16 and the Asset ID Starter Kit Web page:

```
http://www.quetel.com/docs/rfid/starterkit.htm
```

- Asset TraQ from QueTel is their full-function asset management tool, which also interfaces with the RF interface of the EEPROM using a handheld scanner or other RF device (portal, panel, etc.). See 3.2, "QueTel Asset TraQ" on page 35 and the Asset TraQ Web page:

```
http://www.quetel.com/docs/rfid/assetidflyer.htm
```

2.6 Support

The Web page with product information for Asset ID is:

```
http://www.pc.ibm.com/ww/assetid
```

You can obtain technical support for Asset ID and other UM products (LCCM and Netfinity Director for example), both via e-mail and via a moderated forum. Access both of these at:

```
http://www.pc.ibm.com/ww/solutions/enterprise/support/
```

Chapter 3. Asset ID partner solutions

IBM has technology partners that can provide customers with Asset ID solutions that take advantage of the RFID technology available in many models of IBM PCs, workstations, and ThinkPads. A complete list of partners is available at:

`http://www.pc.ibm.com/ww/assetid/partners.html`

IBM enables solutions from these partners through the specifications and interface of the Asset ID EEPROM and antenna.

In this chapter we concentrate on the RFID software products from QueTel Corporation, one of IBM's technology partners. We briefly review the products and their functionality.

In addition to the Asset ID integrated in IBM ThinkPads and desktop PCs, the hardware used by these products are:

- Symbol Technologies 6100 Portable Data Terminal
- HID Corporation AMH100 RF Reader

Here are some hints and tips regarding the use of these devices:

- The Symbol PDTs will shut themselves off after a certain amount of inactivity to conserve battery power. When the unit is powered up again it will resume on the screen that was last displayed.

- The client PC that you want to scan does not have to be powered on or even plugged in to a power outlet for the RFID process to function.

- When using the HID AMH100 to read from or write to the RFID tag, hold the unit approximately 3-5 inches (7-13 cm) from the RFID antenna. If you are too close or too far away from the antenna, the unit and antenna will not communicate successfully.

- The optimum read and write range is obtained when the front of the AMH100 is oriented parallel to the long axis of antenna.

- When reading or writing to the RFID tag, if the HID AMH100 LED flashes green or alternates between red and green, this means the HID AMH100 is communicating with the RFID tag.

    - Green indicates the reader is reading (receiving) or writing (transmitting) from the Asset ID tag
    - Red indicates the reader is searching for the Asset ID tag

- When reading from or writing to the RFID tag, if the HID AMH100 LED only flashes red, it means the AMH100 cannot find or properly

15

communicate with the RFID tag. This may be because of one or more the following factors:

– HID AMH100 is too far from or too close to the RFID tag.
– The RFID antenna is disconnected from the system board.
– A large monitor or similar device that creates a strong magnetic field is turned on and is in very close proximity to the RFID tag or AMH100 and is causing interference.

• There have been reported situations where, during the initial scan of the Asset ID data in a client PC, you see the error message:

`Invalid Checksum`

This error prevents the complete reading of the Asset ID data. The problem is because the user area in the Asset ID EEPROM was not initialized during manufacture. No new systems have this problem, although older systems may experience this.

Solutions to this problem are:

- Use the PDT to write data to any one field in the user area of the Asset ID EEPROM. This will force a recalculation of the checksum.

- Contact the application manufacturer (for example, QueTel). They can provide a workaround that forces a recalculation of the checksum.

3.1 QueTel Asset ID Starter Kit

QueTel has a new product, Asset ID Starter Kit, which is a cost-effective way for customers to start taking advantage of Asset ID.

The Asset ID Starter Kit includes a portable data terminal (PDT) that reads and writes to RFID tags and Asset ID Starter Kit software. The collected asset data from the RFID tag is stored in the PDT and is easily downloaded in a standard format (Comma Delimited ASCII .CSV file) using the Asset ID Starter Kit software. The file can then easily be imported to any standard database or spreadsheet application.

The Asset ID Starter Kit software may be considered a light version of their Asset TraQ software (see 3.2, "QueTel Asset TraQ" on page 35). In fact both the Asset ID Starter Kit and Asset TraQ use the same software engine in the PDT.

The major difference between the two products is how the asset data can be managed and manipulated. The data collected by the Asset ID Starter Kit must be managed by an external database or spreadsheet, whereas Asset

TraQ is an all-encompassing asset-tracking application with its own built-in database and report generator.

The Asset ID Starter Kit has the following components:

- Symbol Technologies PDT 3100 with 640 KB RAM
- HID Corporation AMH100 RFID Reader
- Asset ID Starter Kit software
- PDT software
- Hardware to connect the PDT to a PC via the PC's serial port
- Asset ID Starter Kit User Guide

For more information on this product see:

`http://www.quetel.com/docs/rfid/starterkit.htm`

3.1.1 Installing the Asset ID Starter Kit

In our test environment we installed the Asset ID Starter Kit software on an IBM 300PL (Model 6862) running Windows 2000 Professional. We used the Symbol Technologies PDT 6100 and the HID Corporation AMH100 reader.

We installed the 60-day demo version of the software, which can be obtained from:

`ftp://ftp.quetel.com/pub`

Note: If you do plan to download the software, you will require the Symbol PDT 3100 (or compatible Symbol PDT) and an HID AMH100. QueTel has an evaluation program where these devices can be rented for a small fee. Contact QueTel for more information about this program. See `http://www.quetel.com/docs/corporate/contactdw.htm` for contact information.

Programming the Symbol PDT can be equated to loading an operating system on a PC. The following installation instructions assumes you have these items:

- The file RFIDDE.EXE downloaded from `ftp://ftp.quetel.com/pub`.

- A suitable Symbol PDT and peripheral accessories to connect to a PC.

- The HID AMH100.

- A license key valid for the day you are installing the software. A demonstration key is available by contacting QueTel as described in a dialog box during the application installation.

- Local administrative rights if using Windows NT or Windows 2000.

Notes:

1. When you purchase the Asset ID Starter Kit from QueTel, the Symbol PDT is preprogrammed and the application software is supplied on CD-ROM. If you download the demonstration code from the QueTel Web site, you have to program the PDT as part of the installation process.

2. The size of installed IDE hard disks may be incorrectly reported. For SCSI hard disks, you will not receive any size information because the SCSI subsystem has its own BIOS and that information is not accessible to the system BIOS nor the Asset ID EEPROM.

3. On ThinkPads, the memory amount returned is incorrect (usually half of the actual value). This is a problem with ThinkPad BIOS and Asset ID area and plans are to fix this in future versions of the ThinkPad BIOS. Check `http://www.pc.ibm.com/support` for details.

3.1.1.1 Installing the PC software

1. Locate and run RFIDDE.EXE that you just downloaded.

2. You will be prompted if you want to continue. Click **Yes**.

3. Click **Next** to continue.

4. If the user information is correct click **Next**.

5. You will be prompted for a registration number. This must be obtained from QueTel. If you do not have a registration number, the dialog box lists a phone number to call to obtain a demonstration registration number. Enter your number and then click the **Register Now** button.

6. Complete the installation process by following the prompts.

7. Restart your computer.

8. Attach your Symbol serial connector/charger from the PDT base or mini-docking unit/charger to a COM port on your PC. We have used COM1. Ensure that there is power to the charging unit.

9. On your PC change the serial port settings to the following values. On our PC 300PL with Windows 2000 installed, we followed these steps:

   a. Right-click **My Computer** and click **Properties**.
   b. Click the **Hardware** tab.
   c. Select **Device Manager**.
   d. Expand **Ports (COM & LPT)**.
   e. Double-click **Communications Port (COM1)**.
   f. Click the **Port Settings** tab.
   g. Make the changes as listed in Table 2 then click **OK.**
   h. Close Device Manager.

Table 2. COM1 settings

Setting	Value
Bits per second	38400
Data Bits	7
Parity	odd
Stop Bits	1
Flow Control	Xon / Xoff

3.1.1.2 Installing the Symbol PDT software

Now that the PC software component is installed and the COM port configured, the next step is to install the software on the Symbol PDT.

1. Start the Asset ID Starter Kit application. Figure 9 appears:
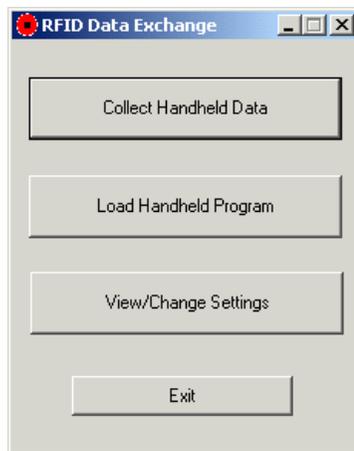
Figure 9. Asset ID Starter Kit main window

2. If you are using a COM port other than COM 1, make the appropriate changes by clicking **View/Change Settings**.

3. Click **Load Handheld Program** in the dialog box. Figure 10 appears.
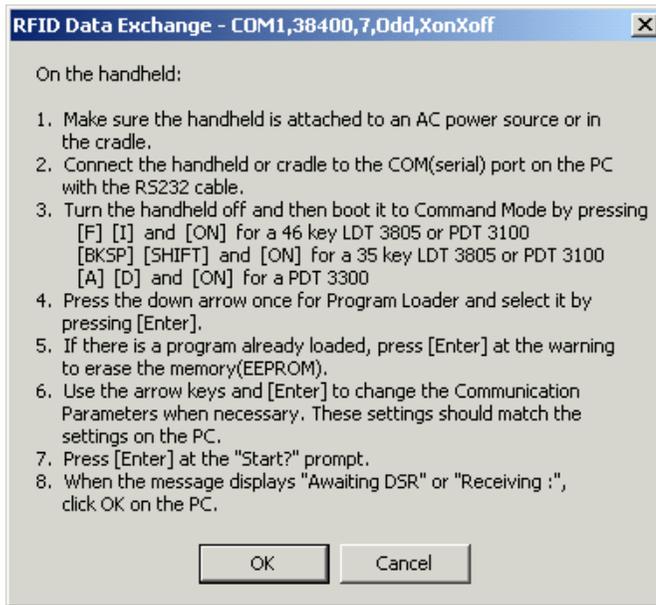
Figure 10. Programming the Symbol PDT

4. Carefully follow the instructions on the dialog box shown.

   Note for step 3: If you have a Symbol 6100, use the steps for the 35-key models.

5. You will have to change the settings on your Symbol PDT communication settings to reflect the PC settings.

6. Press the Enter button on the PDT then click **OK** on the dialog box on the PC. The PC will start downloading data to the PDT. You will see various hex code changing on the PDT if the data is being transferred such as BC00, BD00 etc.

7. The download is completed successfully when you see STATUS 0000 on the Symbol PDT.

8. At the PC, you will see Figure 11.

   Follow its directions carefully to cold boot the PDT. If you are using a Symbol 6100 use the key sequence for the 35-key LDT/PDTs. Cold boot the PDT only if the data has been successfully downloaded. Otherwise, you will have to download the software from the PC again.

RFID Data Exchange

If the handheld's screen displays STATUS 0000, then
the HEX file was successfully loaded.

Turn the handheld off and cold boot it by pressing
[A] [B] [D] and [ON] for a 46-key LDT 3805 or PDT 3100
[SPACE] [FUNC] [UP ARROW] and [ON] for a 35-key LDT or PDT 3100
[F1] [F4] [ENTER] and [ON] for a PDT 3300

If the handheld's screen does not display STATUS 0000, then
the HEX file was not successfully loaded.

OK

Figure 11. Cold booting the PDT

9. Take the Symbol unit out of its charging / serial connection interface. The PDT may turn on automatically when removed from the charging unit. You will see the QueTel welcome screen:

```
Data Collection Pgm
RFID to Asset TraQ

QueTel Corporation

                  ^
Press ENTER to Start
```
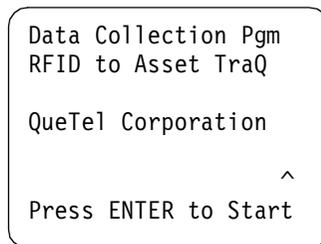
Press Enter to continue. This shows you the technical support address and phone number. Press Enter to continue.

10. Attach the AMH100 Handheld Reader to the Symbol PDT.

11. Power on the Symbol PDT by pressing the small on/off button or by pressing the large yellow buttons on the side. You may have to press the Enter button a few times to bypass the QueTel prompts.

12. At one prompt you will be asked for date and time. Press the Clear button to change this.

13. Enter the current date by using the numbers on the keypad and then press the Enter button. This will bring you down to the time field.

14. Enter the current time using a 24-hour clock and then press the Enter button.

15. You will be prompted if these date and time values are correct. If they are, press the Enter button.

16. The Main Menu now appears.

3.1.2 Viewing and updating the Asset ID data

RFID provides the means to read data from the Asset ID area which is very beneficial for various reasons including tracking physical assets. To further enhance this process, the Asset ID Starter Kit allows you to write to the Asset ID area on the PC. This information can be read through RFID or later read by various pieces of management software such as:

- IBM Director
- IBM UM Services
- IBM LAN Client Control Manager (LCCM)
- Intel LANDesk (with UM integration module)
- Microsoft SMS (with UM integration module)
- Tivoli Inventory (with UM integration module)

To view or modify Asset ID data, do the following:

1. Turn on the Symbol PDT. The HID AMH100 should be attached. Go to the main menu.

```
** Main Menu **
1:Collect New Items
2:Inv On-Hand Items
3:RFID View/Modify
4:RFID Only
5:Utility Menu >>

vSELECT ITEM or CLR
```

2. From the main menu choose option 3, **RFID View/Modify**, using the cursor keys on the keypad. Press the Enter button.

> **Tip**
>
> If you use Option 4, RFID Only, you will move directly to step 5 on page 23. This is very useful if you want to quickly change the contents in Asset ID.

```
Key-in NAME/ID of
Inventory Taker:
........

ENTER/CLR/or FNC+4
```

3. Enter the name of the inventory taker. This is a mandatory field and must be 3-8 characters in length. Entering data into the PDT can be accomplished one of two ways:

   a. Manually key the information through the PDT keypad. You will have to familiarize yourself with the keypad, since many buttons have multiple functions depending on the current mode (Alpha or Function).

   b. Use the Scan button on the Symbol PDT to scan entries from barcodes.

      With third-party tools such as Strandware's Label Matrix, you can create and print barcodes, which you can then scan in using the Symbol PDT. This process is similar to scanning techniques used at the supermarket checkouts. Label Matrix is available for purchase or as a downloadable demonstration version from:

      `http://www.strandware.com/`

4. After entering or scanning in the inventory taker's name, similar screens will appear asking for the following additional data:

   – Location (1-15 characters)
   – Building (1-25 characters)
   – Room number (1-6 characters)

   Note: These answers are used by the QueTel software and are unrelated to Asset ID. The location, building, and room number are the ones for the asset and not the inventory taker.

5. The following screen will then appear:

```
LOCATION
BUILDING
ROOM
 Place reader next
 to RFID Tag, and
 press ENTER when
 ready to scan or
 FNC+6 - Main Menu
```

6. Hold the AMH100 three to five inches from the RFID antenna (see Figure 8 on page 13 for locations) and press Enter to start the scan. You should see a progress indicator on the PDT showing the percentage of the scan completed:

7. Once the RFID scan is completed you will be presented with a screen that will look similar to this:

```
User: ERIC CHONG
CPU: Pentium II
Speed: 450 MHz
Memory: 128 MB
HD: 449
 1:Update Tag
 2:View/Modify Tag
 3Cancel/Scan Next
```

8. Press 2 to select **View/Modify Tag**. You may have to press the Alpha key first to change the function of the key from the letter V to the number 2.

   Note: Unlike some of the other screens, you cannot use the cursor keys to highlight the option.

   You will be presented with the following screen:

```
 ** User Data **
1:Read-only Data
2:User Info
3:Lease Data
4:Warranty
5:Image Profile
6:User Defined
7.Network Connection
8:Update Tag
vSELECT ITEM or CLR
```

Note: The Symbol PDT displays only eight lines of text at a time. Consequently the lines **7:Network connection** and **8:Update Tag** may not initially appear. You have to use the cursor keys to scroll the screen to see it.

These options correspond to the groups in the user area of the Asset ID EEPROM as described in 2.1.3, "User area" on page 5.

9. Here you can select the group you want to view or update. For our example, we choose to update the user information.

10. Highlight option 2, **User Info** by using the cursor keys and then press the Enter button. You will see a screen similar to the following:

```
  ** User Info **
Name :ERIC.CHONG...>
Title:IT SPECIALIST
Dept :TCO
Loc  :Markham
Phone:

    F4-Continue
```

11. This screen displays the data currently in the Asset ID area under the group User Info.

12. If you do not want to make any changes, press Func+4 (press the Func key then press 4) to go back to the previous menu.

13. To make changes, edit the information by keying in the information or scanning it in using a barcode and the PDT's barcode scanner.

14. Press Enter to move to the next field. Any changes made will be saved.

> **Tip**
>
> If you make any changes, press the Enter button four to five times to cycle through all the fields to ensure all changes are saved in memory.

15. Press the Func key then the 4 key. This will bring you back to the user data screen.

16. If you want, use the same procedures to view or edit the other groups: Lease Data, Warranty, Image Profile, User Defined, and Network Connection.

> **Tip**
>
> Many of the fields in the Network Connection group are dynamic. We suggest you use these as read only.

17. Once the viewing and editing have been completed, use the down cursor key to scroll down to option 8, **Update Tag** and press the Enter button.

18. You are prompted to enter (or scan) a barcode. Since we are just updating the tag, press Enter to bypass the prompt.

   Note: If you use the **RFID Only** option (option 4 on the main menu), this prompt is skipped.

19. Press Enter to start the updating process.

20. Hold the AMH100 three to five inches from the RFID antenna. The RFID update starts. You will see a progress indicator showing the status.

   Note: If you are unable to successfully communicate with the Asset ID EEPROM, you will be prompted to rescan the device.

21. If the update was successful, you will see:

```
* UPDATE ASSET ID *

Updat  User Info
Verif  Updated!
       Press any key

Completed: 100%
```
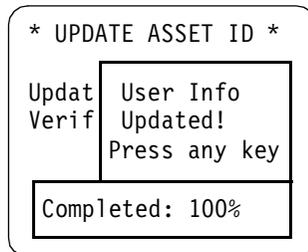
   If there was a problem with the update, you will see an error message.

22. You will be returned to the Changes menu.

```
Changes?

1. None-continue
2. Change Rm No.
3. Change Bldg ID
4. Go To Main Menu

        1
```
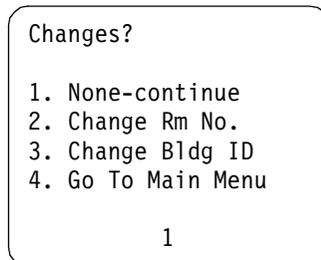
   If there are no more changes, select option 1 and press Enter.

23. You will now be brought back to the menu outlined in step 5 on page 23:

```
 LOCATION
 BUILDING
 ROOM
  Place reader next
  to RFID Tag, and
  press ENTER when
  ready to scan or
  FNC+6 - Main Menu
```

24. Press Enter if you want to view and or update another RFID tag. If you want to exit, hold the Func key and then press the 6 key, which will take you back to the main menu.

3.1.3 Collecting inventory

One of the primary purposes of the Asset ID Starter Kit is to perform an inventory of a set of client PCs (or any other devices with RFID tags). The following steps describe how to gather Asset ID from a group of systems:

1. Using the cursor keys on the PDT, highlight item 1, **Collect New Items** then press the Enter button.

2. We will now need to input the following information:

   - Inventory taker name (3-8 characters)

   - Location (1-15 characters)

   - Building (1-25 characters)

   - Room number (1-6 characters)

   - Barcode label — You can keyin or scan a barcode for this asset. This is a mandatory field for all assets, whether you are using RFID or not. If you manually key in the barcode, you will have to key it in a second time for validation.

   - Description code (1-7 characters)

You can enter these via the PDT keypad or you can scan in a barcode with the information. With third-party tools such as Strandware's Label Matrix you can create and print barcodes which you can then scan in using the Symbol PDT. This process is similar to scanning techniques used at the supermarket checkouts. Label Matrix is available for purchase or as a downloadable demonstration version from:

`http://www.strandware.com/`

The data that you enter or scan in is recorded in the PDT and exported to the CSV file in columns 1-11 as described in Table 3 on page 33.

Note: Each field is mandatory. The inventory taker name field must be at least three characters.

> ┌─ **Hint** ───┐
>
> The barcode field does not have to be unique, so if you don't want to record the actual barcode for the system you are scanning, you could just scan in any barcode and use that same barcode for every system. (You could stick a barcode on the back of the AMH100 for example, and scan that each time.)

3. You will be prompted to **Scan Asset ID (Y/N)**. Since we are using RFID to scan in systems, press Y on the keypad then press the Enter button.

   If you press N, you can enter information manually via the PDT keypad. This will let you collect information on non-RFID enabled assets, such as older PCs.

4. Hold the HID AMH100 unit approximately three to five inches from the RFID antenna (see Figure 8 on page 13 for locations). The LED on the AMH100 should flash between green and red. This indicates that it is working properly. You should also see a progress indicator on the Symbol PDT indicating the transfer is in progress.

5. Once completed you will be prompted for any changes:

```
Changes?

1. None-continue
2. Change Rm No.
3. Change Bldg ID
4. Go To Main Menu

        1
```

   On this screen you can enter a different room number or building number from what you entered in step 2. Since we had no changes, we pressed Enter to accept the default option, **None-continue**.

6. You will now be prompted to enter another unique barcode label to scan in.

   By default, the first four fields you entered in step 2 are assumed to be the same for every scan:

   – Inventory taker name
   – Location
   – Building

– Room number

The premise behind this is that you would scan multiple machines in a specific room. Scan in a new barcode. Repeat steps 3-5 to scan the other systems in this room into the PDT.

7. Once you have completed reading systems into the PDT, enter 4 on the keypad to select **Go To Main Menu** and then press the Enter button.

3.1.4 Uploading information to the PC

Once the information is captured, we will upload it to our PC where the data can be exported in CSV format for use in a spreadsheet or database.

1. Turn off the Symbol PDT.

2. Detach the AMH100 from the Symbol PDT.

3. Plug in the Symbol PDT into the peripheral that connects your PDT to your PC's serial port.

4. From the main menu on the PDT, highlight option 5, **Utility Menu** and press the Enter button.

```
** Utility Menu **
1:Send Data to PC
2:Erase Data on HH
3:Load Lookup Tables
4:Erase Tables on HH
5:Set Date and Time
6:System Help
vSELECT ITEM or CLR
```

5. Highlight option 1, **Send Data to PC**, then press the Enter button.

6. You will be prompted with the communication settings:

```
Set PC comms at:

 19200
 NONE
 8

Press ENTER to start
or CLEAR to Cancel
```

These settings should match the settings on the PC. Do *not* press the Enter button yet.

7. At the PC, launch the Asset ID Starter Kit application. The main window appears:
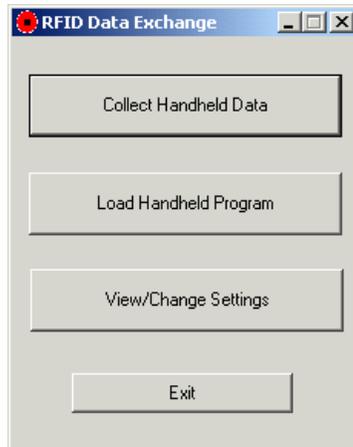
Figure 12. Asset ID Starter Kit application

8. Click **Collect Handheld Data**.

9. The first time you use this function, you will be prompted to select the name of the file to write to.

   If this is not the first time you've used this function, you will jump to step 14.
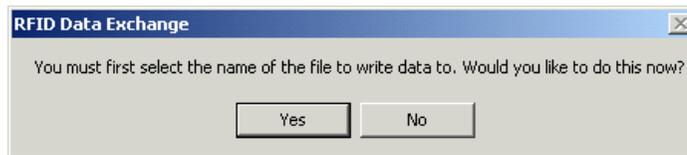
Figure 13. Creation of the CSV file for the first time.

   Click **Yes** to agree and continue. This filename will be used for all subsequent data uploads. Click **No** if you do not want to create this file at this time, the operation will stop and you will be returned to the main menu.

   When you click **Yes**, Figure 14 appears:
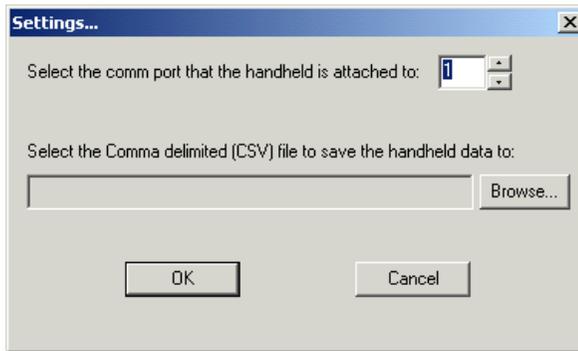
Figure 14. View/Change Settings window

10. You are prompted to specify the name and location of the CSV data file. Click **Browse** to find the directory where you want to save the data to.

   Note: You can update the filename at a later time by clicking the **Collect Handheld Data** button. Figure 14 will appear again and you can change the settings.
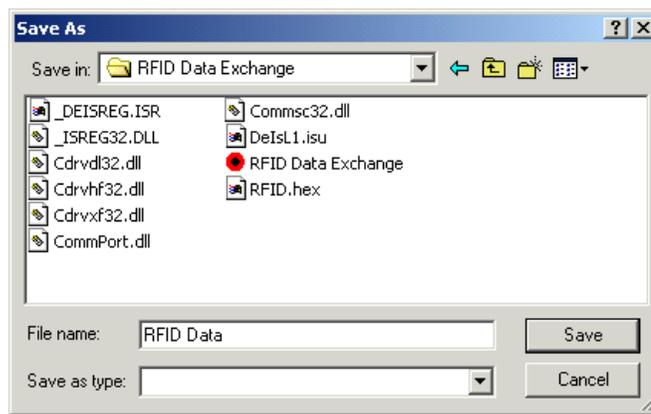
Figure 15. Creating and saving the RFID Data file

11. You can choose to accept the default of a filename of RFID Data.CSV in the My Documents folder, or you can select something else. We chose to save the file in the C:\Program Files\QueTel\RFID Data Exchange folder. Click **Save**.
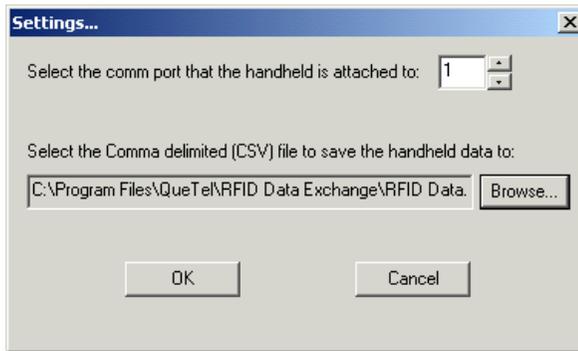
Figure 16. Verifying the location to save

12. Click **OK** to confirm the location and file.

13. You will be returned to the main menu. Click **Collect Handheld Data** a second time.

14. Now, on the PDT press the Enter button.

    Note: You may have to turn the PDT on again.

    You should see a progress indicator showing that data is being uploaded. Both the PC and the PDT will prompt you when this process is complete as illustrated in Figure 17. Click **OK** on the dialog box on the PC.
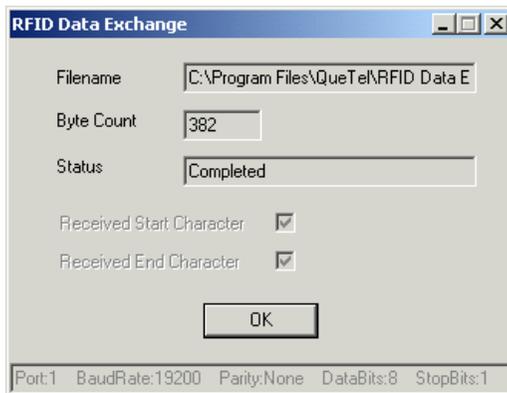
Figure 17. Successful upload to the PC

You now have a file on the PC of all the data that was scanned in. The file that gets created is a text file formatted as a comma-separated variable (CSV) file, which can be imported into applications such as Lotus 1-2-3 or Microsoft Excel.

Table 3 shows the format of the CSV file:

- Columns 1-11 are generated by the QueTel software and are not taken from the Asset ID tag. The remaining columns are directly taken from the Asset ID EEPROM.

- Columns 3-8 contain the data you entered manually in step 2 on page 27.

- Columns 9-11 (asset manufacturer, model and serial number) contain data if you selected No to the question **Scan Asset ID (Y/N)** in step 3 on page 28. If you answered Yes to this question, these fields would be blank.

- Columns 34-38 are the five custom data fields in the user area as described in 2.1, "The Asset ID EEPROM" on page 4. However, the five custom field labels are not retrieved by the software.

*Table 3. Format of the CSV file*

Column	Data	Type
1	Datestamp	Date
2	Timestamp	Date
3	Inventory taker name/ID	Char width 50
4	Location	Char width 50
5	Building	Char width 50
6	Room	Char width 50
7	Barcode	Char width 50
8	Description Code	Char width 50
9	Asset Manufacturer	Char width 50
10	Asset Model Number	Char width 50
11	Asset Serial Number	Char width 50
12	Tag ID	Char width 50
13	Tag Manufacturer	Char width 50
14	Tag Model Number	Char width 50
15	Tag Serial Number	Char width 50
16	User Name	Char width 50
17	User Department	Char width 50
18	User Location	Char width 50

Column	Data	Type
19	User Phone Number	Char width 50
20	User Position	Char width 50
21	Lease Start Date	Date
22	Lease End Date	Date
23	Lease Term	Integer
24	Lease Amount	Currency
25	Lessor	Char width 50
26	Asset Purchase Date	Date
27	Asset Last Inventoried Date	Date
28	Asset Warranty End Date	Date
29	Asset Warranty Duration	Integer
30	Asset Purchase Amount	Currency
31	Asset Number	Char width 50
32	Profile Image Date	Date
33	Profile Image Name	Char width 50
34	User-Defined Value 1	Char width 50
35	User-Defined Value 2	Char width 50
36	User-Defined Value 3	Char width 50
37	User-Defined Value 4	Char width 50
38	User-Defined Value 5	Char width 50
39	UUID	Char width 50
40	MAC Address 1	Char width 50
41	MAC Address 2	Char width 50
42	CPU Family 1	Char width 50
43	CPU Family 2	Char width 50
44	CPU Speed 1	Char width 50
45	CPU Speed 2	Char width 50

Column	Data	Type
46	Memory Size 1	Char width 50
47	Memory Size 2	Char width 50
48	Memory Size 3	Char width 50
49	Memory Size 4	Char width 50
50	FDD1	Char width 50
51	FDD2	Char width 50
52	IDE Type 1	Char width 50
53	IDE Type 2	Char width 50
54	IDE Size 1	Char width 50
55	IDE Size 2	Char width 50

3.2 QueTel Asset TraQ

QueTel's end-to-end PC asset-tracking solution is *Asset TraQ*. Asset TraQ provides all the necessary tools including a database, to inventory your RFID-enabled PCs.

The Asset TraQ application is a comprehensive asset system that can even track non-RFID assets. The functions include:

- Search capability — Perform searches based on multiple criteria.
- Report writer — Present information in an organized format either on paper, screen or digital file.
- Import module — Map and import data from other sources.
- Export module — Export a file to common file formats using selected search criteria.
- Global replace — Identify specific data records and data elements to change.
- Password and security module — Set up users and groups with varying authority to view, read, and write data.
- Purge capability — Identify a class of records to remove or retire and store as archive status.
- Record history — Each time a record is changed, the action is recorded in the history section.

The Asset TraQ solution comprises the following components:

- Asset TraQ software application
- Symbol PDT (Portable Data Terminal) 3100 or 6100
- Peripheral hardware to connect PDT to PC via serial port
- HID AMH 100 RFID Reader
- PDT software application
- User's guide

For more information about this product, visit:

`http://www.QueTel.com/docs/rfid/assetidflyer.htm`

To contact QueTel, see:

`http://www.QueTel.com/docs/corporate/contactdw.htm`

3.2.1 Before you begin

In our test environment we installed Asset TraQ on an IBM 300PL (Model 6862) running Windows 2000 Professional. We used the Symbol Technologies PDT 6100 and the HID Corporation AMH100 reader.

We installed the 60-day demo version of the software, which can be obtained from:

`ftp://ftp.quetel.com/pub`

Note: If you do plan to download the software, you will require the Symbol PDT 3100 (or compatible Symbol PDT) and an HID AMH100. QueTel has an evaluation program where these devices can be rented for a small fee. Contact QueTel for information about this program.

Programming the Symbol PDT can be equated to loading an operating system on a PC. The following installation instructions assumes you have these items:

- The file ASSET_ID.EXE downloaded from `ftp://ftp.quetel.com/pub`
- A suitable Symbol PDT and peripheral accessories to connect to a PC.
- The HID AMH100.
- A license key valid for the day you are installing the software. A demonstration key is available by contacting QueTel as described in a dialog box during the application installation.
- Local administrative rights if using Windows NT or Windows 2000.

Notes:

1. The installation procedure using the downloadable demonstration version is different compared to when you purchase the Asset ID Starter Kit from QueTel. When you purchase the kit, the Symbol PDT is preprogrammed and the application software is supplied on CD-ROM.

2. The size of installed IDE hard disks may be incorrectly reported. For SCSI hard disks, you will not receive any size information.

3. On ThinkPads, the memory amount returned is incorrect (usually half of the actual value). This is a problem with ThinkPad BIOS and Asset ID area and plans are to fix this in future versions of the ThinkPad BIOS. Check `http://www.pc.ibm.com/support` for details.

3.2.2 Installation procedure

To install Asset TraQ, do the following:

1. Attach your Symbol serial connector/charger from the PDT base or mini-docking unit/charger to a COM port on your PC. We have used COM1. Ensure that there is power to the charging unit.

2. On your PC change the serial port settings to the following values. On our PC300 with Windows 2000 installed, we followed these steps:

   a. Right-click **My Computer** and click **Properties**.
   b. Click the **Hardware** tab.
   c. Select Device Manager.
   d. Expand **Ports (COM & LPT)**.
   e. Double-click **Communications Port (COM1)**.
   f. Click the **Port Settings** tab.
   g. Make the changes as listed in Table 4, then click **OK.**
   h. Close Device Manager.

Table 4.   COM1 settings

Setting	Value
Bits per second	38400
Data Bits	7
Parity	odd
Stop Bits	1
Flow Control	Xon / Xoff

3. Locate and run ASSET_ID.EXE.

4. Complete the installation process by following the prompts.

5. Restart your computer when prompted.

6. Log back in with Administrator rights.

7. Launch Asset TraQ.

8. You will be prompted for a registration number. This must be obtained from QueTel. If you do not have a registration number there is a number to call provided in the dialog box. Enter your registration number and then click **Register Now**.

9. You will be prompted with a logon ID and password. Both the logon ID and password are "quetel".

10. Since we are using the downloadable demo version, you will be shown database with three demo records.

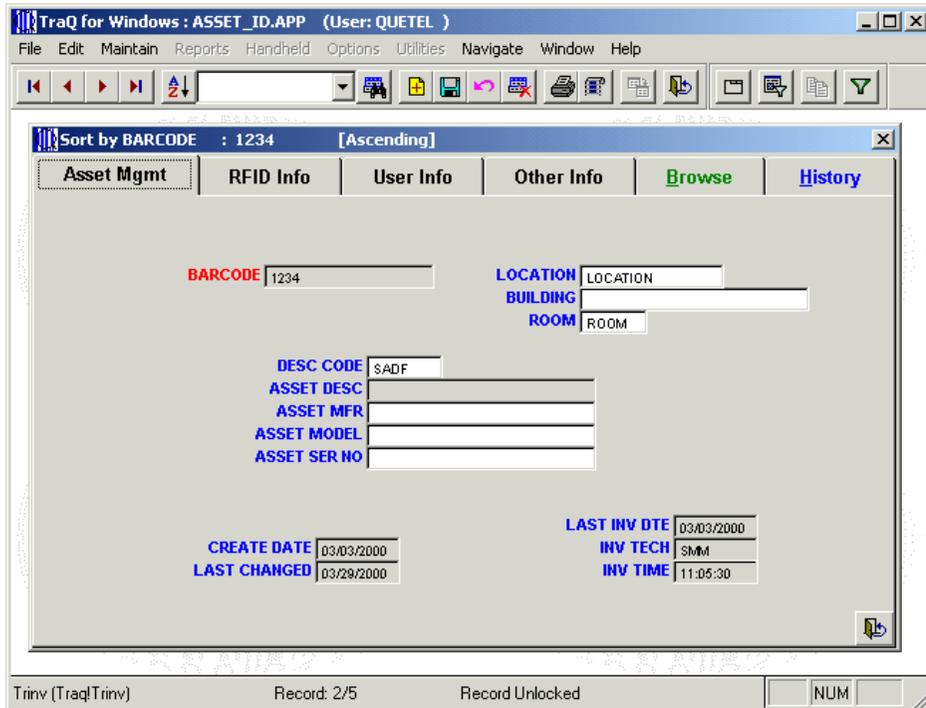

Figure 18. Main window after logon

11. Close this database.

   Note: You must close the database to activate the additional menu items that you need, including the Handheld item.

12. Click **Handheld > Load Program**. Figure 19 appears.

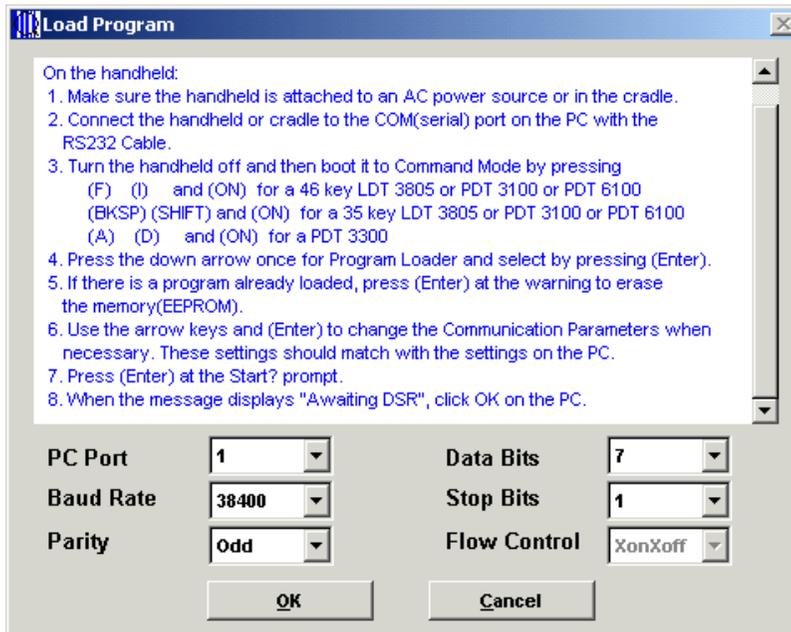*Figure 19. Configuring the COM port*

13. Change the settings to match Figure 19.

14. Follow the instructions in Figure 19. Click **OK** when you have finished these steps.

15. If loaded successfully you will see `Status 0000` on your PDT. Follow the steps in Figure 20 to cold boot the PDT.
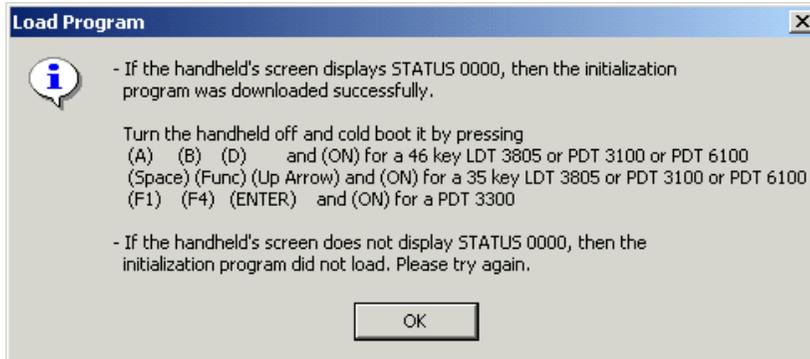

Figure 20. Cold booting the PDT

16. Once your PDT has been rebooted, click **OK** to close the dialog box.

17. Take the Symbol unit out of its charging / serial connection interface. The PDT may turn on automatically when removed from the charging unit. You will be prompted with the QueTel information. Press Enter on the PDT to continue.

18. Attach the AMH100 to the Symbol PDT.

19. Power-on the Symbol PDT by pressing the small on/off button or by pressing the large yellow buttons on the side. Press the Enter button to continue through the two welcome screens.

20. At one prompt you will be asked for date and time. Press the Clear button to change this.

21. Enter the current date by using the numbers on the keypad and then press the Enter button. This will bring you down to the time field.

22. Enter the current time using a 24-hour clock and then press the Enter button.

23. You will be prompted if these date and time values are correct. If they are press the Enter button.

24. You will now see the main menu:

```
** Main Menu **
1:Collect New Items
2:Inv On-Hand Items
3:RFID View/Modify
4:RFID Only
5:Utility Menu >>

vSELECT ITEM or CLR
```

3.2.3 Asset TraQ and the Asset ID Starter Kit

The engine that runs the Symbol PDT for Asset TraQ is the same one used for the Asset ID Starter Kit. Hence the following similarities:

- The steps to view and modify Asset ID data are the same. Refer to 3.1.2, "Viewing and updating the Asset ID data" on page 22 for details.

- The steps to perform inventory data collection are the same. Refer to 3.1.3, "Collecting inventory" on page 27 for details.

- The process to upload data is the same on the PDT side but slightly different on the PC side.

We step you through the upload process in the following section.

3.2.4 Uploading information to the PC

Once the information is captured (as described in 3.1.3, "Collecting inventory" on page 27), it is uploaded to our PC into the Asset TraQ software.

1. Turn off your Symbol PDT.

2. Detach the AMH100 from the Symbol PDT.

3. Plug the Symbol PDT into the peripheral that connects your PDT to your PC's serial port.

4. Launch Asset TraQ

5. Log in with user ID and password ("quetel" for both). The Asset TraQ main window now appears.

6. On the PDT, highlight option 5, **Utility Menu** and press the Enter button.

```
** Utility Menu **
1:Send Data to PC
2:Erase Data on HH
3:Load Lookup Tables
4:Erase Tables on HH
5:Set Date and Time
6:System Help
vSELECT ITEM or CLR
```

7. Highlight option 1, **Send Data to PC** then press the Enter button.

8. You will be prompted with the communication settings. These settings should already be correct, however, do not press the Enter button yet.

9. In Asset TraQ on the PC, close the database window. The Handheld pull-down menu now becomes active:

With the database closed, the Handheld pulldown menu is now active.

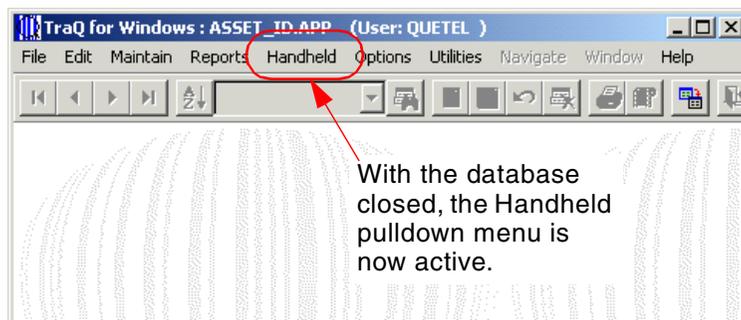*Figure 21. Asset TraQ main window with database closed*

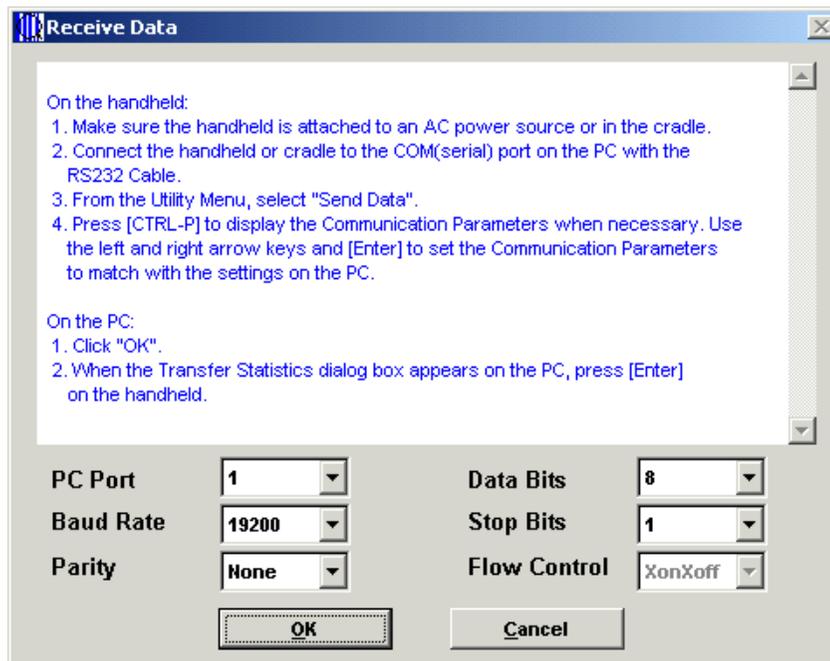10. Click **Handheld > Receive Data**. Figure 22 appears.

Figure 22. Uploading data to the PC

11. The settings should be correct. If not, make the appropriate changes.

12. Click **OK**.

13. Press the Enter button on the PDT.

14. If successful you will see the status change to `Completed` as shown in Figure 23:
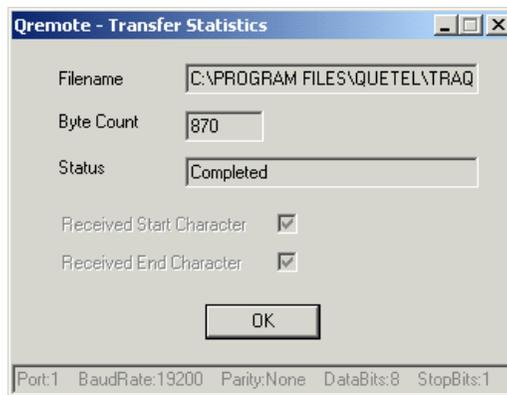
Figure 23. Successful upload

15.Click **OK.**

16.You will be prompted if there is more data to receive. Click **No**.

Figure 24. Receive more data prompt

17.You will be prompted to send the reports to a file. Click **Yes**.
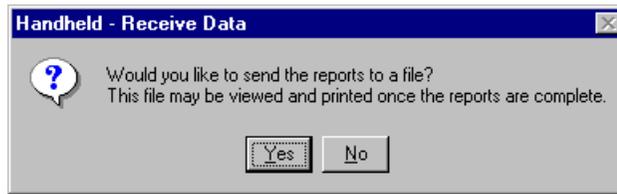
Figure 25. Send data to report file

18.Click **OK** to close the dialog window.

19.You can choose to browse the file but the information will wrap. Click **OK.**

Figure 26. Report dialog

20.Click **OK** to close the dialog box.

3.2.5 LCCM Export Utility

As described in 4.1.2, "Scanning clients into LCCM" on page 58, LCCM must "scan in" clients so LCCM can populate its own database. Once LCCM recognizes these clients then LCCM can process them accordingly.

For LCCM to scan in these clients into its database, the client must boot from the network. One method of forcing the client to boot from the network is remotely waking it up using Wake on LAN. By default IBM PCs with RFID will boot from the network first and then from the local hard drive using its alternate boot sequence. For this to work, LCCM must know the MAC address of each machine that needs to be started.

The LCCM Export Utility in Asset TraQ can help by creating a text file listing all the MAC addresses.

As an example, the following steps will create a text file of all the MAC addresses for systems that have been scanned in ("created") today. You can use other criteria to select the systems you want.

1. Launch Asset TraQ and log in.

2. Close the master database window if it is open.

3. Click **Options > LCCM Export** > **MAC Address Only**.
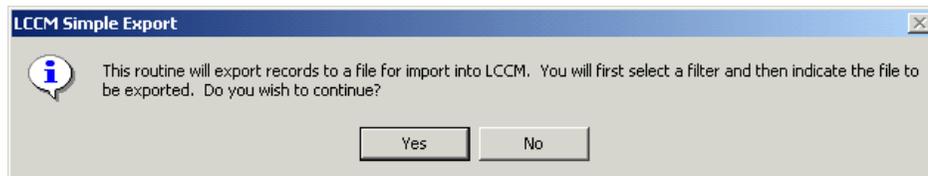
Figure 27. LCCM export prompt

4. Click **Yes** to continue.

5. You may encounter an error prompt. If this occurs contact QueTel and they will provide you with a new version of TRAQW.EXE. In the meantime, bypass the error, because it is not critical.
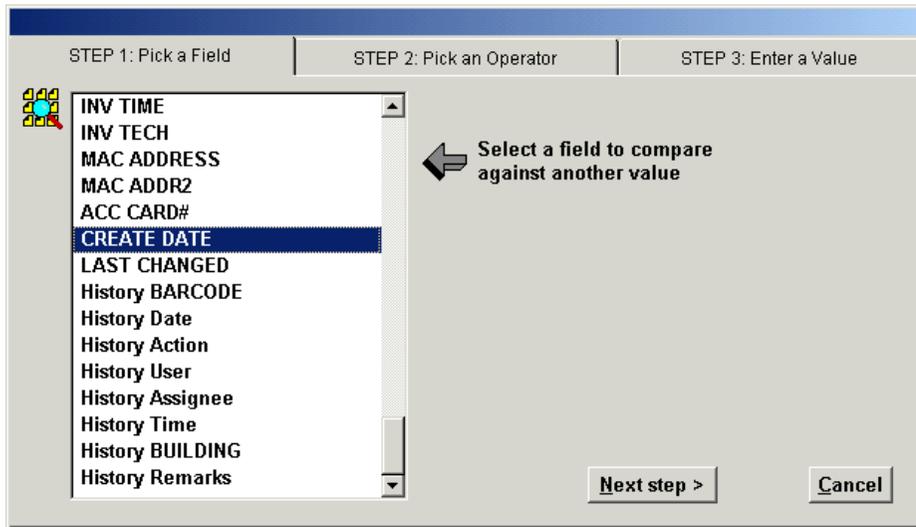
Figure 28. Step 1

6. In the list box, scroll down and select **CREATE DATE**. This means the date the system was scanned into Asset TraQ. You could use other criteria if you want.

7. Click **Next step.**
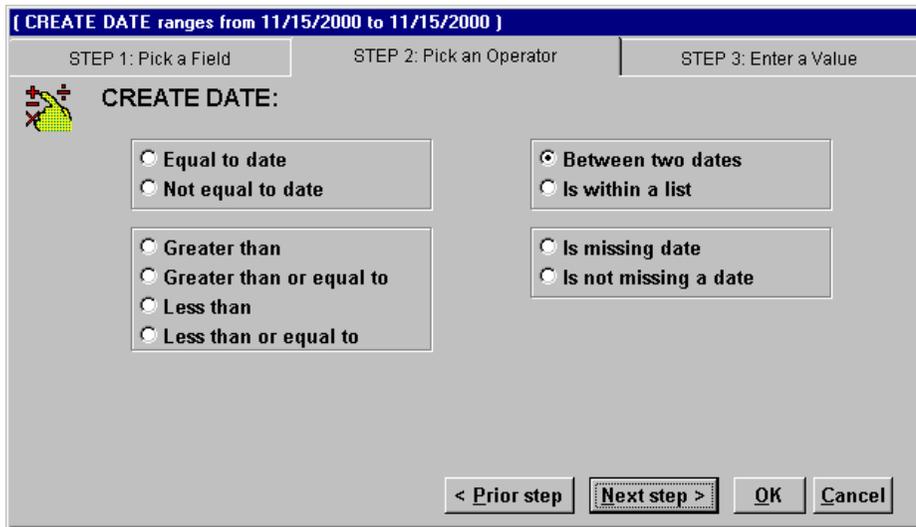
Figure 29. Step 2

8. Select **Between two dates**. The next screen, Step 3, should appear. If it doesn't click **Next step**.

Figure 30. Step 3

9. Put today's date in the From field and tomorrow's date in the To field. This specifies that you want all the systems that were scanned in today.

10. Click **OK**. You will now have a filter condition created.

Figure 31. Filter created

11. Click **OK**.

12. We will keep the default location and file name LCCM_MAC. Click **Save**.

13. Figure 32 appears showing the status of the number of records exported, file name and location. Make a note of the file name and location and click **OK.**
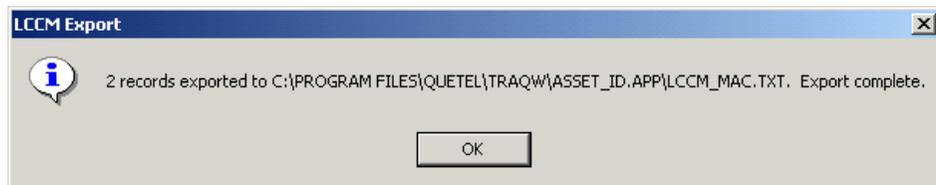
Figure 32. Successful LCCM MAC address export

The LCCM_MAC.TXT file can now be used in LCCM by clicking **Tools > Wake Clients** as described in 4.1.2, "Scanning clients into LCCM" on page 58.

3.2.6 Browsing the master database

Now that you have some records collected, you probably want to view them. There are multiple ways of viewing and sorting records in Asset TraQ. We will look at the most basic method of accomplishing this, using the browse function.

1. If your master database is closed, you will need to open it. There are two ways to do this:

   – Use the hot keys: Ctrl+M.
   – Click **Maintain > Master Database**.

2. You will be presented with different views depending on what tab is selected.

3. Click the **Browse** tab and all the records will show. Note that the database has three demo records.

Figure 33. Master database browse function

3.3 Other RFID solutions

There are other solutions from QueTel and from WiseTrack. These solutions don't use a PDT and are therefore less portable. They require the following items to read and write to the RFID tags:

- A desktop PC or ThinkPad with a serial port
- HID AMH100 transponder
- HID AMH100 Handheld Reader Connector Assembly
- HID AMH100 Handheld Reader power supply
- AC power outlet
- Software from QueTel or Wisetrack

These solutions are less portable because the AMH100 requires a separate power supply, which plugs into a regular AC power outlet.

Please contact QueTel and Wisetrack for more information:

```
http://www.quetel.com
http://www.wisetrack.com
```

Chapter 4. Integration with LCCM and SDA

LANClient Control Manager (LCCM) and Software Delivery Assistant (SDA) are software tools that make it easier to install software packages onto client PCs.

In this chapter, we describe how to use these tools with Asset ID to automate a rollout of operating systems and applications. We also integrate other tools such as imaging products, Microsoft Sysprep and Microsoft ScriptIt to aid with the automation. Imaging products include PowerQuest Drive Image Pro and Norton Ghost.

LCCM supports unattended installations of all WIN32 operating systems. Such operations can take anywhere from 20 minutes to an hour or more depending on the operating system, network throughput, speed of the server, and the speed of the client. While this is sufficient for some customers, there are some problems and inefficiencies:

- Cloning tools such as PowerQuest Drive Image Pro and Norton Ghost can reduce the installation time to under 10 minutes; however, LCCM with its built-in Cloneit tool only supports the cloning of Windows 95/98 systems. We have developed a solution for Windows 2000, and this is documented in this chapter.

- Without LCCM, these cloning programs require that a person start the process manually from each client PC. This can be solved with LCCM.

- The cloned PCs are true clones and must be customized to change the user login ID, computer name, SIDs (Security Identifiers), and so on. This customization problem can be solved through the use of Microsoft Sysprep.

- When a PC is transferred to a new owner or needs to be rebuilt, the customized information such as user ID and computer name must be reentered. This can be solved with Asset ID.

SDA, when used with LCCM and Asset ID, can also install applications onto the client workstations. The combination of these tools makes for a very efficient rollout process.

LCCM, SDA and a third tool, System Migration Assistant (SMA), are available together in the *IBM System Installation Tool Kit*. The tool kit makes it easier to install, configure, and use these tools. For information, see:

`http://www.pc.ibm.com/ww/solutions/lcc/sit.html`

49

4.1 LANClient Control Manager

Technology is rapidly changing in both the hardware and software industries. Most if not all organizations try to keep current with the technology curve. As a result, hardware and software is now deployed, redeployed, reimaged and retired more frequently than in the past. IBM LANClient Control Manager (LCCM) is a deployment and redeployment tool that addresses these needs.

This section is designed to give you a brief overview of LCCM. For more detailed information on LCCM refer to the IBM Redbook *Using LCCM Functions with Servers and Workstations*, SG24-5292 and the LCCM Web site:

`http://www.pc.ibm.com/us/desktop/lccm/`

LCCM uses industry-standard technology enablers found in many IBM products to automate time-consuming and labor-intensive processes. Here is a typical use of LCCM:

1. LCCM wakes up a client PC at a scheduled time.
2. The client machine boots to the network where it receives boot information from the LCCM server.
3. LCCM prepares (fdisk, format etc.) the client PC if required.
4. LCCM remotely installs an operating system and applications over the network.
5. LCCM configures the PC so it has unique attributes such as computer name, domain, etc.
6. LCCM powers off the PC.
7. The user turns on the PC which is now operational.

LCCM performs these tasks using a number of technologies:

- Wired for Management (WfM) baseline Version 2.0 specifications for the PC (client or server).
- Preboot eXecute Environment (PXE) 1.0 specified in the NetPC Hardware Design Guidelines Version 1.0b or PXE 2.0, or later, specified by Intel Corporation (12/98) for the network adapter.
- Wake on LAN (WOL). Although WOL is not required, it makes rollouts much easier because you can power on the client PCs remotely without local intervention.

The remainder of this section describes how to use LCCM, Asset ID and associated tools to roll out new PCs. The process is summarized in Figure 34:
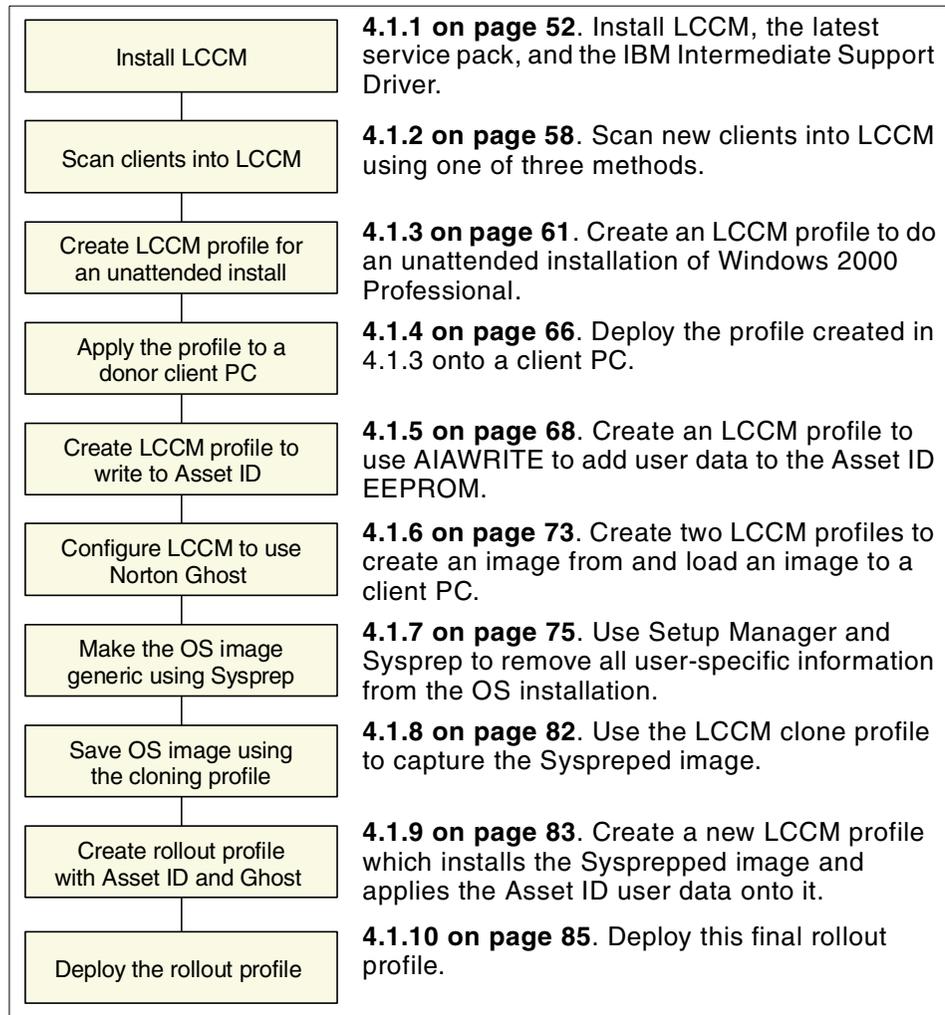
Process Step	Description
Install LCCM	**4.1.1 on page 52**. Install LCCM, the latest service pack, and the IBM Intermediate Support Driver.
Scan clients into LCCM	**4.1.2 on page 58**. Scan new clients into LCCM using one of three methods.
Create LCCM profile for an unattended install	**4.1.3 on page 61**. Create an LCCM profile to do an unattended installation of Windows 2000 Professional.
Apply the profile to a donor client PC	**4.1.4 on page 66**. Deploy the profile created in 4.1.3 onto a client PC.
Create LCCM profile to write to Asset ID	**4.1.5 on page 68**. Create an LCCM profile to use AIAWRITE to add user data to the Asset ID EEPROM.
Configure LCCM to use Norton Ghost	**4.1.6 on page 73**. Create two LCCM profiles to create an image from and load an image to a client PC.
Make the OS image generic using Sysprep	**4.1.7 on page 75**. Use Setup Manager and Sysprep to remove all user-specific information from the OS installation.
Save OS image using the cloning profile	**4.1.8 on page 82**. Use the LCCM clone profile to capture the Syspreped image.
Create rollout profile with Asset ID and Ghost	**4.1.9 on page 83**. Create a new LCCM profile which installs the Sysprepped image and applies the Asset ID user data onto it.
Deploy the rollout profile	**4.1.10 on page 85**. Deploy this final rollout profile.

Figure 34. Using LCCM to roll out PCs

4.1.1 Installing LCCM

In this section, we describe installing LCCM Version 2.5.1 with the latest service pack. At the time of publication, this was Service Pack 4. Before installing LCCM, ensure that your server has the base requirements:

- Windows NT Server 4.0

  - Windows NT Server can be either a Primary Domain Controller (PDC), Backup Domain Controller (BDC), or Stand Alone (member) server.

  - Microsoft Service Pack 6a or higher.

  - Server computer name cannot contain embedded spaces.

  - Optionally, password security can be set to allow zero length passwords, although, as of the latest version of LCCM, this is not required (see "LCCM Password Implementation" on page 30 of *LCCM 2.5.1 Training and Procedures Guides*, available from `http://www.pc.ibm.com/us/desktop/lccm`.

  - NTFS file system.

- 128 MB of RAM minimum with at least an equal or greater sized pagefile

- Pentium 200 MHz processor or faster

- Network connectivity

- Sufficient disk space for all the installation images you wish to deploy

In our environment we have created the following setup. We have attempted to emulate a realistic environment. As such, we will be using the DHCP/PXE functions for LCCM and its clients, and not Remote Program Load (RPL).

Domain: ITSO

- PDC:
  - Netfinity 5000
  - Computer name: ITSOPDC
  - IP Address 9.9.9.9
  - Microsoft DHCP Services with a scope of 9.9.9.20 to 9.9.9.40
  - Gateway (option 3 in Microsoft DHCP) specifies 9.9.9.11 as our LCCM server. You must populate option 3 in Microsoft DHCP; otherwise, the LCCM DHCP proxy service will not function properly. If you do not have a router/gateway as in our case, use the IP address of your LCCM server.

- Member server (not used as part of the LCCM configuration):

  - Netfinity 3000
  - Computer name: ITSOSA4
  - IP Address 9.9.9.10

- Member server (LCCM and IBM Intermediate Support "wedge" Driver):

  - Netfinity 3000
  - Computer name: ITSOSA8
  - IP Address 9.9.9.11

We put LCCM and the IBM Intermediate Support ("wedge") Driver on the ITSOSA8 member server because it offers the following advantages:

- Many organizations already have DHCP implemented.

- A stand-alone server (especially if LCCM is the only application) can be brought up and down with little or no impact to your network.

- If LCCM were installed on either a PDC or BDC, the performance of these servers may be affected since many of LCCM's functions are disk and network I/O intensive.

- Security is less of a factor if LCCM is installed on a stand-alone server. For example you may not want the "deployment" team to have access to the PDC.

One disadvantage with our setup is that user accounts will not be created on the PDC. LCCM does this for you if installed on a PDC. However, this may not be detrimental, since most users will probably have their own user accounts in the domain already.

Before you begin, you should:

- Obtain domain and local administrative access to the servers (the PDC and the LCCM servers)

- Download the following from `http://www.pc.ibm.com/us/desktop/lccm/` and store them on the LCCM server:

  - IBMWEDGE.EXE
  - LCEN251.EXE
  - LCCMSP04.EXE

- Download fixes from `http://www.pc.ibm.com/us/desktop/lccm/house2.html`

4.1.1.1 Installing the IBM Intermediate Support Driver

The IBM Intermediate Support Driver, also known as the wedge driver, is required since we will be using TCP/IP. The wedge driver assists the DHCP services in providing remote clients with boot information.

The wedge driver is installed on the same systems as the LCCM server.

Notes:

1. Original versions of the wedge driver files were placed in the C:\LCCMINST\NT\Wedge directory. However, these are old versions and should not be used. Instead we will be unpacking IBMWEDGE.EXE, which contains the latest driver files.

2. The IBM Wedge driver must be installed and running prior to the LCCM installation; otherwise, the LCCM install will fail.

The wedge driver is installed as part of the IBM System Installation Tool Kit, but you can also follow this procedure to manually install it:

1. Log on with an account that has local administrative rights.

2. Locate the downloaded IBMWEDGE.EXE file and run it.

   It is a self-extracting executable and will unpack by default to C:\TEMP\IBMWedge.

3. Right-click **Network Neighborhood** on your desktop and select **Properties**.

4. Click the **Protocols** tab.

5. Click **Add**.

6. Click **Have disk**. When it prompts you for location, change the location from A: to C:\TEMP\IBMWedge (or the location where you unpacked IBMWEDGE.EXE) and then press Enter. Figure 35 appears.
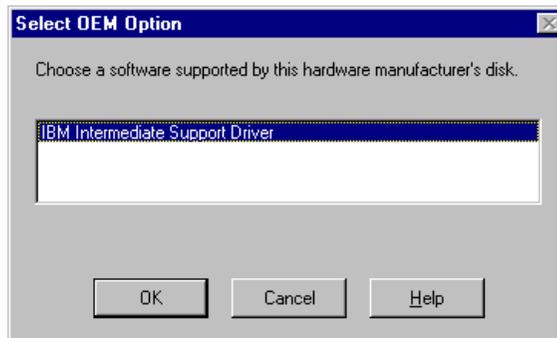

Figure 35. IBM Intermediate Support Driver (wedge) installation

7. Click **OK** and then **Close**.

8. Reboot the server when prompted.

9. Once your server has completed rebooting, log on with an account that has local administrative rights.

4.1.1.2 Installing LCCM 2.5.1

1. Locate the downloaded LCEN251.EXE and run it. It is a self-extracting executable and will unpack the files to C:\LCCMINST.

2. Run SETUP.EXE from C:\LCCMINST\NT.

3. At the LCCM welcome window, click **Next**.

4. You will then be prompted to select a language. The default should be English. Click **Next**.

5. If you agree to the license agreement then click **I Agree**.

6. Leave the default installation as **Perform Server Installation (including workstation files)** and click **Next**.

7. Choose **Custom** for the Installation Type and then click **Next**.

8. Click **Next** so LCCM will be installed to C:\LCCM.

9. Click **Next** to confirm the Windows system directory.

10. Click **Next** for your server name. This should already be populated with your server name. In our case it is \\ITSOSA8.
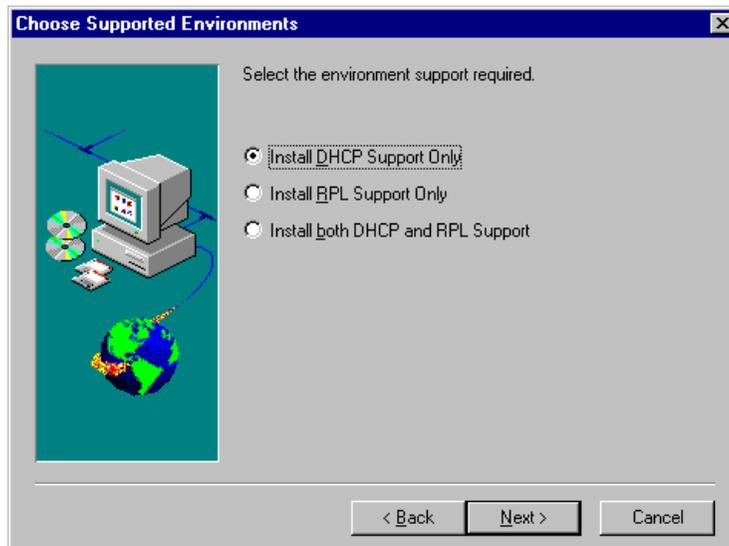

Figure 36. Install DHCP Support only

11. Choose **Install DHCP Support Only** and then click **Next**.

12. Click **Next** to choose the default directories.
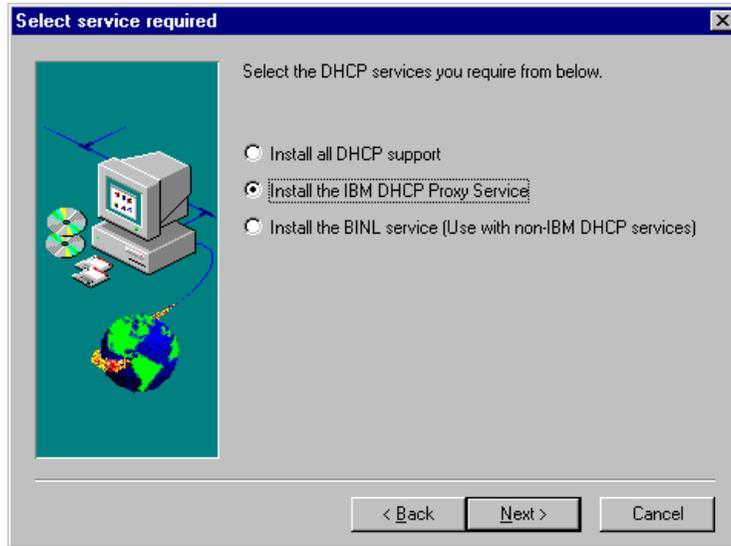
13. Click **Next** for your server's IP Address.

Figure 37. Install the IBM DHCP Proxy Service

14. Select **Install the IBM DHCP Proxy Service** and then click **Next**. We choose this option because there is already a DHCP server on our network.

15. Click **Next**. LCCM should detect that this is a stand-alone server.

16. Click **Next** to select the default program folder. LCCM will now copy over some more files.

17. Click **OK** to close the dialog box.

18. Close any open windows. A reboot is not required.

4.1.1.3 Installing LCCM service pack 4

Install the latest service pack. At the time of publication, this was Service Pack 4.

1. Run the downloaded LCCMSP04.EXE on the LCCM server.

2. Click **OK** to choose the default language of US English.

3. Click **Yes** to continue with the service pack upgrade.

4. Click **Next**.

5. Click **OK** to close the dialog box referring to the reinstallation of the IBM wedge driver. The prompt in this step does not have to be executed since we have already installed the latest version of the IBM wedge driver.

6. Click **Yes** to restart the computer.

7. When the server is finished rebooting, log on with an account that has administrator rights.

8. Read the READMESP4.TXT document in the C:\LCCM directory especially if you are unsure or your environment or your environment is different from ours. The READMESP4.TXT file has detailed explanations for steps 9 and 12.

9. Go to your PDC. Ensure that you have logged on with administrative rights to this server.

10. Connect to the LANC$ADM share on the LCCM machine. For example, enter the following command at a command prompt (ITSOSA8 is our LCCM server):

   ```
   net use x: \\itsosa8\lanc$adm
   ```

11. From the drive that you've mapped to (for example, x:), enter the following command:

   ```
   lccmprep /p
   ```

   The /P parameter specifies a PXE environment. Review the READMESP4.TXT for information about the `LCCMPREP` command. The parameters are not case sensitive.

12. Go back to the server where LCCM is installed. Enter the following command from the C:\LCCM directory:

   ```
   adddom p itso
   ```

   Where `p` refers to a PXE environment and `itso` specifies the domain name. Review the READMESP4.TXT for information about the `ADDDOM` command. The parameters are not case sensitive.

13. You can verify the success of this command by viewing the LCCMDOM.LOG file in the LCCM directory.

4.1.1.4 Install post-SP4 fixes

You should also download any additional fixes from:

```
http://www.pc.ibm.com/us/desktop/lccm/house2.html
```

In particular, if you have NetVista systems, you should download the new versions of AIAREAD and AIAWRITE.

4.1.2 Scanning clients into LCCM

LCCM first has to recognize that the clients exist before it can deploy operating systems to them. In LCCM this process is known as *scanning the clients in*. For this to happen, the client must boot from the network so LCCM can establish a link to it.

The three methods a client can boot from the network and thus be scanned in by LCCM are:

- **Power on the system and press the F12 key**

   This is the recommended method.

   On newer systems, immediately after POST when prompted for "network" or "alternate" boot, you can press F12 to boot to a network device. This applies to most new desktop PCs and ThinkPads supplied with network adapters. As the system is being deployed, the installer could turn the unit on and press F12 once they've attached the cables.

   On a PC, pressing F12 forces the system to boot from the network. On a ThinkPad, pressing F12 brings up a menu where you can select to boot from the mini PCI Ethernet controller usually seen as the Intel Boot Agent (not the network option).

- **Use Wake on LAN to power on the machine**

   If Wake on LAN is supported on your system, you can signal the system remotely requesting that it power up and boot using the Alternate Boot Sequence as defined in the system BIOS.

   The factory default and recommended settings for the Alternate Boot Sequence is Network and then Hard Disk. If you are using this option you must know the network MAC address of each machine in advance. You can determine the MAC address in one of the following ways:

   - Using Asset ID and tools such as QueTel Asset ID Starter Kit or QueTel Asset TraQ as described in Chapter 3, "Asset ID partner solutions" on page 15.
   - Viewing the Ethernet settings in the Setup utility (F1 at boot).
   - Using tools such as Netfinity Director if the PC is already installed and running.
   - Reading the printed label on the network adapter.

   It is easiest if these MAC address are supplied in a text file. The file can be formatted such that each MAC address is on a separate line or on the same line but separated by commas.

Such a text file can be created using QueTel Asset TraQ as described in 3.2.5, "LCCM Export Utility" on page 43.

You can verify the appropriate settings by pressing F1 when the PC boots up and verifying its start options. Here are recommended start options.

Note: The Configuration/Setup Utility differs slightly for each IBM PC model. For ThinkPads using the Ethernet Mini PCI (A, T, and X series) the ThinkPad AC Adapter must be plugged in for the Ethernet mini PCI adapter to receive its trickle charge.

- Devices and I/O ports: Ethernet: Enabled, Network boot: DHCP
- Start Options, Startup Sequence
  - Primary Startup Sequence: Diskette Drive 0, CD-ROM, Hard Disk 0
  - Automatic Power-On Startup Sequence [enabled]: Network, Hard Disk 0
  - Error Startup Sequence: Network
- Power Management, Automatic Power On, Wake on LAN [Enabled] and Start up Sequence [Automatic]
- On newer machines (non-integrated Ethernet) you may have to configure the settings on the network card itself by pressing Ctrl-S when prompted during boot.

- **Boot to network on power-on**

  Set the Primary boot sequence so Network is first on the list and then power on the machine. This will force the machine to boot to the network when powered on.

  We recommend you change the Primary boot sequence back to Diskette Drive 0, CD ROM, Hard Disk 0 once the machine has been scanned in by LCCM. This can be done manually through the BIOS setup or LCCM can make this change for you remotely.

We recommend you use the F12 option to boot the systems to network and scan them in.

However, in our test lab, we were using IBM PC 300PL Model 6862 systems, which do not have the F12 network boot option. Consequently, we used the Wake on LAN option (option 2 from above) to wake up the machines with a text file containing the MAC address of each machine (method 2 from above).

Follow these steps to scan in your clients using Wake on LAN:

1. Start LCCM (Click **Start > Programs > LANClient Control Manager > LANClient Control Manager**)

Note: It is important that the client machines be physically powered off so they can be awakened by LCCM. If they are not powered off, they will not boot from the network and will not be scanned in by LCCM.
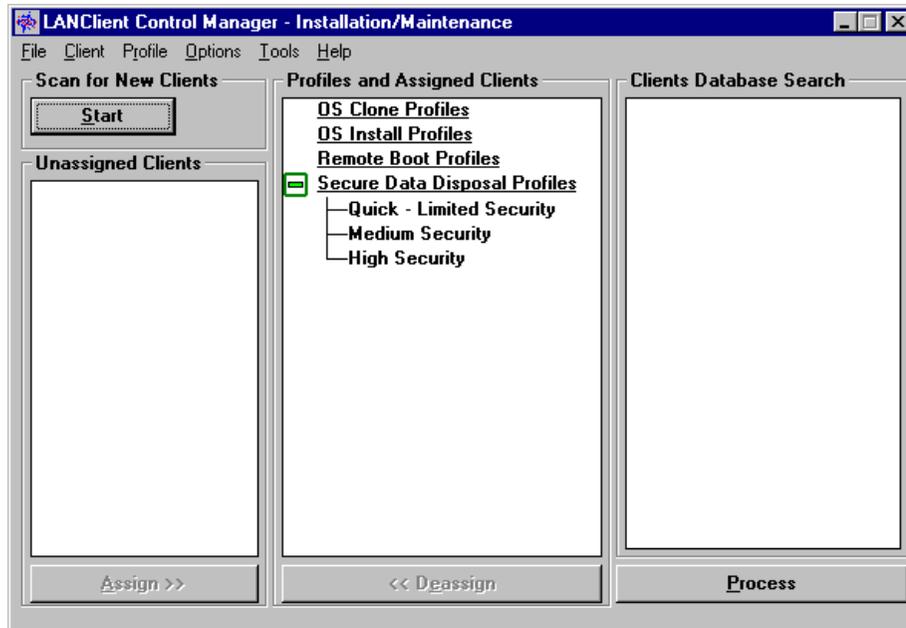

Figure 38. LCCM

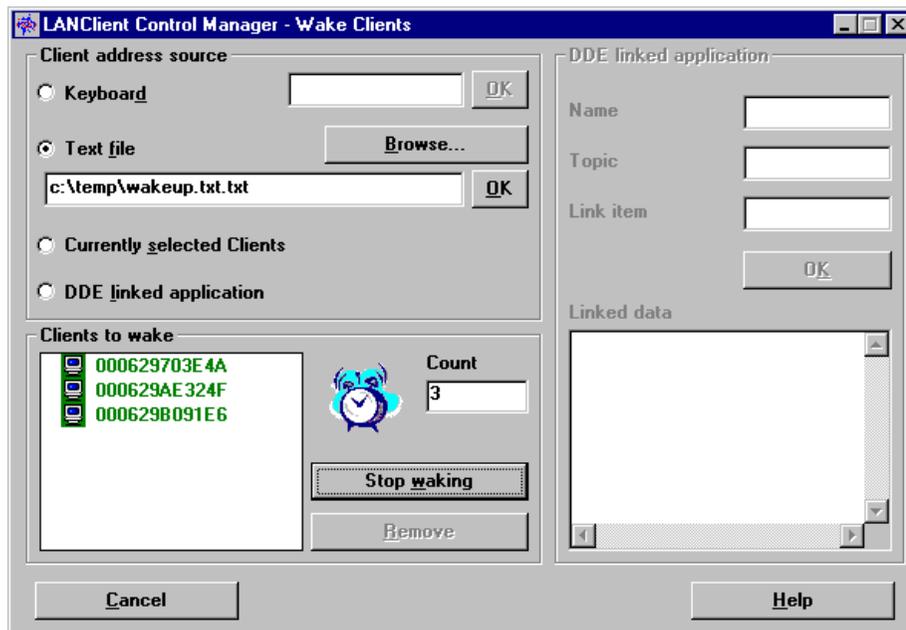2. Click the **Start** button.

3. Click **Tools > Wake Clients**.

Figure 39. Manually waking clients

4. Select **Text file**, then type in the filename of the file containing the MAC addresses or click **Browse** to find the file.

5. Click **OK** and then **Start waking**.

6. Once the list of systems in the Client to wake list box clears, all systems whose MAC addresses were listed in the text file have been scanned in.

7. Click the **Stop waking** button.

8. Figure 38 on page 60 will reappear and you will see your clients now listed in the Unassigned Clients list.

9. Click the **Stop** button.

10. Follow this same process for any other new clients that need to be scanned in.

4.1.3 Creating a Windows 2000 Professional profile

We chose to use Microsoft Windows 2000 Professional because it is a current operating system that provides tools to assist in deployment. In addition many organizations have moved or plan to move to Microsoft Windows 2000 in the near future. Many of the processes and concepts in this section will also apply to other operating systems, with minor modifications.

To create a profile in LCCM for Windows 2000 Professional, do the following:

1. Launch LCCM.

2. Click **Profile > Create new**.

3. Select **Use the Profile Wizard** then click **OK**.

Figure 40. Windows 2000 profile

4. Type Win2000Pro Base in the Profile Name field. Select **Unattended install** and select **Windows 2000 Professional** from the list of supported operating systems. Click **Next**.

5. Click **Next** to choose the default setting of English.

6. Click **Next** to skip the RAID Adapter setup if you do not have a RAID adapter installed.

7. Click **Next** to skip the IBM Rapid Restore options.
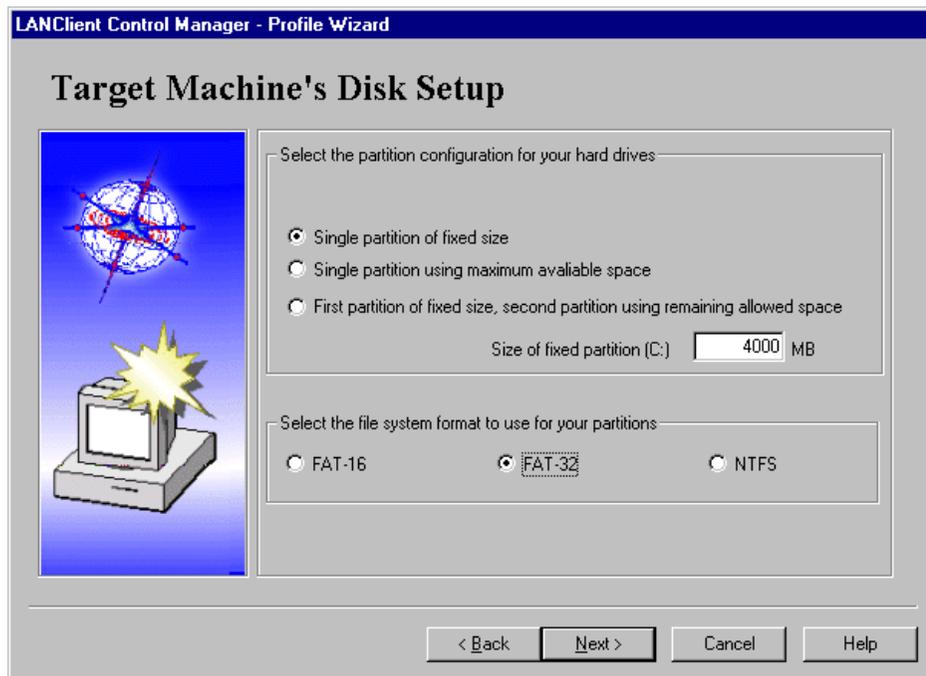
Figure 41. Windows 2000 profile disk setup

8. Select **Single partition of fixed size** and enter your partition size. Make sure your partition will be large enough to hold all your applications.

9. Select the format you want to use then click **Next**. We recommend FAT-32 for these reasons:

   – FAT-32 will give us the ability to create large partitions

   – FAT-32 allows us to read and write to it via DOS with the fat32.exe TSR supplied by LCCM. This will be important, as we will be copying the SYSPREP.INF file to C:\SYSPREP during deployment process

   – FAT-32 will give us the ability to convert to NTFS, which we will be doing during our deployment process.

10. Fill in the Profile Customization information for Company Name and for the Windows 2000 Multi User Product Key. Click **Next**.

11. .Click **Next** to skip the System Migration Assistant.

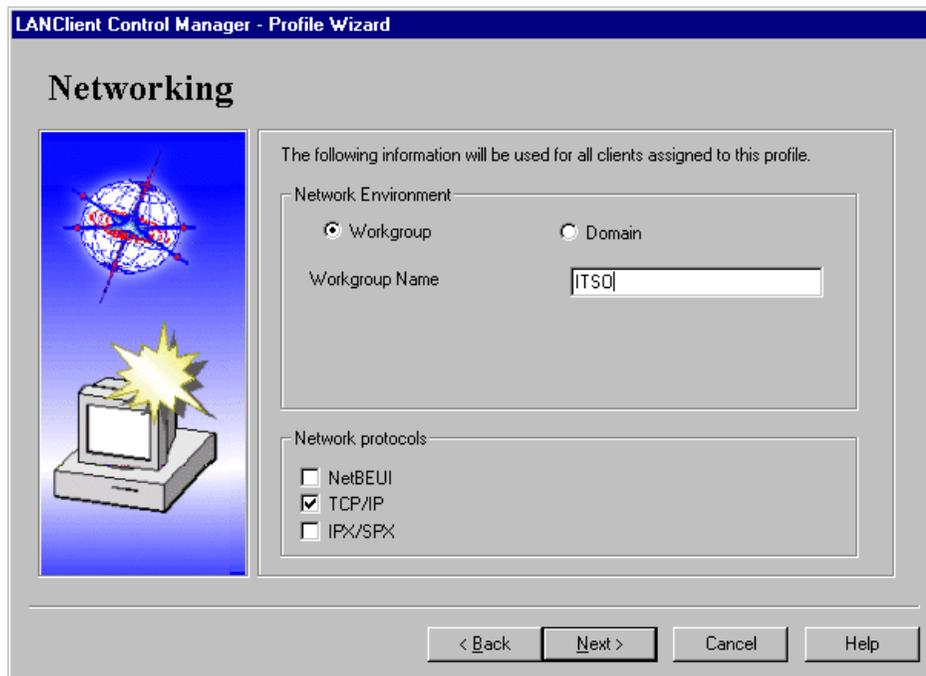12. Choose your default time zone then click **Next.**

Figure 42. Windows 2000 profile networking

13. Select **Workgroup** for your network environment. Microsoft Sysprep will function correctly only if a Workgroup is selected when the PC is being prepared. We used the workgroup name ITSO. A domain can be specified once the machine has been "Sysprepped" and runs the Wizard for the first time. See 4.1.7, "Sysprep: preparing the client for cloning" on page 75 for more information.

14. Select the network protocols you require. At a minimum you should select TCP/IP. Click **Next**.

15. Choose **Obtain IP address from a DHCP Server**. Click **Next**.

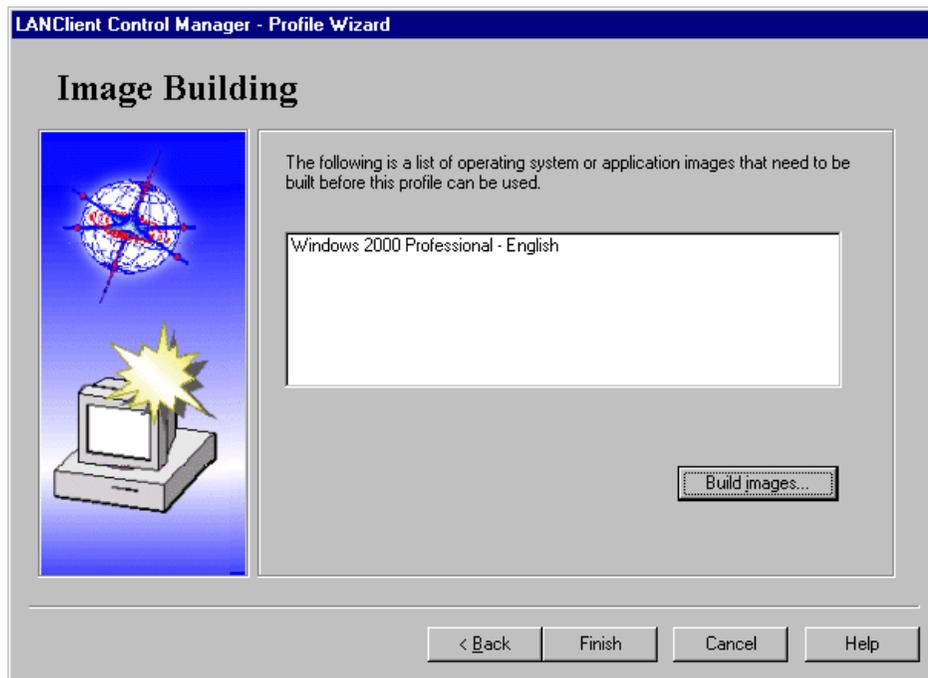16. Click **Next**, since we do not need a description.

Figure 43. Build the image

17.Click **Build images** and then click **Yes**.

Figure 44. Installation file location for Windows 2000 Professional

18.Navigate to the location of WINNT.EXE for Windows 2000 then click **Open**.
   The Windows 2000 Professional installation files will then be copied to the
   designated LCCM profile. You may need the Windows 2000 CD-ROM for
   this.

19. Click **OK** to close the dialog box.

20. Click **Finish**. You should now have a profile called Win2000Pro Base under OS Install Profiles as shown in Figure 45.
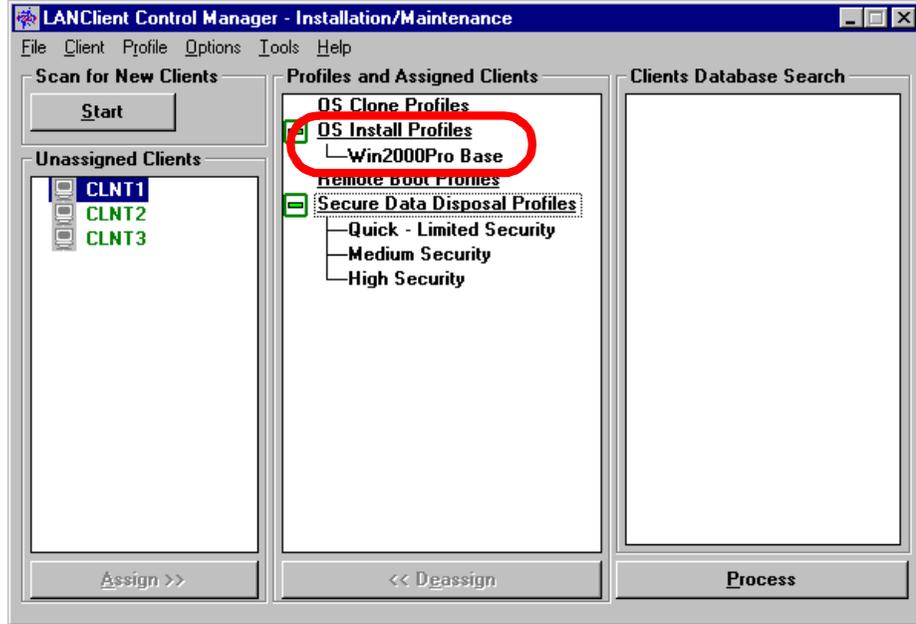

Figure 45. Completed Windows 2000 Professional profile

The next step is to use the new profile to install Windows 2000 Professional on a client PC so that it can be later cloned with Norton Ghost.

4.1.4 Deploying the Windows 2000 Professional profile

Now that we have a profile, we will assign it to (that is, load it on) a selected non-production client PC. We can then use Ghost to take an image of the client build.

If you have different PC models you would assign this Windows 2000 Professional profile to each of them, since the loaded drivers will likely be different from one to another. For example, Models 6862, 6565, and 2628 will each need the profile assigned to them so that we can create three different ghost images.

To assign the Windows 2000 Professional profile to a client PC, do the following:

1. Select a client machine to be the target for our newly created profile.

2. Drag and drop this client to the Win2000Pro Base profile. We have chosen CLNT3 in our scenario.
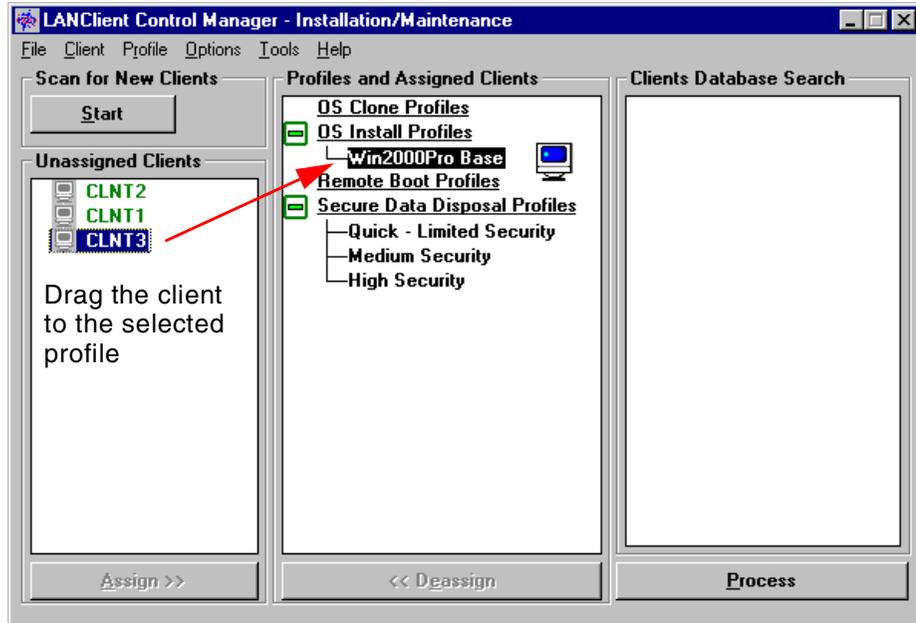

Figure 46. Drag and drop client to Win2000Pro base profile

3. A Client Assignment Wizard should automatically pop up. Click **Next**.

4. Type in your company name (we entered `IBM`) for the LCLI_FREGUSER value. Click **Next**.

5. Click **Next**, since we will use the default value for the first part of the Windows 2000 key.

6. Click **Next**, since we will use the default value for the second part of the Windows 2000 key.

7. Type in `userid` for the LCLI_USERID value. If we were using this profile to deploy to a real production PC, we would use the logon ID for that user. Similarly, we would change our computer name (LCCM client name). LCCM uses the client name for the deployed computer name. In our case, our deployed PC will be known as CLNT3 on the network. Click **Next**.

8. Leave the computer description blank. Click **Next**.

9. A Client Parameter Summary will be presented. Click **Finish**.

10. Because we left the computer description field blank, the wizard asks if we want to go back and enter a value there. Click **No** to continue.

11. You will be returned to your LCCM management console with CLNT3 under the Win2000Pro Base Profile. Click **Process**.

12. The designated remote client will now wake up and LCCM will prepare the remote PC, copy over the Windows 2000 installation files, and then start an unattended install of Windows 2000. The total time for this process is approximately an hour. This time is highly dependent on the speed and amount of memory of your server and client, your network throughput, and the disk I/O of your server and client.

4.1.5 Writing Asset ID data using LCCM

As described in 4.1.4, "Deploying the Windows 2000 Professional profile" on page 66, during the process of installing the operating system on a client PC, you have to enter various user-related data, such as user ID, domain name, computer name and so on. If at a later time, you want to reinstall the operating system image, you may have to re-enter that user information.

With Asset ID, this data can be stored in the Asset ID EEPROM and then later automatically extracted by LCCM and entered during the installation process. This can save much manual effort if you have to upgrade or reinstall many systems.

The first step is to get the user information into Asset ID.

By writing the user variables (domain name, user ID, system name) into the Asset ID EEPROM, LCCM can later extract that information automatically and not prompt the administrator when she wishes to reapply an LCCM profile.

With the use of specific LCCM utilities, these variables can be extracted and used to populate a unique answer file. In our scenario, this will be SYSPREP.INF. With our process we can reimage the machine many subsequent times and each time the machine will be custom configured without having to provide any more user-specific data.

The process will be very beneficial in environments where machines are frequently imaged, such as an educational or training organization. We could also use these same variables to load other operating systems in the same manner. Lastly, we have the ability to change the variables in the Asset ID area should the situation arise. These situations may include:

• New employees, transferred employees and retiring employees
• New, different or amalgamated department(s)

We will be using the following unique variables to simplify this process:

- Computer Name
- Domain Name
- User Name
- Department Name

We have chosen to not use the fields ImageDate and Image from the PreloadProfile group. These fields by themselves will not provide the unique information we require for the client. However these fields together with our defined fields will give LCCM all required information.

You can use the PreloadProfile group to autostart your image download upon initial scan to speed up the deployment. The process for this is documented on page 161 of *LCCM 2.5.1 Training and Procedures Guide* available from `http://www.pc.ibm.com/us/desktop/lccm/docs.html`. We have not incorporated this feature in order to demonstrate the most flexibility in different environments (overnight scheduling, LCCM inputting Asset ID variables for non RFID enabled PCs, preimaged machines from Business Partners as discussed in 7.2.4, "Image delivery location and timing" on page 168). If the autostart feature is useful in your environment, we encourage you to incorporate it into the process outlined in this chapter.

Other predefined variables can be used in addition if necessary.

For more information on available Asset ID fields, refer to the following:

- AIAREAD.TXT and AIAWRITE.TXT, located in C:\LCCM\CLNTFILE

- Appendix 1 of the *LCCM 2.5.1 Training and Procedures Guide*, available from `http://www.pc.ibm.com/us/desktop/lccm/docs.html`

- The Asset ID programming specification, available from `http://www.pc.ibm.com/ww/assetid/standards.html`

To create an LCCM profile that will write to the Asset ID area, do the following:

1. Create a new text file NETWORK.ORG in the C:\LCCM\CLNTFILE directory and insert the following lines:

```
FIELD1=%SYSTEMNAME%
FIELD2=%DOMAIN%
FIELD3=0
FIELD4=0
FIELD5=0
```

Figure 47. NETWORK.ORG

Notes:

- – The NETWORK.ORG file includes fields 3 through 5 with an associated value of 0. These field names and values will be stored in the userdevice group. If we hadn't initialized these names and values, we could have received an error when the Netfinity Director or the UMS agent starts up for the first time.

- – The field names to the left of the equal sign (FIELD1, FIELD2, etc.) are fixed Asset ID names and must be typed in as is.

2. Create a new text file OWNER.ORG in the C:\LCCM\CLNTFILE directory and insert the following lines:

```
OWNERNAME=%OWNERNAME%
DEPARTMENT=%DEPARTMENT%
LOCATION=
PHONE_NUMBER=
OWNERPOSITION=
```

Figure 48. OWNER.ORG

Note: We have left the last three fields blank (location, phone_number, ownerposition). We did this because in some cases, these fields were needed to initialize the ownerdata group on some our test machines. You can provide user variables for these fields to be populated. We have left these blank to simply the process.

3. Create a new text file AIAINPUT.LCI in the C:\LCCM\CLNTFILE directory and insert the following lines:

```
path=s:\;
T:
CD\
MD %CSERIAL%              ❶
CD\%CSERIAL%
lccustom s:\network.org network.txt    ❷
lccustom s:\owner.org owner.txt
aiawrite userdevice /f=network.txt    ❸
aiawrite ownerdata /f=owner.txt
aiaread userdevice /f=aiaudval.txt    ❹
aiaread ownerdata /f=aiaowner.txt
```

Figure 49. AIAINPUT.LCI

Notes from Figure 49:

❶ The value %CSERIAL% is the value of the serial number of the system unit. We are using it because it is an almost unique value. (Actually the combination of machine type, model and serial number is unique, but the serial number alone is sufficient here.) We create a new directory and do not use the default temporary directory created for each client to prevent it from being deleted at the end of the LCCM processing.

All text files created are put in this directory.

❷ The LCCUSTOM command creates a unique .TXT file based on both the .ORG template file and environment variables that we will enter later in step 3 on page 73.

❸ The AIAWRITE command writes the information in the .TXT file into fields in the specified groups in the Asset ID EEPROM. The groups are named userdevice and ownerdata.

We did not use the group networkconnection. Since there was no field for the domain in the Asset ID specification, we used the loginname field to store the domain name but found that this field was not static. The loginnname field would be repopulated with a different value when LCCM subsequently "touched" the PC.

❹ The AIAREAD command reads the values back from the EEPROM and stores them in the specified .TXT files.

4. You should now have three files in C:\LCCM\CLNTFILE:

   – AIAINPUT.LCI
   – NETWORK.ORG
   – OWNER.ORG

5. Start LCCM if it is not already running.

6. Click **Profile > Create new**.

7. Choose **Manually with the Profile Editor** and then click **OK**.
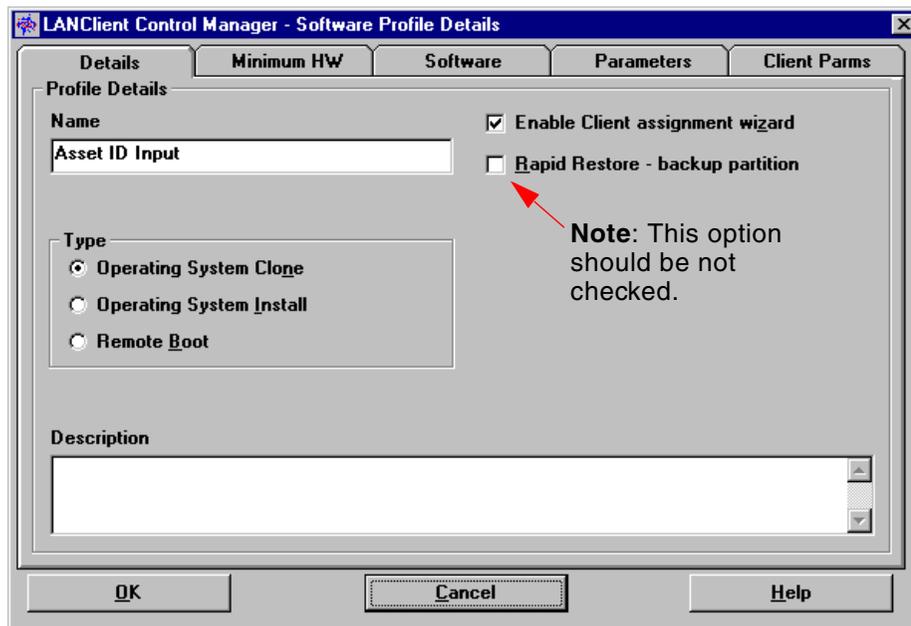
8. Click the **Details** tab.

Figure 50. Asset ID Input Profile Details section

9. Under Name enter the profile name `Asset ID Input` and select the Type as **Operating System Clone**. Ensure that the **Enable Client assignment wizard** is checked. Ensure Rapid Restore option is *not* checked.

10. Click the **Software** tab.

11. Under the **Final Image file name** click the **Browse** button and choose AIAINPUT.LCI and then click **Open**.

12. Leave the Preload Image File field blank.

13. Click the **Client Parms** Tab and enter the following values:

Table 5. Client parameters

Name	Default value	Description
SYSTEMNAME		The network computer name
DOMAIN	ITSO	The Domain this PC and user logs into
OWNERNAME		Who uses this PC
DEPARTMENT		The department of this PC user

14. Click **OK**.

Now that we have a profile to be written to the Asset ID area, we will run a small test to verify it works.

1. Drag and drop one of your clients enabled with Asset ID to **Asset ID Input** profile.

2. You will be prompted by the Client Assignment Wizard. Click **Next**.

3. For each of the following four fields, you will be prompted to enter a value then click **Next**:

    – SYSTEMNAME
    – DOMAIN
    – OWNERNAME
    – DEPARTMENT

    These will be the values populated in the Asset ID area. Click **Finish**.

4. Click **Process**.

5. To verify that the changes are made to the Asset ID area, do the following:

    a. Double-click the client (for example, CLNT1).

    b. Click the **Details** tab. You will see the serial number in one of the fields. In our case it is 238P4YK.

    c. Using Windows NT Explorer, locate the following folder: C:\LCCM\TMPFILES\238P4YK

    d. You will see four or more files in this folder. Open AIAUDVAL.TXT and AIAOWNER.TXT. These were the ones written to by the `AIAREAD` command in Figure 49 on page 70. The contents of these files reflect the data from the Asset ID area after it has been written. If the data matches the data you entered then the test was successful.

    Note: The `AIAREAD` commands in Figure 49 on page 70 perform a dump of all the fields in the groups userdevice and ownerdata, yet we only populated two fields in each group respectively.

We have now verified that we can write to and read from the Asset ID EEPROM. We will be using this later as part of an automated deployment of Windows 2000 Professional as described in 4.1.10, "Deploying the final image" on page 85.

4.1.6 Automating the use of a cloning tool with LCCM

Many of the popular cloning tools such as PowerQuest Drive Image Pro and Norton Ghost require that the installer physically visit the client PC at some point. A common scenario requires the installer to start the PC with a boot diskette (or bootable CD-ROM) that attaches to a network share or local

CD-ROM. The installer then loads the image either from the network or CD. In some cases the process may start immediately. The installer then comes back and custom configures the PC. In all cases, the installer has to physically visit the machine at least once.

With LCCM, a physical presence at the client PC is not required. In this section we describe how to configure LCCM to ghost a machine remotely without the need for local intervention.

In our examples in this section, we are using Norton Ghost. However, the information equally applies to PowerQuest Drive Image Pro. To automate the use of Ghost, we're going to create two profiles:

- A profile to take a ghost image of a system and save it to GHSTCAP.GHO
- A profile to put the ghost image GHSTCAP.GHO onto a client PC.

We use these to easily save the state of a system and easily restore that state if there are problems.

The first step is to create a Ghost directory and share it:

1. On your LCCM server, create a folder called Ghost. We have created one on our C: drive. Make sure you have enough disk space to hold your client images.

2. Make the directory a share of the same name via the folder properties.

3. Copy GHOST.EXE to your shared Ghost directory.

Now we create our first profile to take a ghost image of a system:

1. Create a new text file GHSTCAP.LCI in the C:\LCCM\CLNTFILE directory with the following lines:

```
net use x: \\itsosa8\ghost
x:
ghost -clone,mode=dump,src=1,dst=x:\ghstcap.gho -sure -fx -z9
```

Figure 51. GHSTCAP.LCI

2. Start LCCM.

3. Click **Profile > Create New**.

4. We will choose **Manually with the Profile Notebook** and then click **OK**.

5. Select the **Details** tab. In the Name field, type `Remote Ghost Capture`.

6. Click the **Software** tab.

7. Ensure the field **Pre-load Image file name** is blank.

8. Under **Final Image file name** click the **Browse** button and choose `GHSTCAP.LCI` and then click **Open**.

9. LCCM displays the full UNC path and file name of the image file. Click **OK**.

10. On the main LCCM window you should now see a profile named **Remote Ghost Capture** under OS Clone Profiles.

Next we create a profile to load a ghost image onto a client PC:

1. Create a new text file GHSTDMP.LCI in the C:\LCCM\CLNTFILE directory with the following lines:

```
net use x: \\itsosa8\ghost
x:
ghost -clone,mode=load,src=x:\ghstcap.gho,dst=1,sze1=f -sure -fx
```

Figure 52. GHSTDMP.LCI

2. From LCCM, click **Profile > Create New**.

3. Select **Manually with the Profile Notebook** and then click **OK**.

4. Select the **Details** tab. In the Name field, type `Remote Ghost Clone`.

5. Click the **Software** tab.

6. Ensure the field **Pre-load Image file name** is blank.

7. Under **Final Image file name** click the **Browse** button and choose `GHSTDMP.LCI` and then click **Open**.

8. LCCM displays the full UNC path and file name of the image file. Click **OK**.

These two profiles will make it easy to make and use ghost images.

Note: You can only use one of these profiles at a time and on no more than one client at any time. We could have created these profiles by using variables to set a unique file name for each client so that more than one client can be processed at one time. To simplify the process we did not do this.

4.1.7 Sysprep: preparing the client for cloning

Your designated PC should now be functional with Windows 2000 Professional. In this section we will Sysprep the PC to make it generic. Sysprep is a product provided with Windows 2000 Professional to assist with

deployment. Sysprep and its associated utilities can be found in the DEPLOY.CAB file.

Basically, here is how Sysprep is designed to work:

1. Install Windows 2000 on a donor client.

2. Configure the donor system to your specifications. This may include installing common applications such as Lotus SmartSuite or Microsoft Office. Test your image extensively to ensure everything functions as you planned.

3. Optionally, create a SYSPREP.INF file if you want little-to-no user intervention when you reboot the system after the image is loaded. The SYSPREP.INF file responds to many questions and populates these pieces of information in Windows 2000. If you don't create a SYSPREP.INF, the system will prompt the user for various pieces of information.

   As described in 4.1.9, "Creating the final profile in LCCM" on page 83, we will be automating the creation-unique SYSPREP.INF files for each client as part of our LCCM deployment process.

4. Run SYSPREP.EXE on your donor machine. Sysprep will make the machine generic by stripping machine-unique attributes such as computer name, domain name, SIDs, etc. Sysprep will then shut down the machine.

5. Once the machine is powered off, use a third-party imaging tool such as Norton Ghost or PowerQuest Drive Image Pro to make an image of the operating system in this state.

6. Deploy (clone) this new image to systems that are similar to your donor machine.

7. When the newly cloned machine starts up for the first time, a setup wizard will appear prompting the user for information such as product key, domain name, computer name, etc. If the SYSPREP.INF file exists in C:\SYSPREP, the information is automatically provided for the user.

The SYSPREP.INF file is not unique for each machine, since this is located on the donor machine at the time it is cloned. Microsoft suggests a unique SYSPREP.INF (which may contain a unique computer name, domain name, etc) file on a diskette for each new machine that is to be deployed.

With Asset ID, we can create a unique SYSPREP.INF file locally on the client without the need for a diskette. We can use LCCM to change the generic SYSPREP.INF file remotely and automatically. The information will be extracted from the Asset ID EEPROM, then entered into SYSPREP.INF. The

end result is that the process is automated and does not require a physical visit to each PC.

For more information on Sysprep, see:

`http://www.microsoft.com/windows2000/library/planning/incremental/sysprep.asp`

For the most recent version of Sysprep (Version 1.1 at time of this book) see:

`http://www.microsoft.com/windows2000/downloads/deployment/sysprep/license.asp`

Do the following to prepare the image for cloning:

1. Before beginning, we strongly advise that a snapshot of your current PC and operating system be taken before any changes are made. With the snapshot we can always go back to a known good point in time. We could always do another unattended install to bring us back to this point in time but that unattended install process will take an hour or more where as the clone process takes considerably less time.

   a. Ensure that the targeted client is powered off.

   b. Start LCCM. Drag and drop the client that just had Windows 2000 deployed to it to **Remote Ghost Capture**.

   c. Click **Process**.

   d. The targeted client machine will wake up and the Ghost capture will begin.

   Now that the image is successfully captured, we can experiment and Sysprep our image.

2. Turn on your donor machine (in our case this is CLNT1). Logon as an administrator and then press Enter, since the password is null. (Since we didn't specify a password in our Windows 2000 Professional profile, the password is blank.)

3. Optionally, install any common applications onto the client PC. Refer to 4.2, "Integrating Software Delivery Assistant with Asset ID" on page 87. You may also have to install the appropriate video drivers and audio drivers, because these may not be in the Windows 2000 Professional hardware database. Similarly if you are working on a ThinkPad you may want to install ThinkPad-specific utilities and swap your floppy and CD-ROM or DVD drive so the operating system recognizes it.

4. For Sysprep to work properly you must verify that on the client PC:

   – Your administrator account has a null password.
   – The PC is part of workgroup and not a domain.

These were the settings we chose when we created our profile (in 4.1.3, "Creating a Windows 2000 Professional profile" on page 61) so the settings should be correct.

5. We will use SetupMgr to create the initial SYSPREP.INF file, then we will manually modify it. SetupMgr and the associated files need to be extracted from a CAB file and downloaded from Microsoft:

   a. Create the directory C:\SYSPREP on the client PC.

   b. Locate the DEPLOY.CAB file from your Windows 2000 CD-ROM.

   c. Copy the DEPLOY.CAB file into the SYSPREP folder.

   d. Double click **DEPLOY.CAB**. This should give you a list of the files in the CAB file.

      Note: The SYSPREP.EXE file in DEPLOY.CAB is Version 1.0. We will be downloading Version 1.1 from the Microsoft URL noted previously.

   e. Right-click **SETUPMGR.EXE** and extract this to C:\SYSPREP.

   f. Right-click **SETUPMGX.DLL** and extract this to C:\SYSPREP.

   g. Go to the Microsoft Sysprep download page and obtain the SYSPREP.EXE and SETUPCL.EXE files and copy these to the C:\SYSPREP.

      ```
      http://www.microsoft.com/windows2000/downloads/deployment/sysprep
      /license.asp
      ```

6. Double-click **SETUPMGR.EXE** in the C:\SYSPREP directory.

7. Click **Next**.

8. Click **Next** so we can create a new answer file.

9. Choose **Sysprep Install** and then click **Next**.

10. Click **Next** since we are using Windows 2000 Professional.

11. Choose **Yes** to fully automate the install. Click **Next**.

12. Enter your company name and organization. Click **Next**. We have entered `IBM` and `ITSO`.

13. For computer name, type in `pcsysprep`. Click **Next**.

14. Type in an administrator password. Click **Next**. This will be the local administrator password for this machine.

15. Click **Next**. We will leave the default display settings.

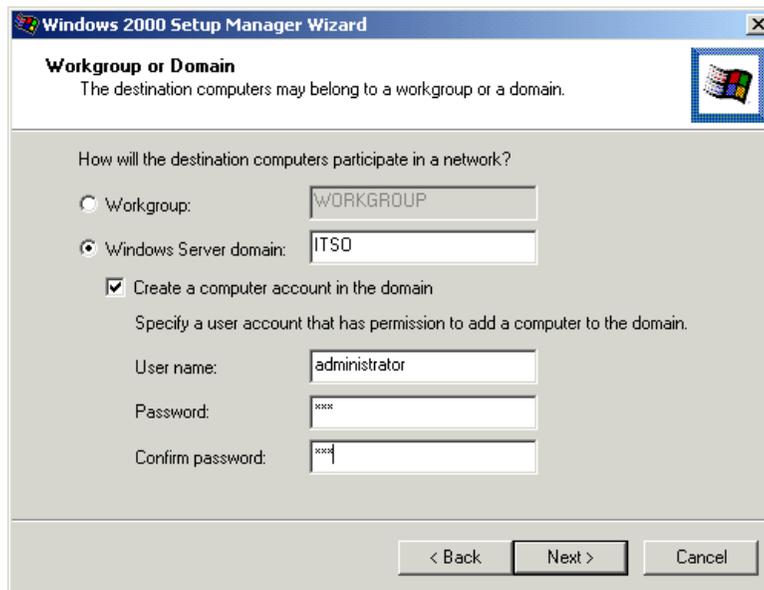16. Click **Next**. We will use the typical network settings.

Figure 53. Setup Manager — creating a computer account on the domain

17. Choose **Windows Server domain** and type your domain name. We used our ITSO domain as shown in Figure 53.

18. Check **Create a computer account in the domain**. Enter the appropriate admin account to create a computer account in the domain. For additional security, you may want to create an account for your domain that only has rights to create computer accounts and use this account here. Click **Next**.

19. Choose the appropriate time zone and click **Next**.

20. Choose **No** to not edit the additional settings. Click **Next.**

21. Choose **Yes** to create or modify the Sysprep folder. Click **Next.**

22. Click **Next**. We will not add any additional commands to run.

23. Click **Next**. We will skip the OEM branding.

24. Click **Next**. We will not use any additional files or folders.

25. You may be asked to specify the location of the SYSPREP.EXE and SETUPCL.EXE files. Point to the C:\SYSPREP directory. Click **Next**.

26. Click **Next**. We will not be using the OEM Duplicator String.

27. Click **Next**. The default location of C:\SYSPREP\SETUP.INF is fine.

28. Click **Finish**.

29. Copy the SETUP.INF file to a floppy as a backup. Note that there are newly created files and folder in the Sysprep folder.

30. Double-click SYSPREP.INF to open the file in Notepad. Edit the file as shown in Figure 54.

Note: If you have installed Windows 2000 from a Microsoft Select CD, you can use `ProductID=string`; otherwise, enter your product key. Please refer to your licensing agreements.

```
[Unattended]
    OemSkipEula=Yes

[GuiUnattended]
    AdminPassword=ibm
    OEMSkipRegional=1
    TimeZone=35
    OemSkipWelcome=1

[UserData]
    FullName=IBM
    OrgName=ITSO
    ComputerName=%FIELD1%
    productid=xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

[Identification]
    JoinDomain=%FIELD2%
    DomainAdmin=administrator
    DomainAdminPassword=ibm

[Networking]
    InstallDefaultComponents=Yes
```

These variables will be replaced at runtime by the values in the Asset ID EEPROM.

Enter your product key here or "string" if you have a Microsoft Select CD.

Figure 54. SYSPREP.INF after changes

31. Once you've made the changes, close Notepad then rename SYSPREP.INF to SYSPREP.ORG.

32. Now we need to delete some unnecessary files. These files and the Sysprep directory will get deleted once the PC is deployed and has been started for the first time. However, we will delete these files as it will make

it easier to determine if a new SYSPREP.INF file is copied over to the Sysprep directory.

Issue the following commands in the Sysprep directory:

```
del setupm*.*
del sysprep.bat
attrib -r deploy.cab
del *.cab
```

33. Move (not copy) the SYSPREP.ORG file from C:\Sysprep to a diskette.

34. At this point, there should be only two files and a subdirectory in C:\Sysprep:

  – I386 [DIR]
  – SYSPREP.EXE
  – SETUPCL.EXE

35. Remove the floppy and label it SYSPREP.ORG.

36. Make any last-minute configurations and close any open windows except your command prompt windows. The state you leave the system is how it will be cloned, so now is the last time you can make these changes.

37. Optionally, if you want an NTFS file system, at the prompt type in:

```
convert c: /fs:ntfs
```

You will be prompted that this will take place on the next reboot. Type in Y and press Enter. If you want to understand the reasoning why we are using this process, refer to Knowledge Base article Q259303, which explains some known bugs with Sysprep and converting to NTFS partitions:

```
http://support.microsoft.com/support/kb/articles/q259/3/03.asp
```

38. We now want to run Sysprep to make the PC generic. Do this by running the following command from C:\SYSPREP:

```
sysprep
```

This command will strip the unique components out of Windows 2000 and shut down the machine.

In our lab we have found that the shutdown was not always graceful when using a IBM PC 300PL Model 6862, 300PL 6565, or NetVista S40 6645. We would receive blue backgrounds with no activity. Ultimately we used Task Manager and the power button to shut down the machine. This

appears to be a bug in Sysprep. We recommend you use the following command instead:

```
sysprep -reboot
```

> ┌─ **Tip** ─
>
> We recommend you shut down the machine and take a ghost image of your client system (using the Remote Ghost Capture profile as described in 4.1.6, "Automating the use of a cloning tool with LCCM" on page 73) just before you run the `sysprep` command.
>
> This way, if the `sysprep` command fails, you can simply use the Remote Ghost Clone profile to reload that same image.

39. Read the next step before continuing with this step. Choose **OK** or press Enter to continue.
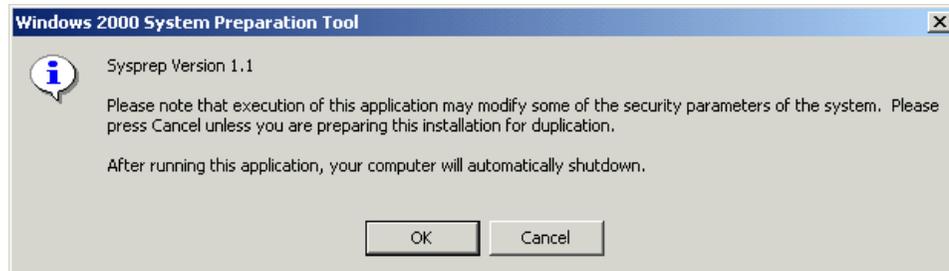
Figure 55. Sysprep warning message

40. **When the machine reboots and you see the Intel boot agent prompt or IBM logo whichever comes first (assuming the prompts are enabled), immediately power off the machine so it does not boot into Windows 2000**.

It is *critical* that the machine not boot back into Windows 2000; otherwise, the Sysprep Mini Setup Wizard will start. If this happens and you did not take a ghost image of the system just before the `sysprep` command, you must go back to step 1 on page 77 and redo these steps.

4.1.8 Creating the ghost image

Now the client PC is ready to be used as a donor for the clone image.

1. The cloning profile we created in LCCM (see 4.1.6, "Automating the use of a cloning tool with LCCM" on page 73) saves the image to GHSTCAP.GHO. Since we want to keep this image, rename it to PRE_SPRP.GHO.

2. Drag and drop the client you have just prepared in 4.1.7, "Sysprep: preparing the client for cloning" on page 75 (in our case it is CLNT1) to the Remote Ghost Capture profile and then click **Process**.

3. Rename GHSTCAP.GHO to W2KGOLD.GHO.

4.1.9 Creating the final profile in LCCM

We now have a ghost image ready to be deployed to clients via an LCCM profile that uses Asset ID, Ghost, and Sysprep.

This profile will remotely deploy the Ghost image, then pull the unique variables out from the Asset ID area on this remote PC, and populate these variables in a SYSPREP.INF file on the PC. When the PC is booted for the first time it will go through an automated configuration without any user intervention.

Now that we have our final image we create an LCCM profile so that it pushes the image to the client and then copies a machine-specific SYSPREP.INF file to that machine.

1. In the C:\LCCM\CLNTFILE directory, make a copy of GHSTDMP.LCI and name it PUSHW2K.LCP.

2. Edit PUSHW2K.LCP with a text editor and change `ghstcap.gho` to `w2kgold.gho`, so that it looks like Figure 56:

```
net use x: \\itsosa8\ghost
x:
ghost -clone,mode=load,src=x:\w2kgold.gho,dst=1,sze1=f -sure -fx
```

Figure 56. PUSHW2K.LCP

3. Create a text file SPRPCSTM.LCI file in the C:\LCCM\CLNTFILE directory to customize SYSPREP.INF on the remote client by pulling out the variables from the Asset ID area. The file should contain:

```
path=s:\;
s:
fat32
T:
CD\
MD %CSERIAL%
CD\%CSERIAL%
aiaread USERDEVICE /S >NETCON.BAT
aiaread OWNERDATA /S >>NETCON.BAT
echo lccustom s:\sysprep.org sysprep.inf >>NETCON.BAT
echo copy sysprep.inf e:\sysprep >>NETCON.BAT
NETCON.BAT
```

Figure 57. SPRPCSTM.LCI - Sysprep customize

Note: E: is the primary active partition on the client system.

4. Copy the SYSPREP.ORG file that was saved on diskette back to the C:\LCCM\CLNTFILE directory.

5. You should now have the following files in C:\LCCM\CLNTFILE:

   – PUSHW2K.LCP
   – SPRPCSTM.LCI
   – SYSPREP.ORG

6. Start LCCM if it is not already running.

7. Click **Profile > Create New**.

8. Select **Manually with the Profile Notebook** then click **OK**.

9. On the Details tab:

   a. In the Name field enter in `W2K with Asset ID Deployment`.
   b. Select **Operating System Clone** under Type.
   c. Ensure the **Enable Client assignment wizard** is checked.

10. Click the **Software** tab.
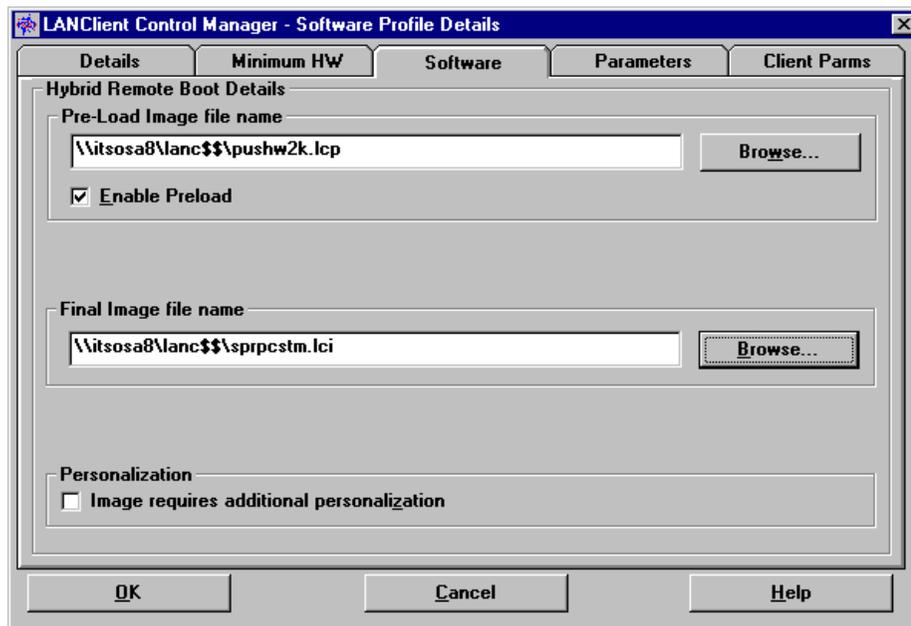
Figure 58. Software profile for W2K with Asset ID deployment

    a. Under Pre-Load Image File Name click **Browse** and select PUSHW2K.LCP and then click **Open**.

    b. Under Final Image file name click **Browse** and choose SPRPCSTM.LCI then click **Open**.

    c. Click **OK**.

> **Tip**
>
> If you want to ensure that only specific hardware can be processed under this file, fill out the hardware prerequisites under the Minimum HW tab.

You should now have a new OS Clone profile titled **W2K with Asset ID Deployment**.

4.1.10 Deploying the final image

Now that we have created the profile, we should test it. For the entire process to work, it is essential that the appropriate Asset ID fields are populated before the final image is deployed.

The key Asset ID fields are:

- FIELD2 — used for domain name
- FIELD1 — used for computer name
- DEPARTMENT - used to identify the group (and applications) for SDA, which will be discussed in 4.2.2, "Building an SDA package" on page 89

The SYSTEMNAME must be different for each system, because you should not have duplicate computer names on the same network. One solution is to use the client PC's serial number as part or all of the computer name. For example if you had a branch office in Hawaii, you could make the unique computer name `HW%CSERIAL%`.

The big advantage of this process is that any subsequent reloads can be all done remotely by dragging and dropping. You no longer need to do any customization on the PC once it is deployed.

To load the fully automated profile onto client PCs, do the following:

1. Drag and drop an Asset ID enabled PC onto the Asset ID Input profile (which we created in 4.1.5, "Writing Asset ID data using LCCM" on page 68).

2. Follow the prompts and enter the appropriate information. You should be asked to provide the following information for each client:

   - Computer Name
   - Domain Name
   - User Name
   - Department Name

   Note: This step is only required for the first time. Entering information into the Asset ID area in this process is not required if you have populated the required Asset ID fields through other methods, such as:

   - RFID solutions provided by QueTel

   - Batch files that include AIAWRITE on a bootable floppy. A process similar to the one we have written for LCCM to remotely write to the Asset ID area could be done with a bootable DOS floppy locally.

   - Installer input at the time of the initial scan. The installer can be prompted for the Asset ID information where it will be populated at that time. This will require you to write a custom application and modify the LCCM scan process.

3. Click **Process**.

4. When the processing has successfully completed, drag and drop the clients from the Asset ID Input profile onto the W2K with Asset ID

Deployment profile (as long as they are from the same product family; see "Tip" on page 85).

Note: You may want to schedule these events to occur after hours.

5. Click **Process**. This is what will occur:

   a. The client(s) wake up and boot to the LCCM server.

   b. Ghost will be started and the Windows 2000 Syspreped image will be pushed down (PUSHW2K.LCP).

   c. The client(s) reboot and again attach to the LCCM server. This time the Asset ID information is read from each client and a SYSPREP.INF file is created based on the Asset ID information and stored on each client. (SPRPCSTM.LCI).

   d. LCCM reboots the client again to verify everything is fine and then remotely powers off the machine.

   e. LCCM indicates that this process has completed by giving a check mark beside each successfully completed client.

6. Now, when a user goes to power on the machine for the first time, the system will run Sysprep with the customized SYSPREP.INF file.

   If you want this process to take place before the user turns on his or her machine, send a wakeup packet to each machine via LCCM to power up the client so that it will boot from the hard drive and start the Sysprep process. This may be a good idea, since it will save the user a few minutes on first boot. In addition, part of the Sysprep process is to create a computer account in the domain (PDC). It is probably best this happen outside of peak hours if many machines are involved.

In summary, the addition of Asset ID to LCCM makes for a much easier deployment of client systems. With Asset ID, you have to enter the user information only once before the first time you load the operating system and applications. On subsequent reloads, the user data is simply extracted from the Asset ID EEPROM by LCCM when required.

4.2 Integrating Software Delivery Assistant with Asset ID

Windows 2000 was developed with systems management in mind. This can be seen with tools built in Windows 2000 such as Sysprep and Active Directory. If Windows 2000 is deployed both on the server side and client side, there really is no need to load applications on the client side on a per machine basis. Windows 2000 servers can either publish or push the

applications via Microsoft Installer (MSI) packages to the desired clients based on group policies.

MSI packages are Windows 2000's version of software distribution. One of the premises behind the MSI packages is that you minimize the number of images you manage. These MSI packages are managed centrally (installed or uninstalled remotely). There is a downside to this model and that is the LAN traffic that occurs when the applications are installed in addition to the extra load on your servers. Some of these problems can be circumvented by scheduling to deploy at off peak hours by using technology enablers such as Wake on LAN.

There are many cases where using MSI packages to push applications down is not a viable solution. These scenarios may include:

- Your client infrastructure is not 100% Windows 2000 Server or Windows 2000 Professional. That is, you have Windows NT 4.0 or Windows 9x clients deployed.
- Remote locations where WAN connections are very slow or non-existent.
- Mobile users who are rarely connected to the LAN.

In some of the above scenarios, LCCM may not be a viable option at all times. IBM Software Delivery Assistant addresses these issues of loading user-specific software while maintaining the minimum number of base images.

In this section, we describe how to integrate Software Delivery Assistant with Asset ID and LCCM where appropriate.

Software Delivery Assistant (SDA) is a product that allows you to minimize the number of images that you have to create. This is accomplished by having a core image such as the base operating systems and possibly some common applications. In addition to this core image, there is an SDA "super" package that includes all the installation code for the various applications for each scenario. The scenarios could include the combinations of different languages, different operating systems, and different departments. Now when you deliver the image, whether it be Windows 2000, Windows NT 4.0 or Windows 95/98, with the SDA package you are assured that the user will receive the correct applications for his or her environment.

SDA can be configured so that the users pick and choose their applications from a menu or where the user picks his or her department where only the applications for that department are installed.

For our example scenario, the value of the Department field in the Asset ID area will determine what predefined set of applications are installed locally on a PC.

For more information about Software Delivery Assistant, see:

`http://www.pc.ibm.com/ww/software/applications/sda/`

4.2.1 Installing Software Delivery Assistant

Software Delivery Assistant can be downloaded from:

`http://www.pc.ibm.com/ww/software/applications/sda/download.html`

Internet Explorer 4.01 or later must be installed on the target machine to run SDA. We are using SDA V1.2, which was the most current version at time of writing.

The procedure to install Software Delivery Assistant is just like any other Windows application. Simply follow the prompts to install the product.

Note: You should be logged on with an account that has local administrative rights.

4.2.2 Building an SDA package

Before building any SDA Package, you must plan the various scenarios and how the SDA package will be used. For example, will the SDA package be used interactively and if so will it be department-based or application-based? Similarly, which applications will be associated with which departments and are there any common applications? Refer to the SDA online documentation for more information.

For our scenario, we will build an SDA package as described in Table 6. To simplify the process, we will assume that we are using only a Windows 2000 client environment. However, SDA can support different WIN32-based operating systems within the same SDA package.

Table 6. Example SDA packages

	IT	Sales	R&D
IBM Director 2.2	Yes	Yes	Yes
Adobe Acrobat 4.0	Yes	Yes	Yes
System Migration Assistant 2.1	Yes		
Microsoft Word Viewer 97	Yes	Yes	

	IT	Sales	R&D
Microsoft Excel Viewer 97		Yes	Yes
Microsoft Power Point Viewer		Yes	

With SDA, you want to eliminate all user intervention if possible. Most applications have an unattended installation process or support silent installs. Applications that do not natively support silent installs can be installed silently if they use InstallShield. If we cannot automate the installation of the programs, then the use of utilities such as Microsoft ScriptIt is required to simulate user clicks. Without this, the installation process will halt requiring user intervention.

4.2.2.1 Creating an automated install for programs

If your program does not natively support silent installs, but does use InstallShield for its installation process, you can create the file SETUP.ISS for this program. As an example, here are the procedures to create a SETUP.ISS file for Adobe Acrobat Reader:

1. Locate a machine that does not have Adobe Acrobat installed.

2. Ensure that you have local administrative privileges.

3. Locate the installation files for Adobe Acrobat Reader 4.0. The file may be one self-extracting file such as AR405ENG.EXE. If this is the case follow these steps:

   a. Double click the single file package. In our case AR405ENG.EXE.
   b. This will start the unpacking of files and will launch the setup program.
   c. Do not continue with the install but instead press Ctrl+Esc to temporarily break out of the installation and bring up the start menu.
   d. Launch Windows Explorer and copy all the installation files to another directory such as c:\acroinst. The temporary installation files are usually found in the c:\Temp directory.
   e. Cancel the installation that was started from the single self-extracting package.

4. Locate the setup file for Acrobat Reader and its location. In our case it is C:\acroinst\setup.exe.

5. From a command line, enter in the following:

   `C:\acroinst\setup.exe -r`

   The `-r` indicates that you want to record the settings chosen for this instance of the installation to the file SETUP.ISS.

6. Choose the items for this manual installation as you normally would.

7. Once the installation process is complete, locate the SETUP.ISS file in the %windir% directory (For Windows NT 4.0 and Windows 2000, this is C:\WINNT by default).

8. Move the SETUP.ISS file to c:\acroinst.

9. For future installations on different machines you can use the command `setup -s` which will now run the installation process unattended. All user responses will be taken from the SETUP.ISS file.

Notes:

- The various Microsoft Office viewers we used natively support silent install with the /q1 switch. We used the viewers for time savings in our lab environment.

- For IBM Director 2.2 we used a custom SETUP.ISS file that installs only the Director client with remote control. Please refer to the SETUP.ISS supplied with Director for more information. Similarly refer to 6.2.2, "The SETUP.ISS file for unattended install" on page 131.

Tips:

- Always use a non-production machine when developing the unattended or silent installs.

- Try the unattended or silent install from a command line first. If the unattended or silent install does not work from a command line, then it will not work from SDA either.

- Test the functionality of the program that has been silently installed.

- Some unattended and silent installs are very path specific. For example, with some versions of Lotus SmartSuite, you have to specify the exact path of the response file. The path of this response file will require changes once the SDA package is created and thus must be modified within the SDA installer package.

4.2.2.2 Creating the SDA Installer package

At this stage you should have already planned how your package will look and tested the silent installs for the applications you are installing. There are two pieces to SDA:

- Administrator console — where the package gets built
- Software installer — the mechanism that installs the software on the client

In this section we will be using the administrator console.

The procedure to build the SDA Installer package is as follows:

1. Create a directory named SDAAPPS. In our case this is D:\SDAAPPS.

2. Copy the installation code for each application into its own subdirectory in D:\SDAAPPS. For example we have the following directories:

   D:\SDAAPPS\acroinst
   D:\SDAAPPS\nf22clnt
   D:\SDAAPPS\smainst
   D:\SDAAPPS\ppview97
   D:\SDAAPPS\wdview97
   D:\SDAAPPS\xlview97

3. Launch the SDA Installer by clicking **Start > Programs > IBM Software Delivery Assistant v1.2**.

4. Select **US English** and click **OK**.

5. Click **Next** at the Welcome window. Figure 59 appears.
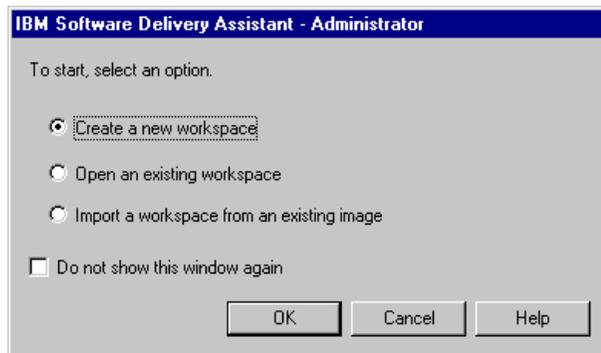
Figure 59. Software Delivery Assistant main window

6. Click **Create a new workspace** and click **OK**. You are now prompted to enter the details for the new workspace.
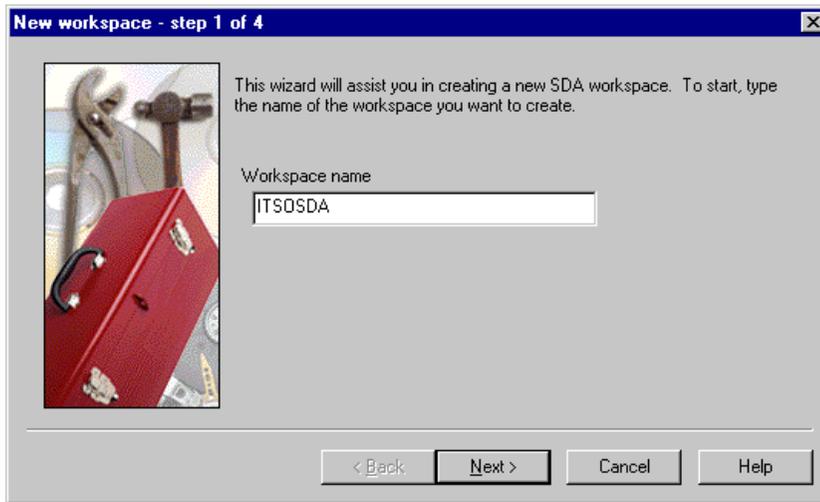
Figure 60. New workspace, step 1

7. Enter the name of your workspace and click **Next**. We used ITSOSDA.
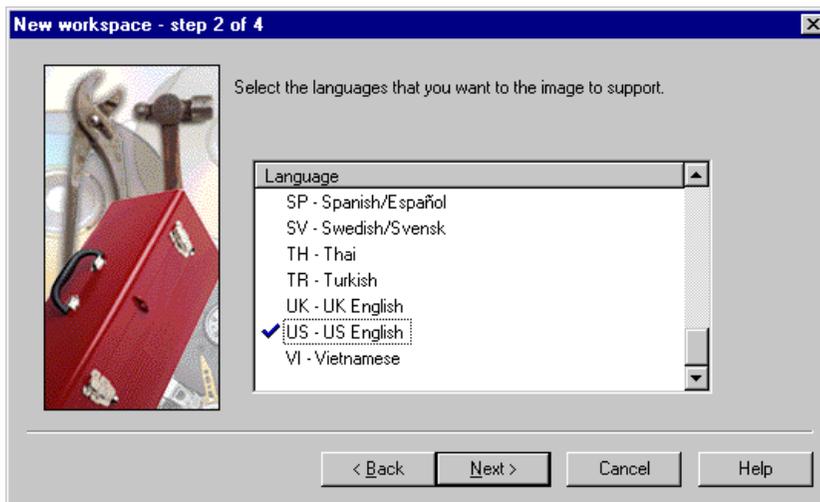
Figure 61. New workspace, step 2

8. Select the languages you want to use. If required, you can select multiple languages. We selected **US English**. Click **Next**.
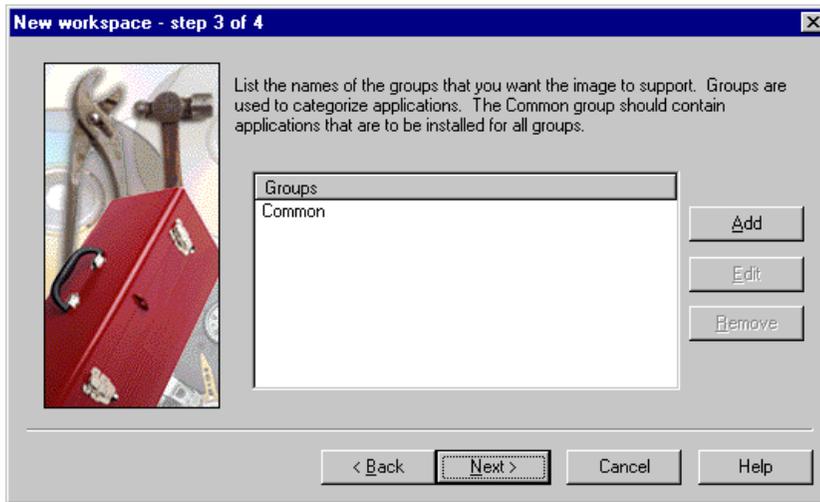
Figure 62. New workspace, step 3

9. Click **Add** and enter three new groups, IT, Sales, and R&D. These correspond to the groups we defined in Table 6 on page 89. Verify that you now have four groups listed: Common, IT, R&D, and Sales. The Common group will contain the applications that are common to all users. Click **Next.**
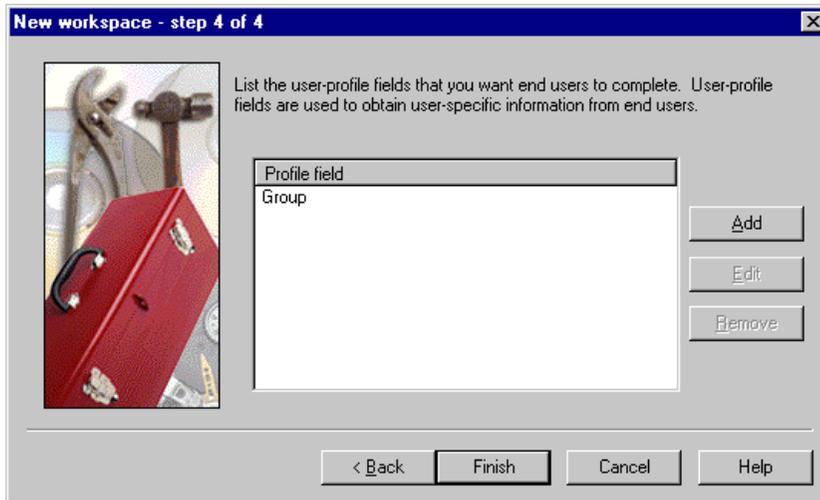
Figure 63. New workspace, step 4

10. Since we only want to prompt the installer for the group name (that is, IT, Sales, or R&D), we don't need to add any other user profile fields. Click **Finish**.

11.The ITSOSDA workspace now appears. Expand the ITSOSDA tree, then expand the US English tree.

Figure 64. New workspace created

12.We are now ready to install applications. You can install applications only within Groups.

We will populate the Common group first with Adobe Acrobat and Director. These are the applications that all three user groups have, as listed in Table 6 on page 89.

13.Select the **Common** group. The right pane now displays application details although at this point no applications are listed.
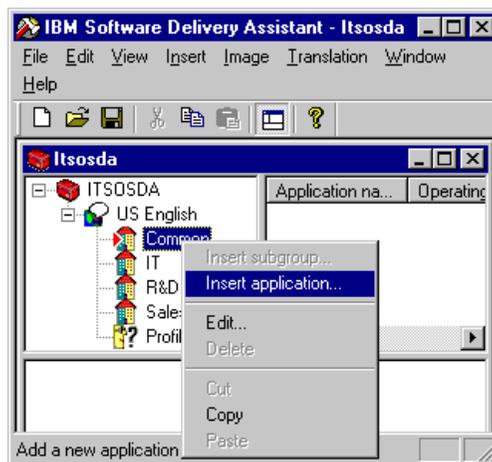
Figure 65. Inserting an application

14.Right click the Common group and click **Insert Application**.
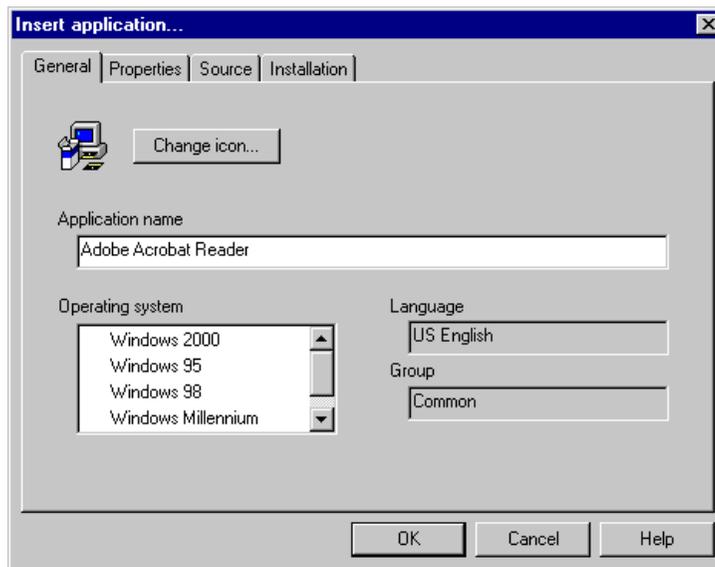
Figure 66. General tab

15.Enter the application name, in our case, Adobe Acrobat Reader.

16.Select all the operating systems that this application can be installed on.

17.Select the **Properties** tab.
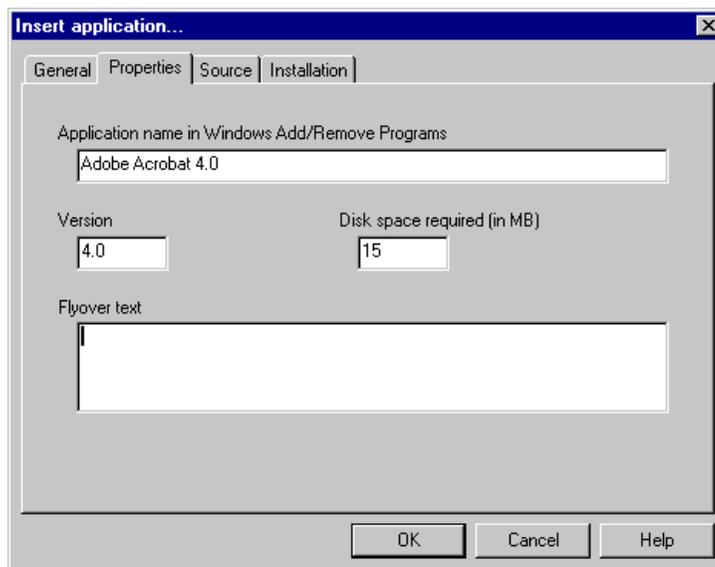
Figure 67. Properties tab

18.In the Application name in Windows Add/Remove Programs field, type in the name of the program as it appears in Add/Remove Programs once the application is installed (refer to your test machine). For our example, it is `Adobe Acrobat 4.0`.

This is very important if you want to use SDA to uninstall your applications. SDA must know exactly how the applications are "labelled" in Add/Remove Programs. However, since we are deleting the SDA installer once at the end of this process, it is not as important in our scenario.

19.In the Version field, enter the version of the software. For our example, it is `4.0`.

20.In the disk space field, enter the amount of disk space the application consumes once it's installed. This value appears if you run SDA manually using the SWSELECT utility and is for informational purposes only.

21.We will leave the Flyover Text box empty. This text is useful if someone will be physically present during the client installation, but since we are automating the process, there will be no one to see it.

22.Select the **Source** tab.
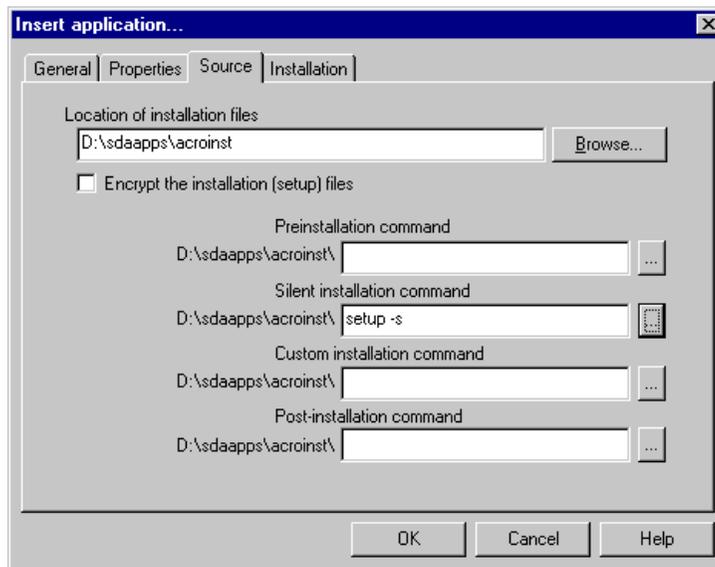
Figure 68. Source tab

23.In the Location of installation files field, enter the location of the installation files. In our case this is `D:\sdaapps\acroinst`.

24.In the Silent installation command field, type `setup -s`. In our example, we'll leave the other fields blank; however, you could use them if the

application needed further customizations (for example, applying a patch or copying of additional files).

25. Select the **Installation** tab.
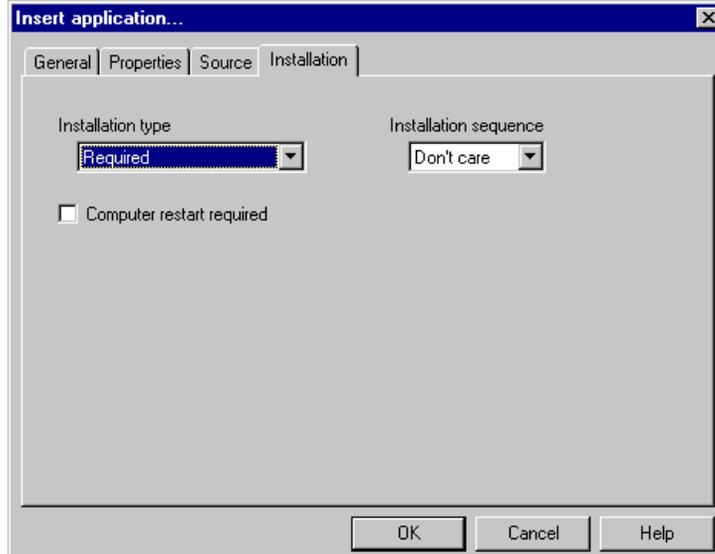
Figure 69. Installation tab

26. Review the installation type options, and leave **Required** as the choice. This means that this application will always be installed for this group. Alternatives include **Recommended**, where the user is prompted if he or she wants the application installed. We select **Required** because there won't be a user present during the installation.

    Do not select **Computer restart required**, since SDA will ask for this anyway based on other options we have chosen (delete image). The computer restart will prompt you only to restart and not actually perform the restart.

    Leave the installation sequence as **Don't care**. Here you can specify if multiple applications are to be installed in a specific order (for example, application X has to be installed before application Y).

27. Click **OK**. There should now be a new entry in the Common group for the application you've just configured:
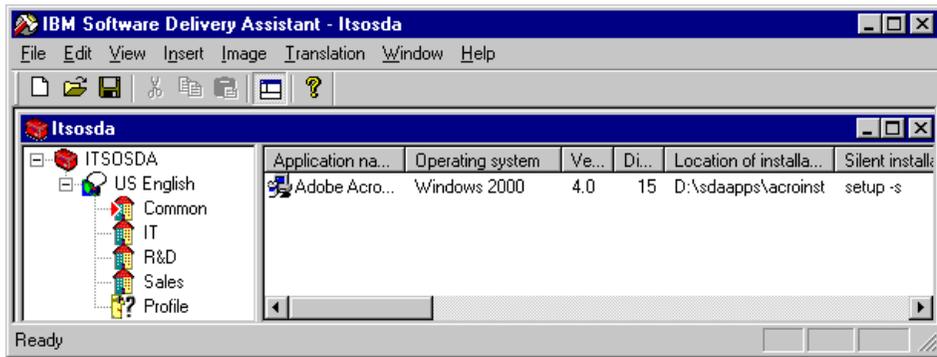
Figure 70. New entry for common group

28. Repeating steps 14 to 27 beginning on page 95, we will add IBM Director 2.2 client to the common group with the values. Ensure the Director SETUP.ISS file does not have the reboot option enabled (verify this by editing the ISS with a text editor).

Table 7. IBM Director installation options

Tab	Field	Value
General	Application name	Director
General	Operating System	Windows 2000
Properties	Application name in Windows Add/Remove Programs	UM Services
Properties	Version	2.2
Properties	Disk space required	40
Source	Location of installation files	D:\sdaapps\nf22clnt\ec
Source	Silent installation command	en\setup -s -sms
Installation	Installation type	Required
Installation	Installation sequence	Don't care
Installation	Computer restart required	leave unchecked

29. Using the same process outlined in the previous step, we populated the IT group with System Migration Assistant and the Word Viewer using these values.

    Tip: You can right-click an application from another group and copy and paste it into another group.
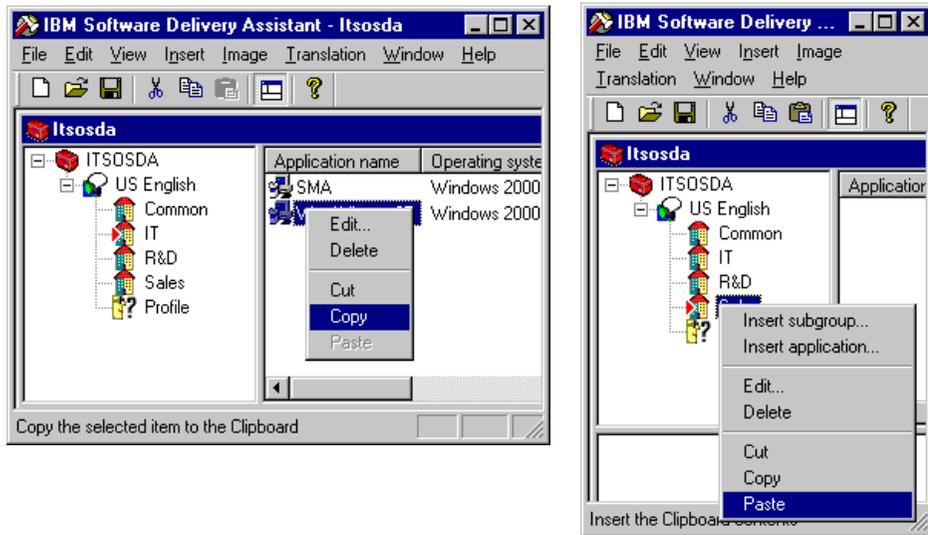
Figure 71. Copying and pasting applications from one group to another

Table 8. SDA values for System Migration Assistant

Tab	Field	Value
General	Application name	SMA
General	Operating System	Windows 2000
Properties	Application name in Windows Add/Remove Programs	IBM System Migration Assistant 2.1
Properties	Version	2.1
Properties	Disk space required	8
Source	Location of installation files	D:\sdaapps\smainst
Source	Silent installation command	setup -s
Installation	Installation type	Required
Installation	Installation sequence	Don't care
Installation	Computer restart required	leave unchecked

Table 9. SDA values for Word Viewer

Tab	Field	Value
General	Application name	Word Viewer 97
General	Operating System	Windows 2000

Tab	Field	Value
Properties	Application name in Windows Add/Remove Programs	Microsoft Word Viewer 97
Properties	Version	97
Properties	Disk space required	6
Source	Location of installation files	D:\sdaapps\wdview97
Source	Silent installation command	setup /q1
Installation	Installation type	Required
Installation	Installation sequence	Don't care
Installation	Computer restart required	leave unchecked

30. We used similar values to populate the Sales (Word, Powerpoint and Excel viewers) and R&D (Excel viewer) groups.

31. Next, we want to change the configuration of the ITSOSDA image so that the installer files are not saved on the user's workstation after installation is complete. Click **Image > Properties**.

32. In the Image tab, click **Remove SDA-Installer from the user's hard disk** then click **OK**.
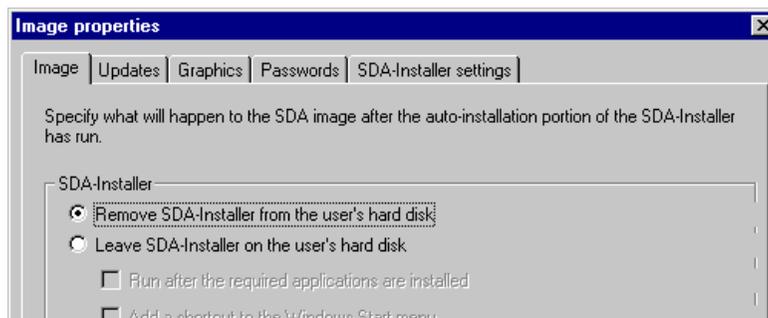
Figure 72. Remove SDA Installer from the user's hard disk

33. Once all the appropriate applications are in their respective groups, the next step is to build the "package" containing all these applications. Click **Image > Build**.

Figure 73. Beginning the image build

34. You will be prompted for the location where you want to save the SDA image. We have chosen D:\sdaapps.
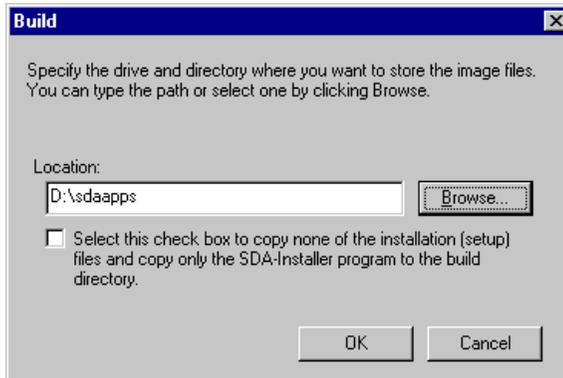
Figure 74. Image build location

35. Click **OK**.

36. The build process now begins. Once it is completed you will see a dialog box. Click **OK**.
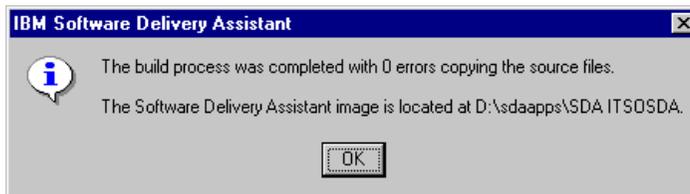
Figure 75. Image build complete

37. Click **File > Save** to save your workspace.

38. In D:\sdaapps (or the directory you entered in Figure 74), a new directory has been created: SDA ITSOSDA. To simplify matters, rename the SDA ITSOSDA folder to ITSOSDA.

39. Create a share point to the SDAAPPS folder.

40. We will now test the SDA package to ensure it works manually. Use LCCM profile Remote Ghost Capture to capture a Windows 2000 Professional installation, as described in 4.1.6, "Automating the use of a cloning tool with LCCM" on page 73. You may have to rename your previous GHSTCAP.GHO file to prevent it from being overwritten.

41. After the LCCM capture is complete, restart the client machine and log into the machine with administrative rights.

42. Copy the ITSOSDA folder from the SDAAPPS share to the test client machine.

43. From the local ITSOSDA folder you just copied, run SWSELECT.EXE file. You will be presented with the following window.
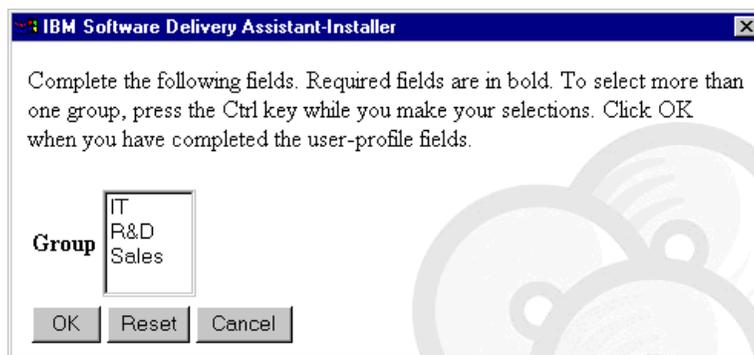
Figure 76. Choosing a group in SDA

44. Select one of the groups and click **OK**. In our example, we selected **Sales**.

45. You will now see SDA installing the applications that apply to the group Sales only.
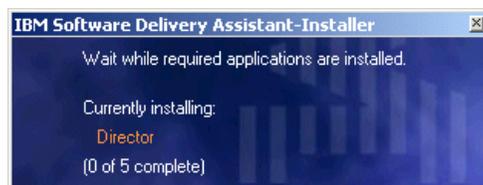
Figure 77. Applications being installed

46. If the Sales group works properly, restore the image you captured in step 40 on page 103 (that is, without any applications installed using SDA).

47. Follow steps 43 to 46 beginning on page 103 and verify that the other groups also work properly.

If everything functions as designed we are now ready to automate the process. If there were errors, you will need to correct these and rebuild the package.

The next step is to incorporate the use of Asset ID to completely automate the process.

4.2.3 Integrating SDA with Asset ID and LCCM

The SDA installer can be started by manually launching the SWSELECT executable or by putting keys in the registry or combinations thereof. In our situation, we want to incorporate Asset ID and pull the department name from there to use as the group name in SDA.

When the Installer is launched it will look for C:\SDAPROF.INI. If this file is found, the SDA installer will automatically install the predefined applications for the group specified in the SDAPROF.INI. We will use LCCM and AIAREAD to pull the department name from the Asset ID area and populate the SDAPROF.INI file with the appropriate department (group).

The procedure to do this is as follows:

1. Create the text file SDAPROF.ORG in C:\LCCM\CLNTFILE\ and add the following lines:

```
[User information]
Group=%DEPARTMENT%
```

> **Error in SDA 1.2 online help**
>
> The online help in SDA V1.2 (search on SDAPROF) indicates a different syntax from that listed above. Our testing has shown that syntax listed there is incorrect and does not work.
>
> The syntax in the SDA2MST.PDF product manual for V1.2 is correct, however, as is the information for SDA V1.1.

2. Make backup copies of SPRPCSTM.LCI and SYSPREP.ORG, both found in C:\LCCM\CLNTFILE.

3. Modify SPRPCSTM.LCI to look like the following. The highlighted lines are the ones to add.

```
path=s:\;
s:
fat32
T:
CD\
MD %CSERIAL%
CD\%CSERIAL%
aiaread NETWORKCONNECTION /S >NETCON.BAT
echo lccustom s:\sysprep.org sysprep.inf >>NETCON.BAT
echo copy sysprep.inf e:\sysprep >>NETCON.BAT
echo lccustom s:\sdaprof.org sdaprof.ini >>NETCON.BAT
echo copy sdaprof.ini e:\ >>NETCON.BAT
NETCON.BAT
```

Figure 78. Modified SPRPCSTM.LCI

4. Modify SYSPREP.ORG to look like the following:

```
[Unattended]
    OemSkipEula=Yes

[GuiUnattended]
    AdminPassword=ibm
    AutoLogon=Yes
    AutoLogonCount=2
    OEMSkipRegional=1
    TimeZone=35
    OemSkipWelcome=1

[UserData]
    FullName=IBM
    OrgName=ITSO
    ComputerName=%FIELD1%
    productid=xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

[Identification]
    JoinDomain=%FIELD2%
    DomainAdmin=administrator
    DomainAdminPassword=ibm

[Networking]
    InstallDefaultComponents=Yes

[GuiRunOnce]
    Command0="c:\itsosda\startsda.bat"
```

Figure 79. Modified SYSPREP.ORG

5. In the above `Command0` line (the last line) we start the batch file STARTSDA. The purpose of this batch file is to start SDA and then reboot the machine. SDA inherently does not have the ability to restart the machine. Create the following file STARTSDA.BAT in D:\SDAAPPS\ITSOSDA.

```
c:\itsosda\swselect.exe
start /low c:\itsosda\scriptit c:\itsosda\close.ini
```

Figure 80. New STARTSDA.BAT

STARTSDA.BAT launches the ScriptIt. ScriptIt is a free unsupported utility provided by Microsoft. It can be downloaded from:

`http://www.microsoft.com/TechNet/winnt/winntas/tools/scriptit.asp`

We chose to delete the files once SDA has installed them (option **Remove SDA-Installer from the user's hard disk** in Figure 72 on page 101). With this option you will be prompted to restart the computer now or at a later time. Since we want to fully automate the process we require the ability to automatically reboot the PC by responding to the prompt — hence the use of ScriptIt.

6. Copy SCRIPTIT.EXE to D:\SDAAPPS\ITSOSDA

7. Create CLOSE.INI (a response file for ScriptIt) in D:\SDAAPPS\ITSOSDA with the following lines of text. Type this line in exactly as it typed here.

   Tip: The last line is case and space sensitive.

```
[SCRIPT]
run=
IBM Software Delivery Assistant-Installer+To complete=~
```

Figure 81. New CLOSE.INI

Notes:

– In Figure 80 on page 106, we used the `start /low` command in STARTSDA.BAT because the ScriptIt utility will use a large proportion of CPU capacity waiting for the SDA reboot window to appear. This window does not appear until all the required applications are installed. We have found it best to keep the ScriptIt utility at the lowest priority preventing possible CPU utilization problems with the application installation process.

– In Figure 81, the last line indicates ScriptIt should look for a window with the title "IBM Software Delivery Assistant-Installer" and the text "To

complete...". Once it finds this window, it simulates pressing Enter to reboot the client.

– In Figure 79 on page 105, the purpose of the [GuiRunOnce] group and the use of STARTSDA.BAT is to automatically install the applications specific to the predefined group and secondly to reboot the machine so that the Director agent can initialize and start so the machine can be discovered. When the Director Server discovers the client, we then know our process has completed successfully.

– Since we are installing the applications while being logged into the client as an administrator, some applications may not put program icons in the All Users folder so that they are available when other users log into this PC. If this is the case with your applications, you may have to create a batch file to copy the contents of those program folders from the Administrator folder to the All Users folder. In Windows 2000, both of these folders are found in the Documents and Settings folder on the client.

– The above process can be further refined by creating two partitions where the SDA Package is copied on the second partition. Ultimately you can manage the operating system partition and the SDA package partition separately. Thus any changes made to the SDA package do not affect the rebuilding of the operating system partition which is key when working with different hardware platforms. You would use a two-partition cloning process to accomplish this.

– Similarly, SDA has features for synchronization with a server if the SDA installer package is left on the system. Refer to the SDA documentation for information.

8. From your donor machine, copy the ITSOSDA folder from the shared resource \\ITSOSDA8\SDAAPPS to your local machine.

9. Follow steps outlined in 4.1.7, "Sysprep: preparing the client for cloning" on page 75 and the steps outlined in 4.1.8, "Creating the ghost image" on page 82.

10. We now should have a Sysprepped ghost image with the SDA installer package on it. We will test this Image and package combination. Again it is crucial that the key Asset ID fields (Field1, Field2 and Department) are correctly populated before we deploy the image.

11. Follow the steps outlined in 4.1.10, "Deploying the final image" on page 85.

12. Once the cloning process completes, the client machine will shut down. This will be indicated by the checkmark beside each client in the LCCM processing window.

At this point if the user turns on the machine it will run through the automated setup wizard and the automated SDA installation. Depending on how many applications are installed, this may take some time. One potential problem with this is that the user may inadvertently intervene in the process causing problems.

To solve this, we propose to wake up the machine so it can run these processes before the user uses the PC for the first time. If the rollout occurs after hours this should not be a problem or if the user is away on lunch, training or out of the office.

13. We now want to power on the machine remotely. There are two ways we can do this:

– Create a text file with the MAC addresses by exporting the LCCM database to simplify the process.

a. From the LCCM menu, click **File > Export > Clients database**. This will export the database to a TXT file.

Figure 82. Saving the LCCM client database

b. Enter a filename and location or just click **Save** to select the defaults.

c. Click **OK** when prompted to create the database.

d. Click **OK** at the prompt indicating success.

e. Use a program such as Lotus 1-2-3 to import the text file and strip everything except the MAC addresses so it looks like Figure 83. Macros will expedite this process, especially if many machines are

involved. This step may not be required if you have used the QueTel Asset TraQ, since it has the ability to create this file for you based on the machines inventoried, as described in 3.2.5, "LCCM Export Utility" on page 43.

```
0004AC6318C4
00062929B10E
0010A4A663A7
```

Figure 83. WAKEUP.TXT

  f. Save the file as WAKEUP.TXT in C:\LCCM.

  g. From the LCCM menu click **Tools > Wake Clients**.

  h. You will be presented with a window. Choose **Text file**, enter
      C:\LCCM\WAKEUP.TXT and click **OK**.
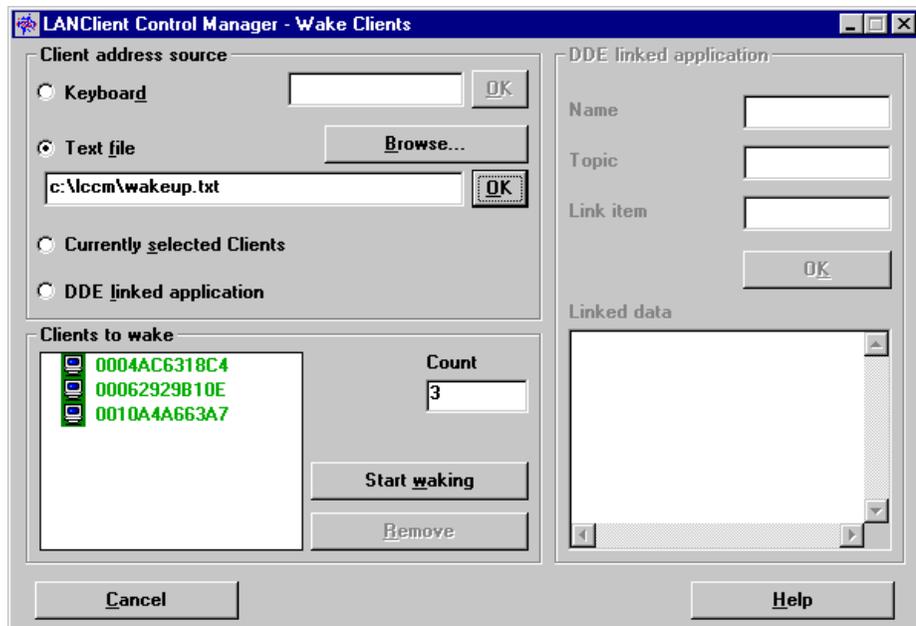
Figure 84. Wake Clients window

  i. Click **Start waking**, wait about 1-2 minutes and then click **Stop
      waking**.

  – Manually type in the MAC address of the PC to wake it up.

    The process is very similar to the one above with the exception that you
    choose **Keyboard** instead of Text File in LCCM. The MAC addresses

for each machine can be found on the Details tab on each client machine as shown in Figure 85.
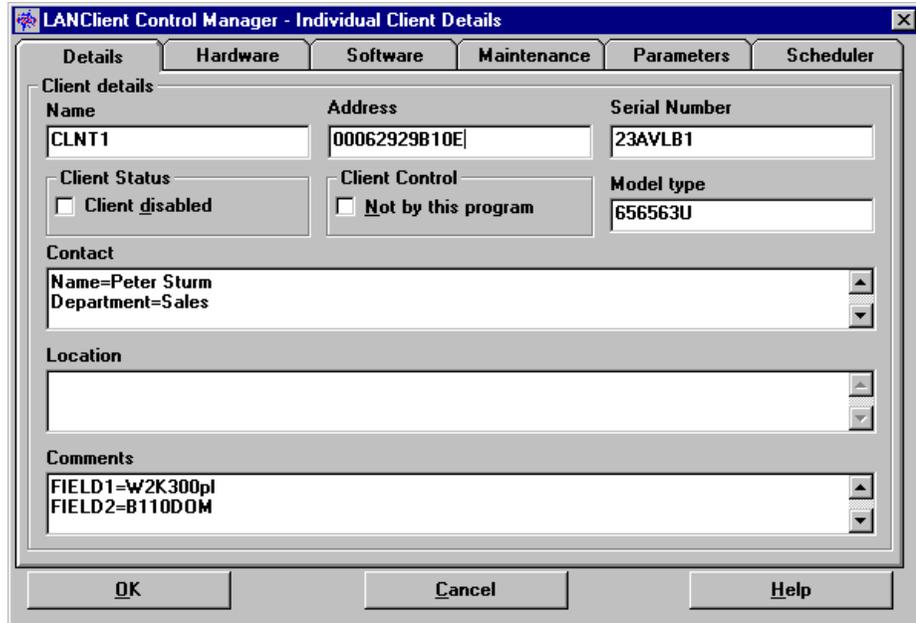
Figure 85. Finding the MAC address manually

14. The client PC will power on and will run through the setup wizard and then reboot and install applications via SDA. It will reboot once more and automatically log on as administrator. We want the machine in this state because an initial logon as administrator is required to properly complete the Director installation.

   Now is an optimum time to discover the Director clients because its agent should now be up and running.

15. Once the Director clients are discovered, use Director to either power off the PCs or restart the PCs so they do not remain logged on as administrator. More importantly, after the restart or power down, the machine will be ready to use by its intended user. You will have to notify the user to log into the domain rather than into the machine locally (which is the default after this reboot or power off) in advance.

   Tip: You may want to create a dynamic group in Director based on lease dates or purchase dates so that only the machines you deployed will be restarted or powered down.

Chapter 5. Integrating with IBM Director

IBM Director (formerly Netfinity Director) is a centralized management tool using industry standard specifications that facilitates the remote management of both servers and clients. Its list of functions is very comprehensive and includes:

- Event monitoring
- Event action plans
- Process management
- Remote control
- Hardware inventory
- Remote hardware configuration
- Dynamic and static grouping

We will be using IBM Director to remotely configure Asset ID and demonstrate how some of the fields in Asset ID can be used.

IBM Director and Netfinity Director

While this chapter refers to IBM Director 2.2, it equally applies to Netfinity Director 2.12. When there are any differences, they are noted.

5.1 Installing IBM Director

For detailed instructions on the installation of IBM Director, refer to Chapter 4 and Chapter 6 of the redbook *Migrating from Netfinity Manager to Netfinity Director*, SG24-6155. In our environment we have the following setup:

Domain: ITSO

PDC:

- Netfinity 5000
- Computer name: ITSOPDC
- IP address 9.9.9.9
- Microsoft DHCP services
- IBM Director Agent 2.2 (UM Services 2.2)

Member server:

- Netfinity 3000
- Computer name: ITSOSA4
- IP address 9.9.9.10

• Netfinity Director Server 2.12

Member server:

• Netfinity 3000
• Computer name: ITSOSA8
• IP Address 9.9.9.11
• IBM Director Server 2.2

Various clients:

• Installed with the Netfinity Director 2.12 and IBM Director 2.2 (UM Services) clients

Note: For this section we are using Netfinity Director 2.12 and pre-release of IBM Director 2.2. The changes in the interface between 2.12 and 2.2 are minimal.

5.2 Netfinity Director 2.12 patch

Netfinity Director 2.12 and earlier have a defect where they do not properly calculate the amount of actual free space available in the Asset ID area. As a result, you are limited to the amount of information you can actually write to the Asset ID EEPROM using Netfinity Director.

The patch, IC28527, is available from:

`http://www.pc.ibm.com/qtechinfo/MIGR-4R4PZ7.html`

You can also go to `http://www.pc.ibm.com/support` and search on "IC28527".

Note: This patch should be installed on all Netfinity Director 2.12 clients, servers and consoles. If you do not install the patch, you will be limited as to how much data you can enter via Netfinity Director.

Without the patch, Netfinity Director 2.12 incorrectly reports that too many characters have been entered.
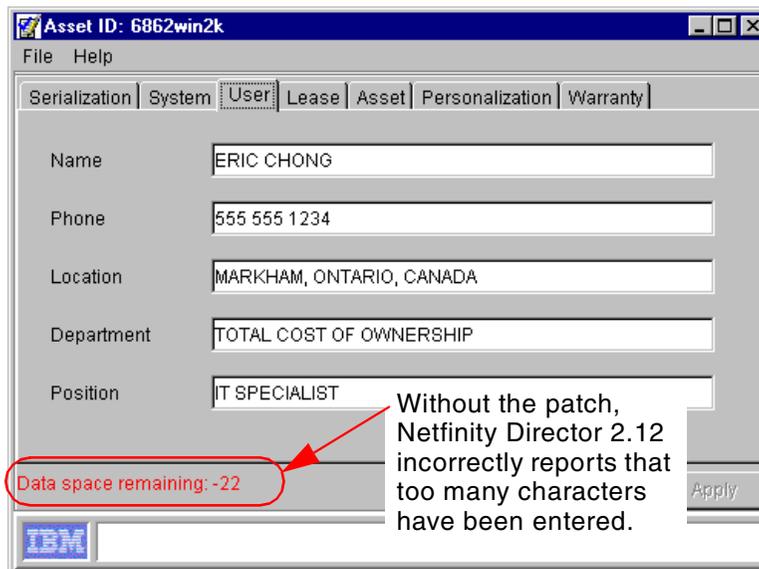
Figure 86. Netfinity Director 2.12 incorrectly reports the amount of free space available

In the Netfinity Director Asset ID window, Figure 86, each time an additional character is typed into a field, the counter at the bottom will indicate the amount of total free space that is available for all the fields.

The defect is that the calculation for the value of `data space remaining` is wrong. The result is that much less data can be entered than should be.

If too much data is entered, this value will turn to red and display a negative sign, as shown in Figure 86. When this occurs, you will be unable to apply any changes you have made, because the **Apply** button will be greyed out.

If the Asset ID EEPROM has been previously populated by other tools such as an RFID solution from QueTel or using AIAWRITE from LCCM, Netfinity Director will show that information in the dialog box. If Netfinity Director calculates that the space has been overcommitted, you will only be able to read the data but you cannot change it unless you delete enough data to make the free space counter positive again.

5.2.1 Installing the patch on Netfinity Director clients

To install the patch on a Netfinity Director 2.12 client, do the following:

1. Log on to the client as a local administrator.
2. Run IC28527.EXE.

3. Specify the directory where you want the fix unpacked to.

4. After unpacking the fix, the text file LC28527.FIX will be displayed using Notepad. This file contains the instructions on how to install the patch. However, at the time of publication, there were errors in the file.

5. Issue the following command to stop the Windows CIM interface:

   ```
   winmgmt /kill
   ```

6. Copy the following two files from the fix installation directory:

   - Copy ASSETCI.DLL to C:\Program Files\IBM\UMS\CI
   - Copy IBMASSTW.DLL to C:\Program Files\IBM\UMS

7. Restart the system.

The patch is designed to be run on each machine with the Netfinity Director 2.12 already installed and running. If, however, you are deploying 2.12 clients as per the procedures in section 6.2 "Unattended installation of UMS" in the redbook *Migrating from Netfinity Manager to Netfinity Director*, SG24-6155, we suggest you take the following steps:

1. Create an unattended install file for the Netfinity Director client using the provided SETUP.ISS file. Ensure that the auto reboot option is not enabled. For more information refer to the SETUP.ISS file and README files.

2. Copy the assetci.dll and ibmasstw.dll file to your share. Copy these files from the share to the local system to replace the old files.

3. Create a batch file that will automatically install Netfinity Director client as per step 1 and then run the batch file in step 2. For Windows 2000 Professional it may look something like the following:

   ```
   net use z: \\server\212clnt
   z:\en\setup -s -sms
   copy z:\en\assetci.dll C:\Program Files\IBM\UMS\CI /Y
   copy z:\en\ibmasstw.dll to C:\Program Files\IBM\UMS /Y
   C:
   net use z: /delete
   ```

4. Use the batch file to run the installation.

Note: You will need local administrative rights for the install and first reboot.

5.2.2 Installing the patch on the Netfinity Director server

To install the patch on your Netfinity Director 2.12 server, do the following:

1. Log on to the server as a local administrator.

2. Run IC28527.EXE.

3. Specify the directory where you want the fix unpacked to.

4. After unpacking the fix, the text file LC28527.FIX will be displayed using Notepad. This file contains the instructions on how to install the patch. However, at the time of publication, there were errors in the file.

5. Copy the following two files from the fix installation directory:

   – Copy ASSET.JAR to C:\Program Files\IBM\Director\clases\nfdjar

   – Copy ASSET.SCRIPT.4 to C:\Program Files\IBM\Director\classes\ cimqueryscripts\asset.script (**Note**: You need to rename the file to ASSET.SCRIPT)

   – Copy ASSETCI.DLL to C:\Program Files\IBM\Director\UMS\CI

   – Copy IBMASSTW.DLL to C:\WINNT\System32

6. Restart the server.

5.3 Asset ID support in IBM Director

IBM Director, like LCCM, writes to and reads from the Asset ID subsystem via the EEPROM's system interface (that is, not via the RF interface).

Because of this, IBM Director works with systems that have the full Asset ID tag (that is, both the EEPROM and the antenna) plus those systems that just have the Asset ID EEPROM but not the antenna (for example, some ThinkPad models normally do not have the antenna installed as standard).

In addition, IBM Director can simulate the functionality of the EEPROM on those systems that do not have Asset ID hardware at all, by reading and writing to a file, ASSETCI.DAT, which is stored in the %WINDIR% directory. On Windows NT and Windows 2000 systems, this is C:\WINNT by default. On Windows 98 systems, this is C:\Windows by default.

Note: Unlike the Asset ID EEPROM, the ASSETCI.DAT file can be erased or the C: drive can be formatted, resulting in all Asset ID data lost from those systems. You should take the necessary backup steps to ensure this data is not lost.

Asset ID is a task in the IBM Director main window:
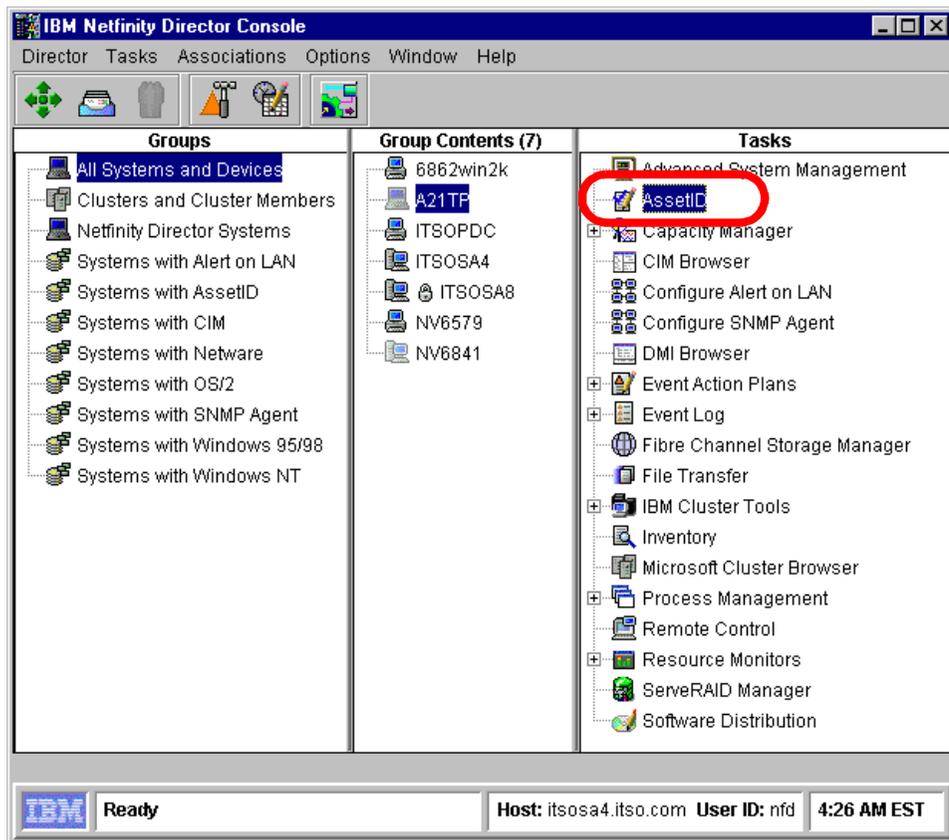
Figure 87. IBM Director/Netfinity Director main window with the Asset ID task

Like other tasks in IBM Director, you can activate Asset ID on a client, in one of two ways:

- Drag the Asset ID task onto the client in the Group Contents panel or vice versa.
- Right-click the client in the Group Contents panel and click **Asset ID** from the drop down menu.

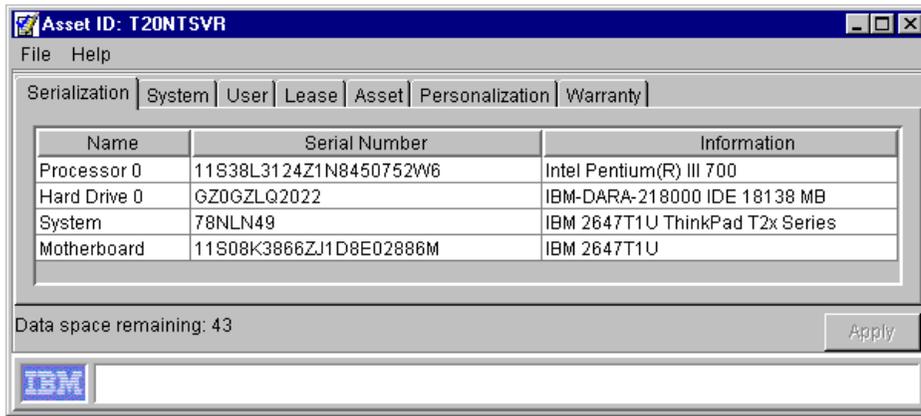**Note**: You cannot drag the task onto multiple systems or a group of systems. The Asset ID task only works on one system at a time.

Figure 88 appears:

Figure 88. Asset ID task

The tabs in this window correspond to the groups in the User area in the EEPROM as described in 2.1.3, "User area" on page 5. The remaining tabs in the window are as follows:
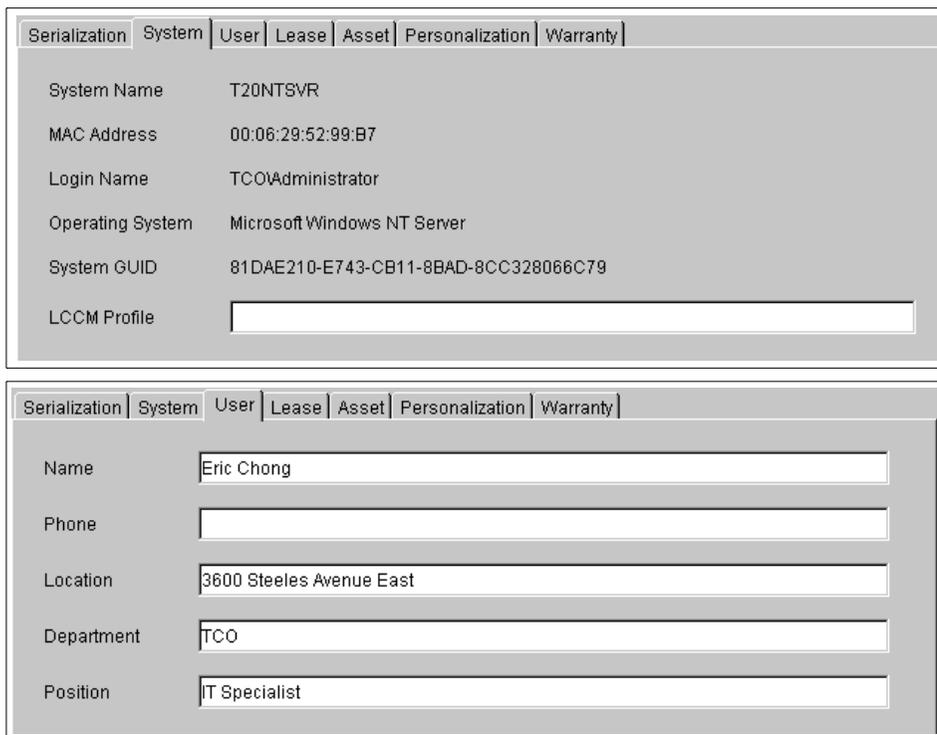
Figure 89. IBM Director Asset ID interface (System and User)

Figure 90. IBM Director Asset ID interface (Lease, Asset, Personalization, and Warranty)

As described at the beginning of 5.3, "Asset ID support in IBM Director" on page 115, a client can support Asset ID in one of three ways:

- Complete, with both the EEPROM and antenna installed
- Partial, with just the EEPROM installed
- Simulated, with neither the EEPROM nor the antenna installed, but IBM Director uses the file ASSETCI.DAT to store the asset data.

To determine what type of Asset ID support a client has, do the following:

- Review the Asset tab in the Asset ID window. If the RFID field has a value (264T1U78NLN49 in Figure 90), then the client has both the Asset ID EEPROM and the Asset ID antenna installed.

- If the Data space remaining field (see Figure 88 on page 117) is less than 200, but there is no RFID value in the Asset tab, then there is only partial Asset ID support (the EEPROM is installed, but not the antenna)

- If the Data space remaining field is greater than 200 (usually close to 1000), then Asset ID support is simulated by IBM Director.

5.4 Reading and writing to Asset ID

The process of reading and writing the Asset ID information to a client using IBM Director is very simple:

1. Open the Asset ID task on the client (right-click the system or drag the task onto the system).

   Note: You can access the Asset ID information only on one client system at a time. You cannot update data to multiple systems at the same time.

2. Click the tab corresponding to the data that you want to read or update. For example, click the **User** tab.
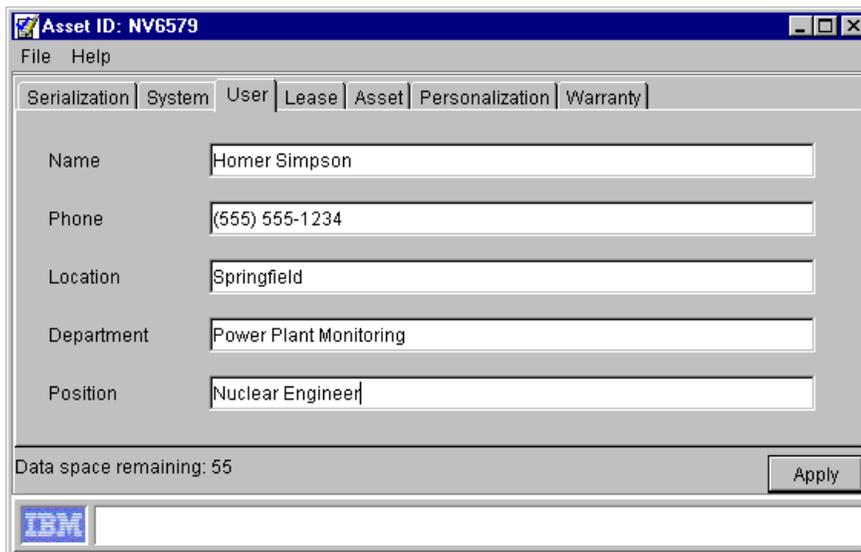
Figure 91. User tab

3. If data was already stored in Asset ID, that data will be displayed. Make any changes you required.

4. While the Data space remaining field remains positive, you can enter more data in other fields and in other tabs. However once you've exceeded the space available, the Apply button will be greyed out until you remove some characters.

5. To save the changes on all tabs, click **Apply**. The information is now written to the EEPROM (or the ASSETCI.DAT file on systems where Asset ID is simulated by Netfinity Director).

    Note: If you close the window without first clicking the Apply button, your changes will *not* be saved. Ensure you click **Apply** before closing.

6. Close the Asset ID window.

5.5 Building a query using Asset ID information

The information stored in Asset ID can be used for various functions. As we have seen in 4.1, "LANClient Control Manager" on page 50 we used Asset ID to rapidly deploy and redeploy Windows 2000 Professional.

As the name indicates, Asset ID is used for identifying assets. Many organizations are now finding leasing beneficial in their environment. However, if you cannot locate your machines or determine when the lease is

due, the benefits of leasing are negated and in fact leasing may become detrimental. Asset ID enhances the process of locating machines and determining when machines leases are due.

In this section, we use the built-in query functions in IBM Director to determine where our PCs are located and when their leases are up.

Note: It is essential that these fields be populated prior to running the query. It doesn't matter whether these fields get populated through LCCM, IBM Director, or an RFID application such as the Asset ID Starter Kit.

In our environment we are using the default database (Microsoft Jet) that ships with IBM Director.

1. Ensure that the IBM Director database has the latest Asset ID information by performing an inventory collection. This should be done before the query is run.

   Updating the inventory can be done in one of two ways:

   – Manually, by right-clicking the group **All Systems and Devices** and clicking **Perform Inventory Collection**. Click **Execute Now** to perform the collection immediately, or **Schedule** to program the collection to occur at a later time. A status window will appear showing the progress of the collection.

     Notes:

     a. If you have many systems, requesting inventory on all of them may cause a heavy load on your network. Consider using the schedule option to run the inventory overnight.

     b. If you have some systems offline, they will return an error in their status in this window.
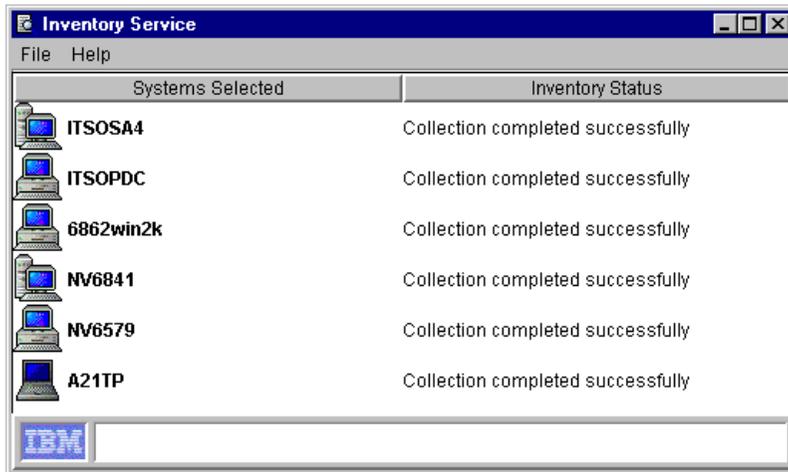
Figure 92. Successful inventory collection

       – Automatically, by configuring an interval to perform regular inventory collections. Click **Options > Server Preferences** then in the Inventory Collection Preferences tab, specify how often (in days) you want inventory collected.
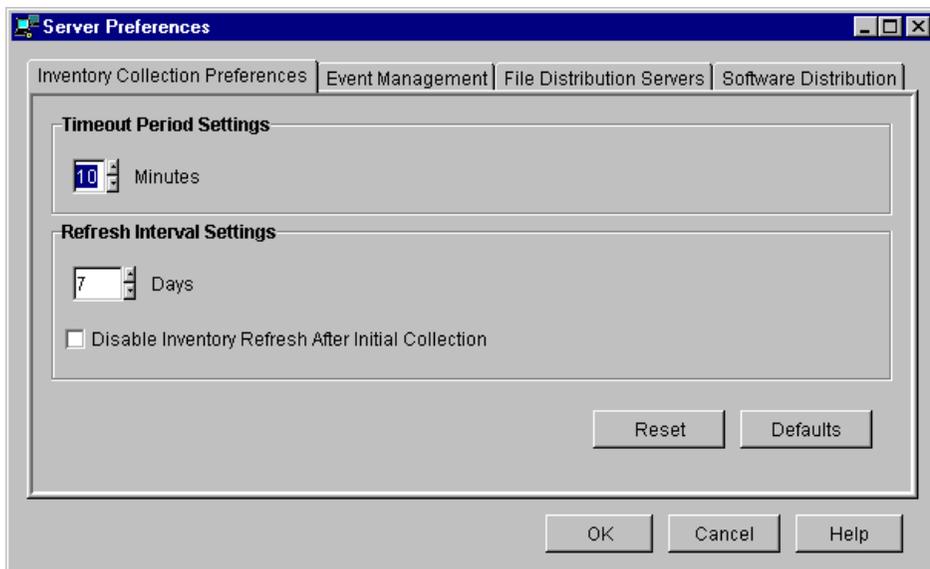

Figure 93. Inventory collection preferences

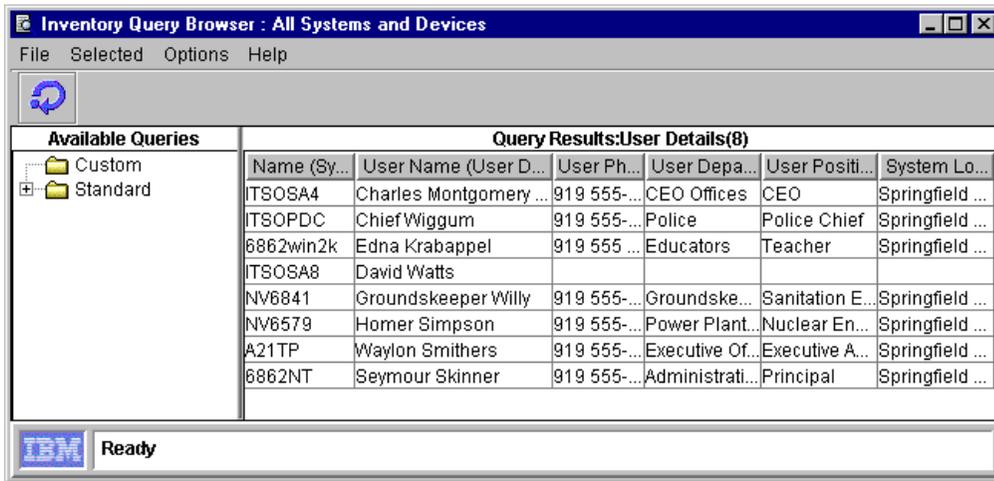2. Double-click **Inventory** from the Tasks panel on the main window of the console.

Figure 94. Netfinity Director Inventory Query Browser

3. Right-click **Custom** from the tree view in the left pane and click **Build Custom Query**. The Inventory Query Builder window appears:
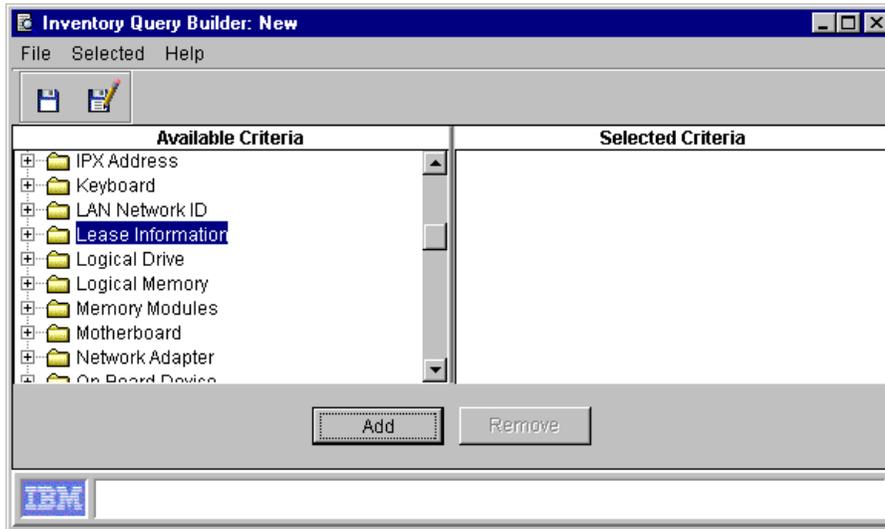
Figure 95. Inventory Query Builder

4. From the Inventory Query Builder window, add the contents from the Lease Information and User Details folders under Available Criteria to the Selected Criteria. To do this, highlight **Lease Information** and click **Add**, then highlight **User Details** and click **Add**.

The Query Builder window should now look as follows:
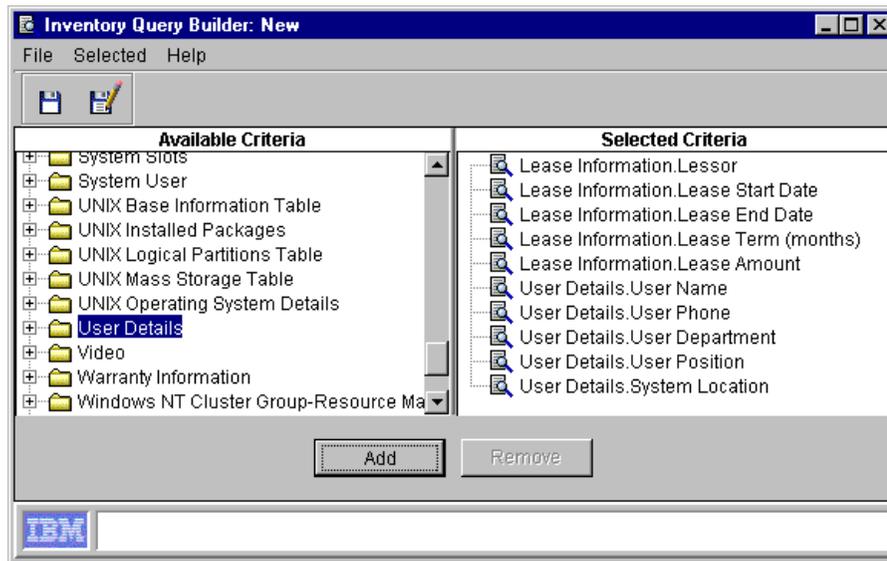
Figure 96. User Details and Lease Information added

5. If you wish, you can change the order of the fields in the Selected Criteria list box. The order you select when the query is saved is the order in which the columns appear when the query is run.

   – To change the order, drag entries to the new location. Dragging item X on top of item Y will make item X appear below item Y.

   – An item can be removed by highlighting it and clicking **Remove**.

   We reordered our example as shown below:
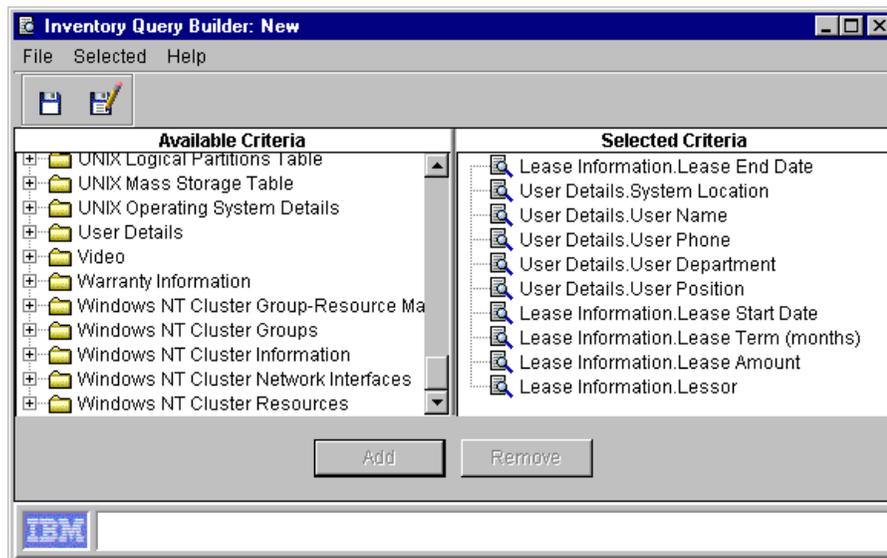
Figure 97. Reordered query

6. Click **File > Save** from the menu or click .

7. You will be prompted for a query name. Enter `Lease data from Asset ID`.
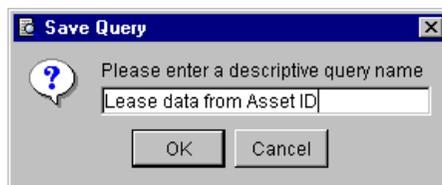

Figure 98. Naming the custom query

8. Click **OK**.

9. Close the Query Builder.

10. Expand the Custom folder in the Inventory Query Browser window. Click the entry named **Lease data from Asset ID**. You custom query will now appears:
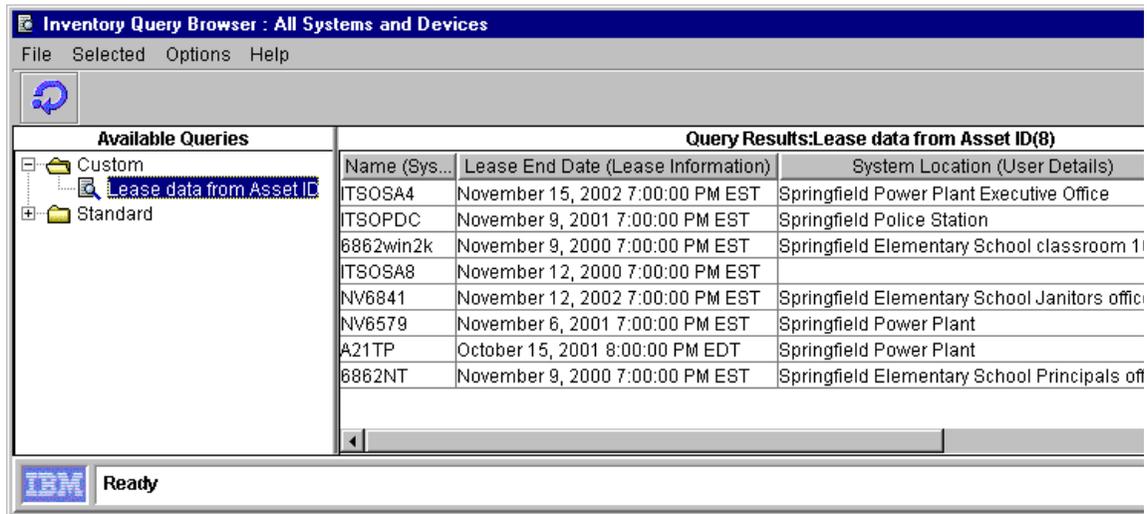
Figure 99. Custom Query Browser

11. With this query view, you can sort the information in ascending or descending order by right-clicking the column and selecting the sort method you want. You can sort the data on any column.

In addition, you can process the report with other tools:

– Export this data to a CSV file using **File > Export > Spreadsheet (.CSV)** and use a spreadsheet application.

– Use the database itself to perform the sorting operations. Since we are using the default Netfinity Director database, Microsoft Jet, we could use Microsoft Access to perform the appropriate sorting and reporting functions. Similarly, if the database is stored in Microsoft SQL Server or IBM DB2, we could use those DBMS applications to analyze the data.

With this report, we can see the following:

• The second column shows the expiration dates for each of the systems. You can sort on this column to show which systems will have leases that expire soon.

• The third column is the system location, which you can use to find where the client PC is located.

Chapter 6. Integrating Asset ID with Tivoli Inventory

Many large organizations already have the Tivoli product set implemented to help them manage their computing environment because it is designed to work in heterogeneous environments and it is highly stable and reliable.

The Tivoli Framework is the core building block. Together with modules such as Tivoli Inventory, they form a Tivoli Managed Environment (TME).

To work with any vendor's systems, the Tivoli products such as Tivoli Inventory normally only retrieve a common core set of attributes, such as memory size, processor speed, etc. However, to maximize the investment in IBM systems, IBM provides a Tivoli Plus Module, a plug-in into Tivoli.

When the Plus Module is used in conjunction with IBM Universal Manageability (UM) Services, it enhances and extends the capabilities of Tivoli products by giving you access to the IBM-specific functions such as Asset ID and Wake on LAN.

In this chapter, we describe the Tivoli Plus Module in terms of Asset ID, how to install the Plus Module and how to use the Plus Module with Asset ID. We are covering only a small subset of the features of the Plus Module. For more information, see the file UM_Services_Plus.PDF file found in the UM Services Plus for Tivoli folder on the Netfinity Director or IBM Director CD-ROM.

6.1 UM Services and Tivoli

The Tivoli Plus Module relies on various components in UM Services to feed the information up to Tivoli products. UM Services can be obtained from either the IBM Director CD or as client code from:

`http://www.pc.ibm.com/ww/software/applications/ums/index.html`

The compressed file may seem quite large at 66 MB for Version 2.12. This is because it includes the upward integration modules for all the various enterprise managers it supports. It is very unlikely that all the UM options will be installed. The footprint on our Windows NT 4.0 6862 was approximately 30 MB (20 MB for UM services + 10 MB for WBEM + very small VM files).

On Windows 2000 systems, the WBEM component is built into the operating system. We will briefly discuss the components that relate to the Tivoli Plus Module. For more information on UM Services please refer to the supplied user manual or:

`http://www.pc.ibm.com/ww/software/applications/ums/index.html`

6.1.1 Base services

The core of UM Services is the base services. Base services provides the underlying enabling capability for both UM Services (and its upward integration to other enterprise managers such as SMS, and Intel LANDesk) and IBM Director. For example, when installed, Base services includes utilities that reads CIM information and creates a static MIF file and modules that add power-off capabilities for Windows NT 4.0. Base services is the absolute minimum required for Tivoli integration with UMS.

6.1.2 Web-based access

The next important piece in UM Services is Web-based access. This allows both local and remote access via a supported Web browser (IE 4.01+ or Netscape 4.5+) to system configuration information such as Asset ID. Note that you will require one of these Web browsers on the Tivoli system you are administering from. UM Services can be used as a peer-to-peer workgroup management tool by itself. To administer the machine locally, open a supported Web browser at `http://localhost:411` where 411 indicates the port address. Similarly, you could type in `http://hostname:411` to access a remote host. In both cases you will be prompted for a user ID and password. The Web-based access is important because it is the interface to change settings on the client whether it be Asset ID or Alert on LAN.

6.1.3 System health monitoring

Although this piece is not used for Asset ID, this option allows for system events to be forwarded to Tivoli. The events may include a chassis intrusion or low disk space.

6.1.4 SNMP access and trap forwarding

This component is not required for Asset ID. This module will allow you to forward alerts via SNMP.

6.2 Installing the Tivoli Plus Module

This section describes how to install the client component of the Tivoli Plus Module. For additional general guidelines, refer to the redbook *Universal Manageablity: Enterprise Management Integration*, SG24-5388. However, there have been a number of updates made to the Tivoli products that may make the details of the installations covered in this redbook inaccurate.

Our Tivoli Environment consists of the following versions of Tivoli produts and associated components outlined in Table 10. We used the Plus Module for

Tivoli from IBM Director 2.2. We used Windows NT 4.0 as our TMR installed with the various modules on the TMR to simplify the install for our environment.

Table 10. Our test suite of products

Product	Version / Patch
Tivoli Framework	3.6.2
Tivoli Inventory	3.6.2
Tivoli Software Distribution	3.6.1
Tivoli Enterprise Console	3.6.2
Tivoli Distributed Monitoring	3.6.2
Microsoft SQL	7.0 with SP2
UM Services Plus for Tivoli	1.3
Plus Module Support	3.1.j

In reality very few TMEs use Windows NT 4.0 as their TMR (Tivoli Management Region) and or have the various modules installed on the TMR. TMRs are usually midrange computers because of their stability and scalability. Below, we briefly describe our Tivoli Management Environment (TME). We have not described how the Tivoli suite is installed, since the installation for each TME differs vastly and can be quite complicated.

Please refer to the UM_Services_Plus.PDF file found in the UM Services Plus for Tivoli folder on the Director CD for installation instructions. However, we will review the installation of an endpoint from scratch with the pieces required for the Plus Module.

Our lab setup is as follows:

Domain: ITSO

- PDC:

    - Netfinity 5000
    - Computer name: ITSOPDC
    - IP address 9.9.9.9
    - Microsoft DHCP Services

- Member server:

    - Netfinity 3000
    - Computer name: ITSOSA4

- IP address 9.9.9.10
- Tivoli Managed Node

- Member server:
  - Netfinity 3000
  - Computer name: ITSOSA8
  - IP Address 9.9.9.11
  - TMR with all the modules installed.
  - SQL 7.0 with Service Pack 2

6.2.1 Installing the client code

There are different scenarios in terms of installation:

1. The Tivoli endpoint is already installed on the client PC.
2. The Tivoli endpoint with UM Services (older version) is already installed and running the Plus Module (older version).
3. UM services is installed but the endpoint is not installed.
4. The Tivoli endpoint and UM services is not installed on the client PC.

In any of the above cases you will require some current enabling UM software on the client in addition to the Tivoli endpoint client, also known as the Light Client Framework (LCF). Also, if you are using UM Services version 2.12 you will need to apply the Asset ID patch to the client PCs or upgrade to a more recent version. The latter will be easier because this can be done remotely.

See 5.2, "Netfinity Director 2.12 patch" on page 112 for information on the Asset ID patch.

6.2.1.1 Installing UM on existing endpoints

If the endpoints exist and software distribution is installed, you would use software distribution to deliver the UM pieces to the endpoints. Instructions are provided for this process in the UM_Services_Plus.PDF file found in the UM Services Plus for Tivoli folder on the Director CD. In fact, the Plus Module provides some objects that facilitate this process.

6.2.1.2 Updating the UM software on Tivoli endpoints

Similar to 6.2.1.1 above, you would use Tivoli software distribution to update the UM software on the endpoints whether you are installing the Asset ID patch for UM Services v2.12 or the latest version of UM Services.

6.2.1.3 Installing the endpoint on systems with UM Services

You would install the endpoint as you normally would in your TME. Once the endpoint is installed, you may need to update your UM services version to a

more current version if applicable. Alternately you could use similar procedures outlined in 6.2.1.4 below but use the update option in the SETUP.ISS file.

6.2.1.4 Installing UM on a new system

Installing the LCF and the required UM components is an easy process because this can be done in one step. The UM / Director client includes an option to install a TME client. We recommend an unattended install at the time of deployment because it provides consistency and requires less user (installer) intervention, which reduces the potential for human error. We could use SDA in our LCCM process (see Chapter 4, "Integration with LCCM and SDA" on page 49) to perform the unattended install. Any UM install requires local administrative rights.

6.2.2 The SETUP.ISS file for unattended install

The SETUP.ISS file is common to the installation of both an existing endpoint and a new installation. However, the items chosen differ somewhat.

Here is the sample SETUP.ISS file from the pre-release version of IBM Director 2.2 we used to install both the UM modules with the Tivoli LCF on a new system. We have added notes (**1**, **2**, etc.) to assist you when deploying the UM Services with or without an existing endpoint. The notes are listed beginning on page 134.

```
[InstallShield Silent]
Version=v3.00.000
File=Response File

[Application]
Name=UMS
Version=2.2
Company=IBM

[DlgOrder]
Dlg0=SdAskOptions-0
Dlg1=AskDestPath-0
Dlg2=AskSecurInfo-0
Count=3

[SdOptionsButtons-0]
Result=103

[SdOptionsButtons-1]
Result=101
```

```
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;               USER CONFIGURABLE SECTION                   ;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;UMS detected on system. Would you like to upgrade? Yes or No
;Available options:
;        1 = Yes
;        0 = No
[UpgradeYesNo]
```
1 `Result=0`

```
;The following is a list of available options. If adding options in the
section below,
;Component-count must be accurately indicated, and all options must be
sequentially numbered,
;starting at zero. Available options: (note: Basic Services cannot be
removed as an option)
;Component-x=0     Director Support
```
2 `;Component-x=1     Web Based Access`
3 `;Component-x=2     System Health Monitoring`
4 `;Component-x=3     Web Based Remote Control`
```
;Component-x=4     LANDesk(TM) Management Suite Integration
```
5 `;Component-x=5     Tivoli Management Agent`
6 `;Component-x=6     SNMP access and trap forwarding`
7 `;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
```
8 `Component-count=3`
9 `Component-0=1`
10 `Component-1=2`
11 `Component-2=5`
12 `Result=1`

```
;installation directory
[AskDestPath-0]
szPath="C:\Program Files\UMS"
Result=1

;username and password for web access
[AskSecurInfo-0]
```
13 `svUser=TivoliPlus`
14 `svPassword=tivoli`

```
      svConfirm=tivoli
15  svPort=411
      Result=1

      ;DMI machine type
      ; Options: 1=Desktop
      ;          2=Mobile
      ;          3=Server
      [DMI]
      DMIType=1

      ;Do you want icons on the start menu?
      [Icons]
16  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=0

      ;Auto Reboot machine when install is finished?
      [AutoReboot]
17  Result=1

      ;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
      [UseIIS]
      Result=1
```

Notes to the SETUP.ISS file:

1 `Result=0`

We have chosen result 0 since we are using this unattended install on a new system. If your system already had a previous version of UM services installed, such as 2.12, you would use option 1 for upgrade.

2 `;Component-x=1     Web Based Access`

This option is necessary if you want the ability to remotely write to the Asset ID area. This is done through a Web browser that is launched on the Tivoli console that remotely reads and writes the information to the client/endpoint. This option uses a bit of additional system overhead on the client system.

3 `;Component-x=2     System Health Monitoring`

This option is not required for Asset ID but is required if you want to use the other functions of the Plus Module, such as receiving alerts from the client even when it is powered off via Alert on LAN technology. This option will also use a bit of additional system overhead on the client side.

4 `;Component-x=3     Web Based Remote Control`

Do not choose this option if you are already using or plan to use Tivoli Remote Control. Similarly, do not choose this option if you are using IBM Director remote control. Lastly, this remote control module is not as secure as the Tivoli or IBM Director remote control because of its Web-based nature.

5 `;Component-x=5     Tivoli Management Agent`

Install this option if you are installing onto a new machine (that is, a machine without the existing Tivoli endpoint software, Tivoli Management Agent). In our testing with the pre-release version of Director 2.2 this option did not overwrite the existing endpoint. However, as a precaution do not choose this option if you have an existing endpoint already installed. The TMA version is 3.6.2 in our pre-release software.

6 `;Component-x=6     SNMP access and trap forwarding`

This option is not required for Asset ID but is required if you want to use the other functions of the Plus Module such as receiving alerts from the client.

7 `;Component-x=7     DMI Support`

Do not use this option. Tivoli Inventory (without the Plus Module) does require DMI support to generate a MIF file. However, UM Services and the Plus Module will generate the MIF file for you without the requirement for DMI. UM services uses the more current CIM standard and writes a

backwards compatible MIF file for Tivoli. This option uses quite a lot of system resources and should be avoided.

8 `Component-count=3`

This denotes that we have chosen three options to install. In our case the options are Web-based access, system health and monitoring, and Tivoli Management Agent.

9 `Component-0=1`

The number 0 represent the first of the three items chosen. The number 1 represents the option for Web-based access

10 `Component-1=2`

The number 1 represents the second of the three items chosen. The number 2 represents the option for System Health and Monitoring.

11 `Component-2=5`

The number 2 represents the third and last of the three items chosen. The number 5 represents the option for Tivoli Management Agent.

12 `Result=1`

Do not change this line.

13 `svUser=TivoliPlus`

This is the User ID you will supply when Web-based access is used. We have chosen TivoliPlus. If you are using the same SETUP.ISS file for your deployment, all your administrative user IDs and passwords for UM Services will be the same. They can, however, be changed after the install and/or new user IDs can be added. The user IDs are case sensitive to provide more security. For ease of management we do suggest a common user ID and password throughout.

14 `svPassword=tivoli`

This is the password associated with the above administrative user ID. The passwords are also case sensitive. We have chosen "tivoli". We suggest you choose a password and user ID that is more secure. Secure the user ID and password just as you would any other administrative password.

15 `svPort=411`

This is the default port the Web-based access communicates through. You will be prompted for this when launching "UM Services" from Tivoli. From an ease of management and consistency standard, the same port should be used throughout.

16 `Result=0`

If we had chosen 1 to put a UM services icon in the start menu, users may click this where the local Web browser will be launched and the user will prompted for a UM services user ID and password (specified in items 13 and 14). It is best to leave this option as 0 to avoid potential problems.

17 `Result=1`

We have chosen to autoreboot the machine when the installation is completed. We have chosen this option just to let us know that it has indeed finished, since this is a silent install. If you are using Tivoli software distribution you want this item to read `Result=0` and let the Tivoli software distribution manage the reboot functions.

6.3 Using the Plus Module with Asset ID

Reading and writing to the Asset ID with the Tivoli Plus Module is very similar to that of IBM Director as discussed in Chapter 5, "Integrating with IBM Director" on page 111. The similarities include:

- Writing to the Asset ID area is performed on a client-by-client basis. You cannot update data to multiple systems at the same time.

- Reading multiple Asset ID entries is possible once the inventory has been collected.

- UM Services (the client side) also simulates Asset ID on non-Asset ID systems. See 5.3, "Asset ID support in IBM Director" on page 115.

- The Web interface reads and writes to Asset ID on a client by client basis and looks and functions almost identicaly to IBM Director.

Depending on the UM components that were installed, you will have different levels of access to the Asset ID information. More specifically, here are the different scenarios assuming you have installed or will install the TMA and the TMR has the prerequisite Tivoli Modules:

- All functions in the Plus Module:

  - Base services
  - Web-based access
  - System health and monitoring
  - SNMP access and trap forwarding

- Asset ID read and write functions:

  - Base services
  - Web-based access

- Asset ID read functions:
  - Base services

Our TME is outlined in 6.2, "Installing the Tivoli Plus Module" on page 128. In addition to this:

- Internet Explorer Version 5 is installed on ITSOSA8 (TMR) and ITSOSA4 (managed node)

- The endpoints have the following UM Service components installed: Base Services, Web-based access and system health and monitoring.
  - We installed UM Services on existing endpoints with both Windows 2000 Professional and Windows NT 4.0 workstation.
  - We installed UM Services with its supplied 3.6.2 TMA on a new Windows 2000 Professional systems.

- Our endpoints are listed in Table 11:

Table 11. Endpoints in our lab environment

Model	Product name	Operating system
2628-G1U	ThinkPad A21	Windows 2000 Professional
6862-R1U	IBM PC 300PL	Windows 2000 Professional
6862-E9U	IBM PC 300PL	Windows NT 4.0 with SP 6a
6841-GAU	NetVista A40P	Windows 2000 Professional

6.3.1 Writing to Asset ID using the Plus Module

Tivoli does not actually write directly to the Asset ID area; instead it uses UM Services to perform this task. However, the UM Services Web browser is launched from Tivoli.

To write to Asset ID:

1. Log on to your machine with local administrative privileges. In our lab, this is ITSOSA4.
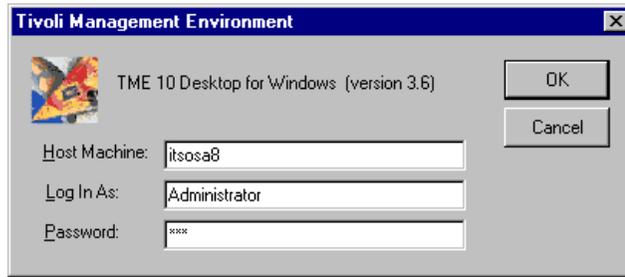
Figure 100. Log on to the TMR

2. Log into your TME Desktop. In our case we are logging in from ITSOSA4 into our TMR ITSOSA8.

Figure 101. Tivoli Desktop

3. Double-click the **TivoliPlus** icon ⬦ on the desktop. Figure 102 appears.
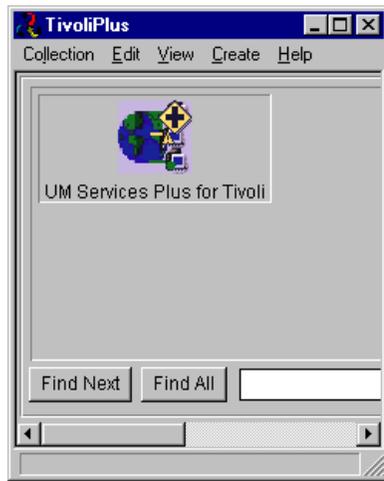
Figure 102. Tivoli Plus window

4. Double-click the **UM Services Plus for Tivoli** icon.
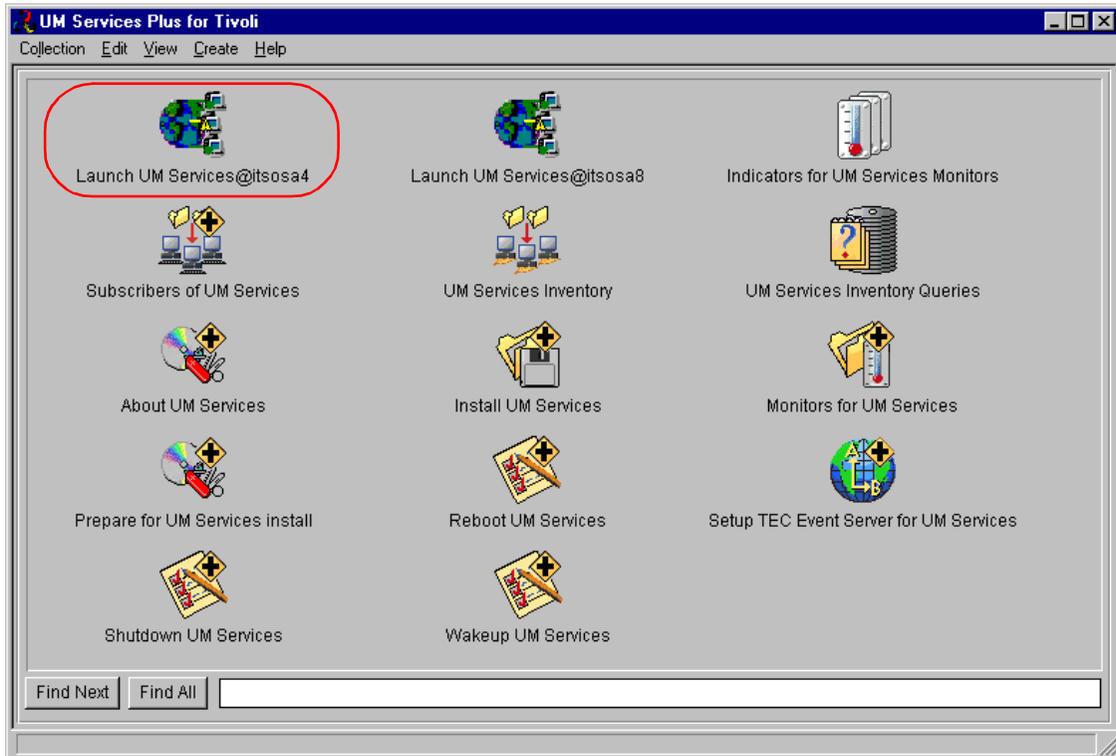
Figure 103. UM Services Plus for Tivoli Desktop (launching UMS on the local machine is highlighted)

5. Next you will double-click the **Launch UM Services** icon for the computer where you're logged on. In our case we are on our managed node ITSOSA4, so we will click the icon ![icon] circled in Figure 103.

6. You are prompted for a hostname and port. In our case we used 6862NT and 411 respectively.
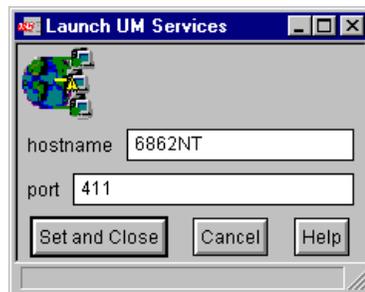
Figure 104. Entering a hostname and port

7. Click **Set and Close**.

   Hint: If you attempt to launch the console on a machine other than yours you will get the following error message at this point:
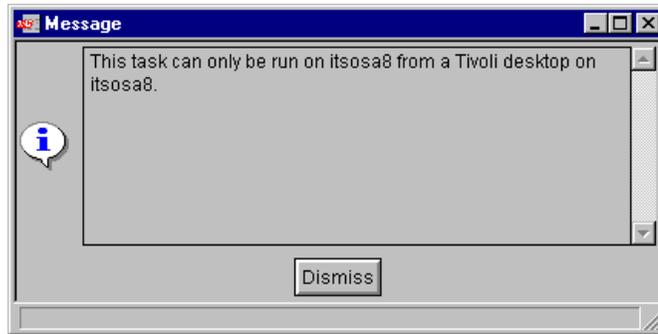
Figure 105. Attempting to launch UM Services from the wrong console

8. If you have started the console on the correct machine, your Web browser will be started.

   Note: You may be prompted to further configure your Web browser depending on which account you logged on with.

9. You will be prompted for a user name and password:

Figure 106. UM Services user ID and password prompt

10. Enter the user name "TivoliPlus" and password "tivoli" that we specified in our SETUP.ISS file (see **13** and **14** on page 132).

   Note: The user ID and password are case sensitive.

11. Click **OK**.

12.If this is the first time you are launching UM services on this machine you
may be prompted to download and install Microsoft Virtual Machine:
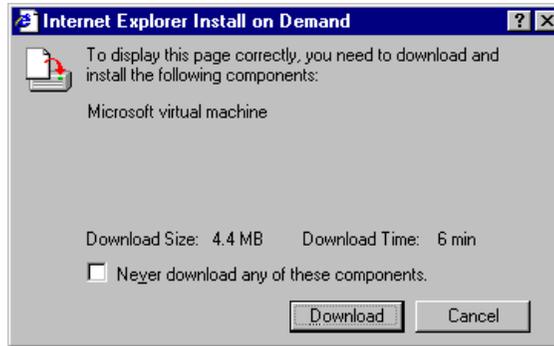
Figure 107. Virtual Machine download

13.Click **Download**.

Note: If you did not log into the system with local administrative privileges
you may receive the following error.
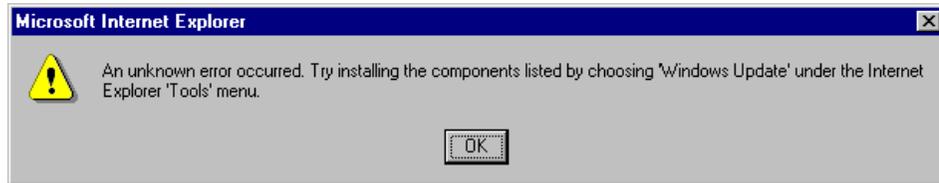
Figure 108. Virtual Machine download error

14.Once the download and installation completes, you will be prompted to
download and install Swing/JFC support.
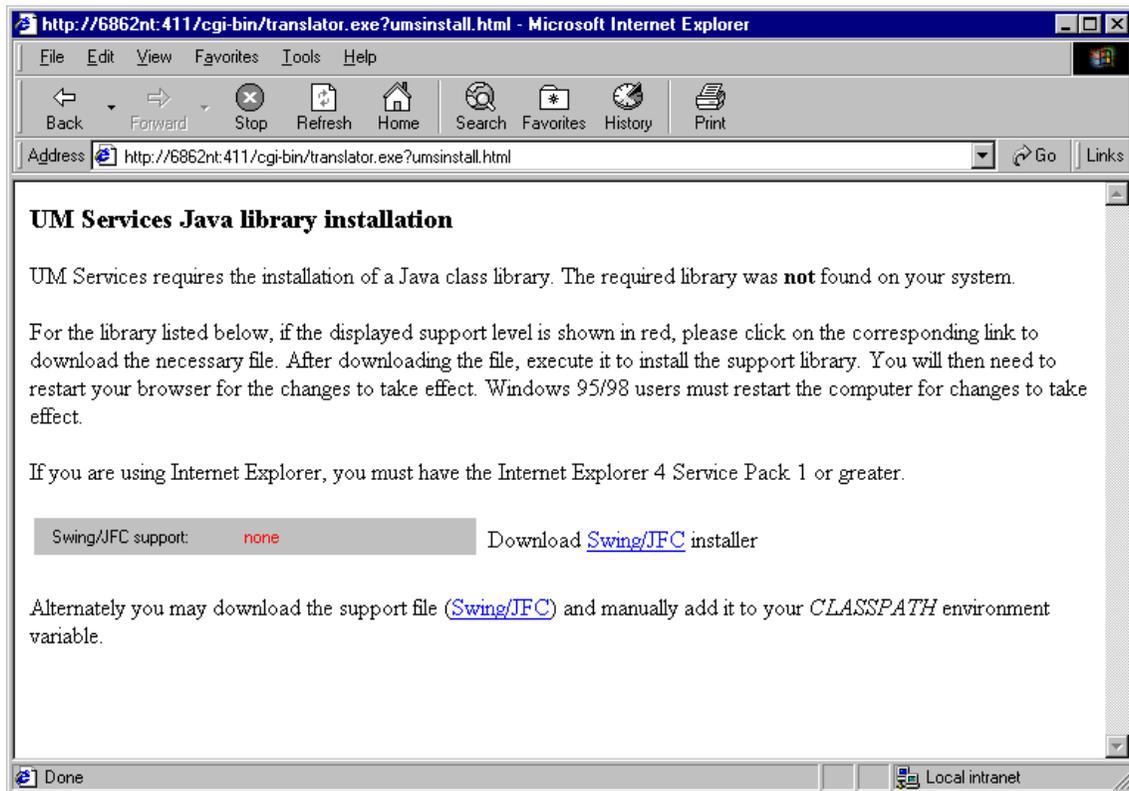
Figure 109. Swing/JFC installation

15. Follow the instructions in the window to install these components.

16. Once the installation is complete, you should see the UM Services main window in your Web browser:
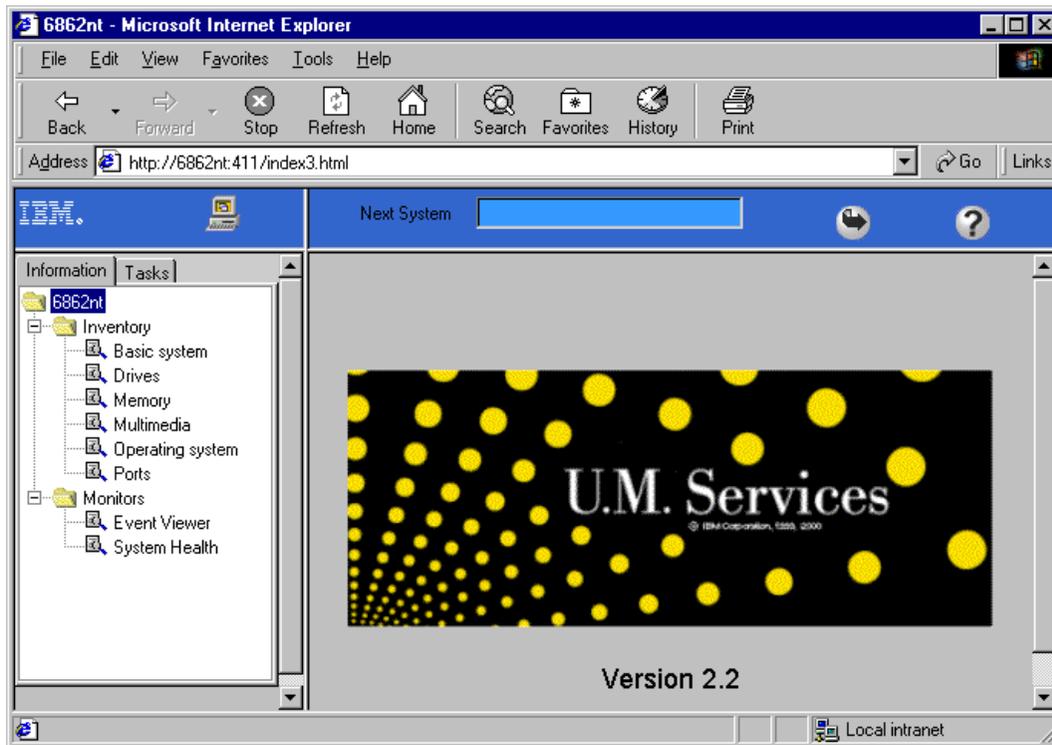
Figure 110. UM Services Browser main window

17. Click the **Tasks** tab in the left-hand pane.

18. Click the **Asset ID** option in the Tasks window. Figure 111 appears.
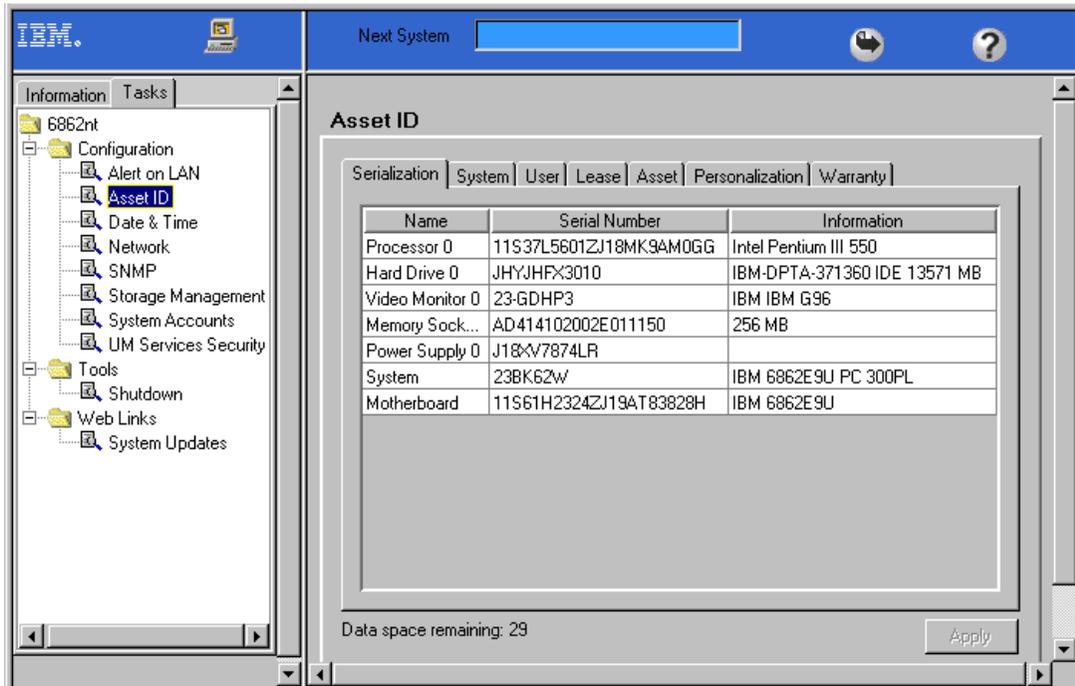
Figure 111. Asset ID window in UM Services browser

19. From this point, viewing and changing the Asset ID information is the same as in IBM Director as described in 5.3, "Asset ID support in IBM Director" on page 115 and 5.4, "Reading and writing to Asset ID" on page 119.

20. Make the changes to the Asset ID you want. For a listing of all the available tabs refer to Figures 88-90 on pages 117-118. For example, click the **User** tab and change the data in the fields there:
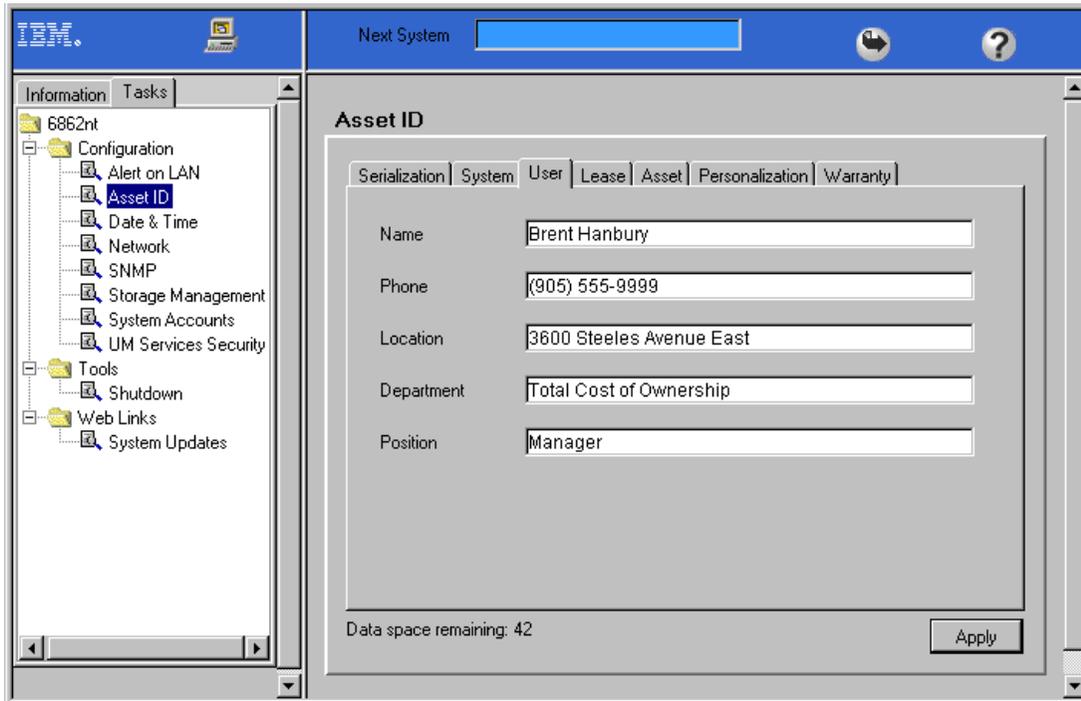
Figure 112. Changes in the User fields

21.Click **Apply** to save the changes, then close the browser.

Tips:

- These changes will not be reflected in the **Inventory** option (Figure 110 on page 144) until the next inventory collection. Similarly, any changes made to the Asset ID area including those made through RFID and LCCM's AIAWRITE interfaces will not be reflected until the next inventory collection.

- You can use the **Launch UM Services** icon to launch any system with UM Services with Web-based access installed even if it doesn't have a TMA installed.

- If using UM Services V2.12 you will require the Asset ID patch or an upgrade to a more current version of UM Services. See 5.2, "Netfinity Director 2.12 patch" on page 112 for instructions.

6.3.2 Viewing UM Services inventory

In 6.3.1, "Writing to Asset ID using the Plus Module" on page 137 we were able to write and read the Asset ID information from each client on a client-to-client basis. In most cases, however, you would want to view multiple pieces of information at one time. The Plus Module facilitates the process by providing objects to perform most of the work.

6.3.2.1 Adding subscribers to UM Services

A subscriber is an object that can be associated with a task in Tivoli. You need to specify subscribers (use existing ones or define new ones) before you can perform the operation.

We will add the subscribers to the Subscribers of UM Services object in case this has not already been done. This is not required for Asset ID but it does simplify the process for other Plus Module functions.

1. Log on to Window.

2. Log into your Tivoli desktop.

3. Open the UM Services Plus for Tivoli Desktop as shown in Figure 103 on page 140.

4. Right-click the **Subscribers of UM Services Object** and click **Subscribers**.
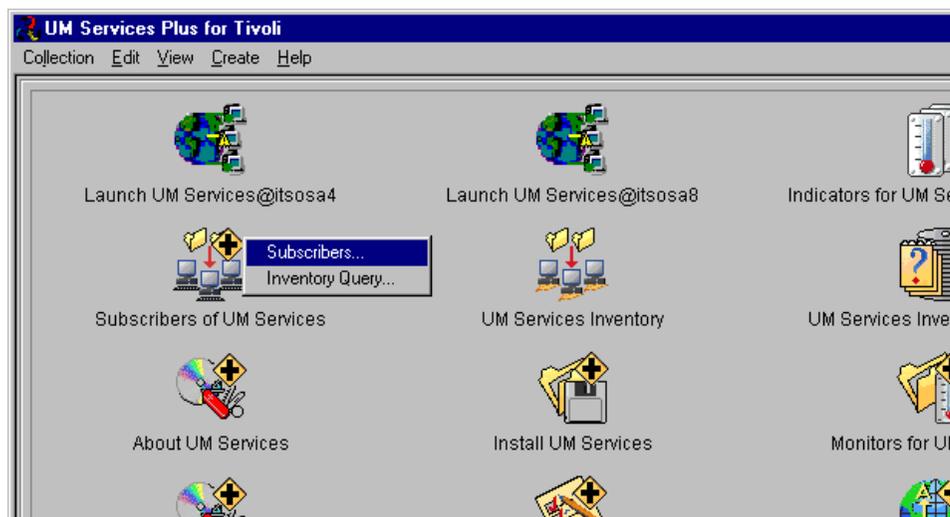
Figure 113. Subscribers of UM Services

5. In the Available to become Subscribers list box on the right, select the appropriate endpoints and click ◀. In our case we have chosen the endpoints: 6862nt, 6862win2k, NV6841, a21tp and itsosa4 as shown in Figure 114:
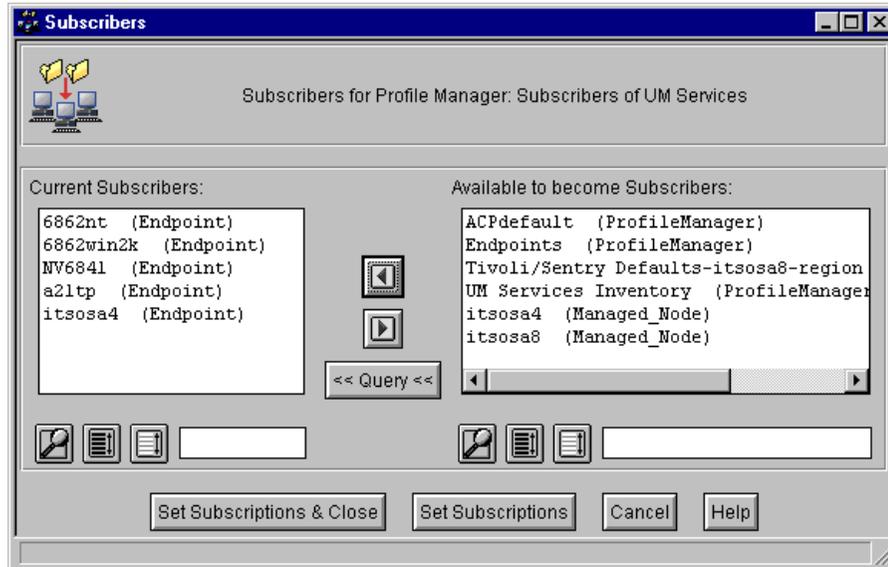
Figure 114. Adding endpoints to subscribers of UM Services

6. Once your endpoints have been added, click **Set Subscriptions & Close**.

6.3.2.2 Adding subscribers and initial database population
We will add our clients (subscribers) to the UM Services Inventory and then populate our Microsoft SQL Server database.
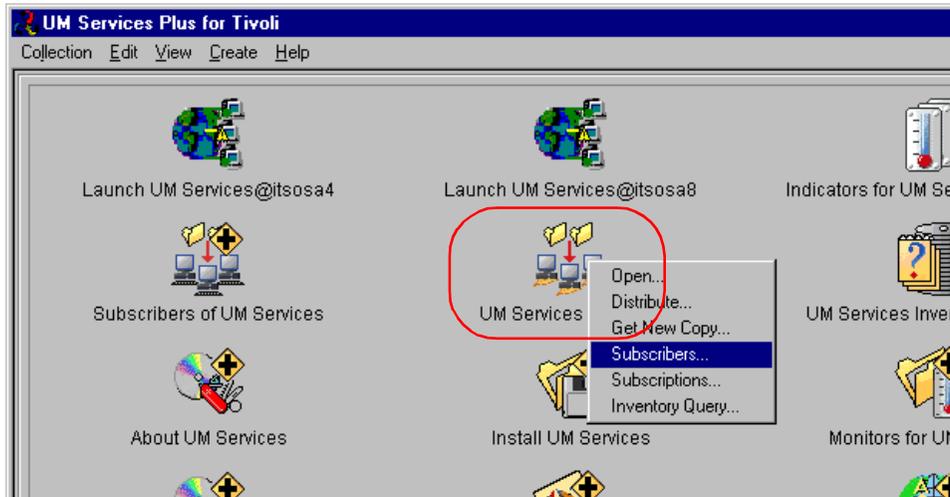
Figure 115. Add subscribers to UM Services Inventory

1. Right-click **UM Services Inventory** and click **Subscribers**.
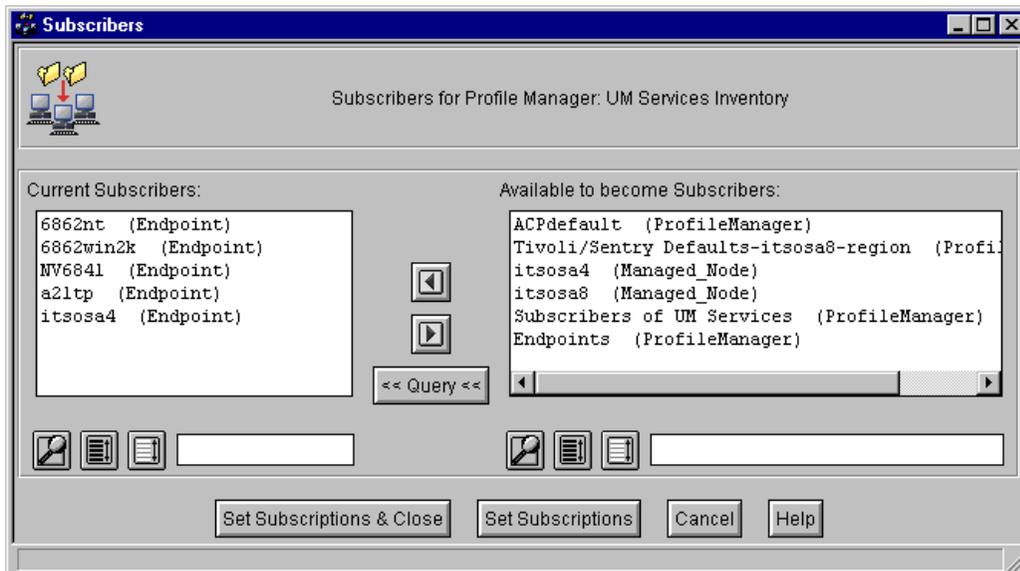
Figure 116. Adding subscribers to UM Services Inventory

2. Select **Subscribers of UM Services (Profile Manager)** from the right listbox and click ◀ to insert it into the Current Subscribers listbox. In our

case we have chosen the endpoints: 6862nt, 6862win2k,NV6841, a21tp and itsosa4.

3. Click **Set Subscriptions & Close**.

4. Double-click **UM Services Inventory** from the main window (Figure 115 on page 149).
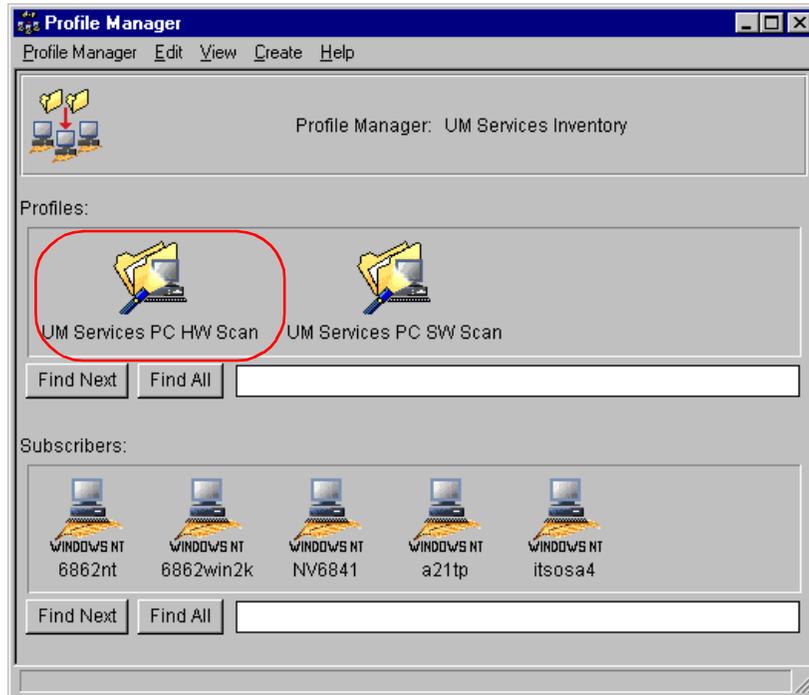
Figure 117. UM Services Inventory main window

5. Right-click **UM Services PC H/W Scan** and click **Discover**.
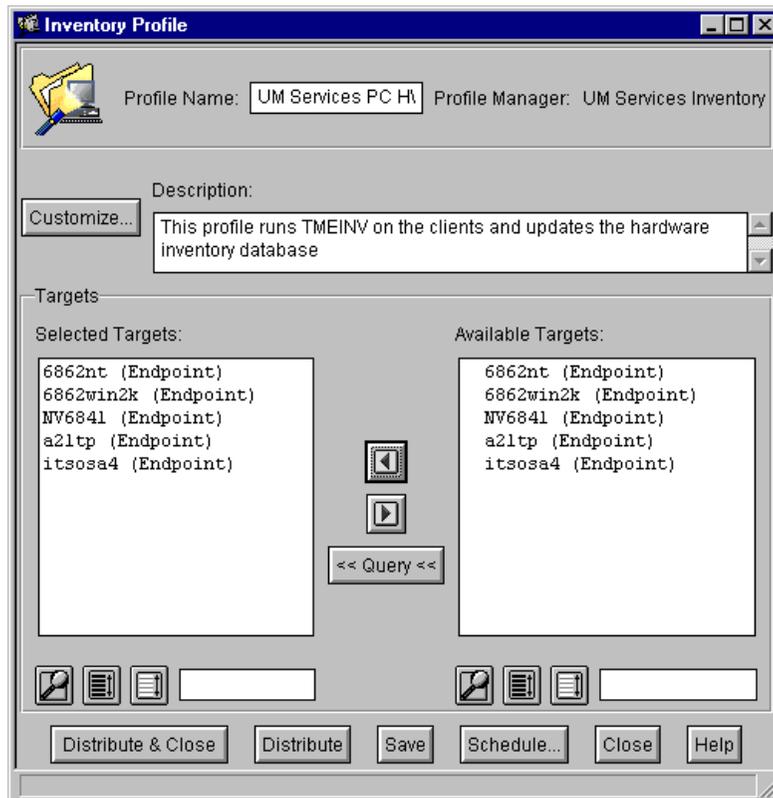
Figure 118. Selecting target endpoints for distribution

6. Highlight all entries in the Available Targets list and click ◀ to copy them to the Selected Targets list box.

7. Click **Distribute & Close**.

8. Repeat steps 5-7, this time right-clicking on **UM Services PC S/W Scan**.

6.3.2.3 Viewing and creating UM queries

Now that our database is populated we can view our UM data with the predefined queries in the Plus Module. We will also create a custom query.

To view a predefined query do the following:

1. Double-click **UM Services Inventory Query** from the UM Services Plus for Tivoli desktop.

2. Right-click one of the queries and select **Run Query**. We have chosen **User**, since this information comes from the Asset ID area.
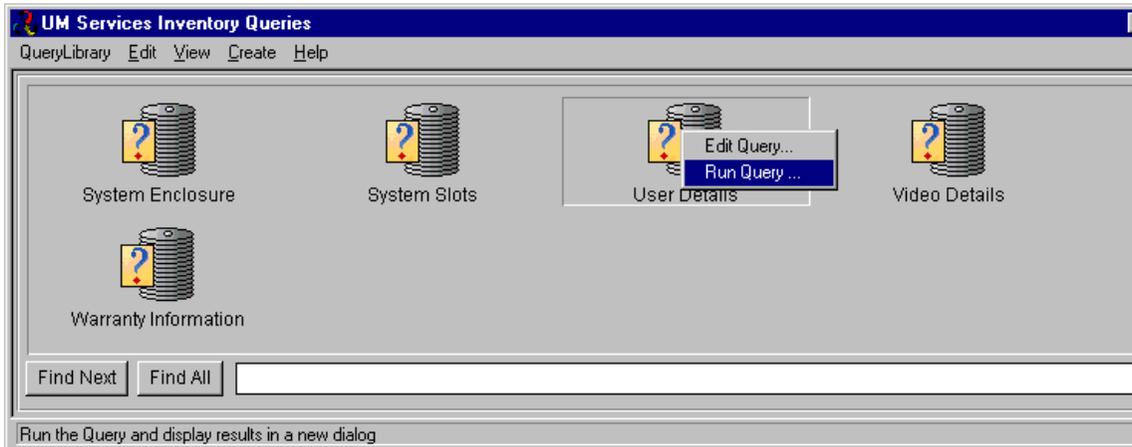
Figure 119. Choosing and running a query

3. You will be presented with a view similar to the following:

Figure 120. User Details query

4. At this point you can click Close or Export. If you click **Export** you can export the results to the text file:
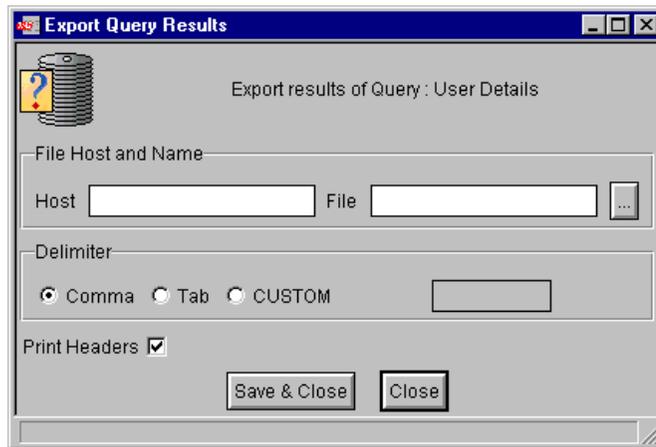
Figure 121. Export feature in UM query

If the predefined queries do not meet your requirements you can always create custom queries. We will use the UM Services Inventory Queries to create our custom query to find all PCs with a specific lease expiration date and its location.

Note: The date fields for the lease group are defined in the SQL Server database as "varchar" and not converted as an integer or date field. Searching within a time span will not be accurately reflected natively. For example, a search on all machines with a lease date prior to 12/31/01 will not yield the desired results.

To properly query these fields for time and date do the following:

- In the Tivoli UM custom query specify all the dates in that range. For example, you want find the lease expiration dates from December 1 to December 31, 2000. Populate the UMA_VLease_Information.Lease_ End_Date = value with 31 different entries namely 12/01/00, 12/02/00 .... 12/31/00. Combine each of these arguments with "or".

- Use the functions available in your hosting database (in our case SQL Server) for date conversion and query creation. Run the query from the toolset provided with your hosting database outside of Tivoli.

- Once the Tivoli custom query is run, use the export function to create a file that can be read by other tools (for example, Lotus 1-2-3 or Excel) that can do the required sorting.

Procedures:

1. Right-click the **UM Services Inventory Queries** from the UM Services Plus for Tivoli desktop. Choose **Create Query**.
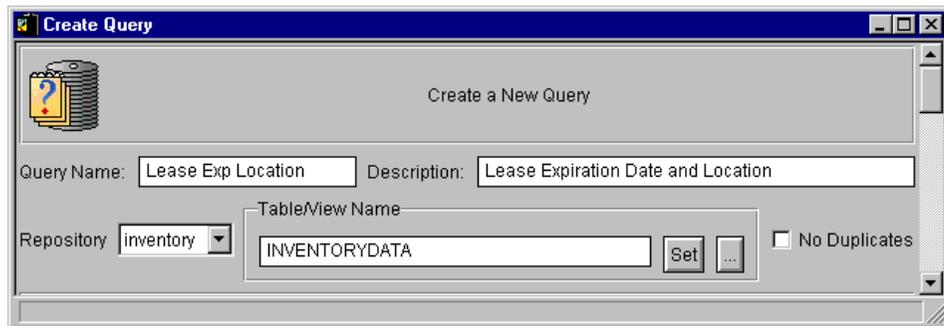

Figure 122. Creating a custom query

Figure 123. Populating query name and description

2. We will populate the initial fields with the following values:

   Query Name: `Lease Exp Location`
   Description: `Lease Expiration Date and Location`
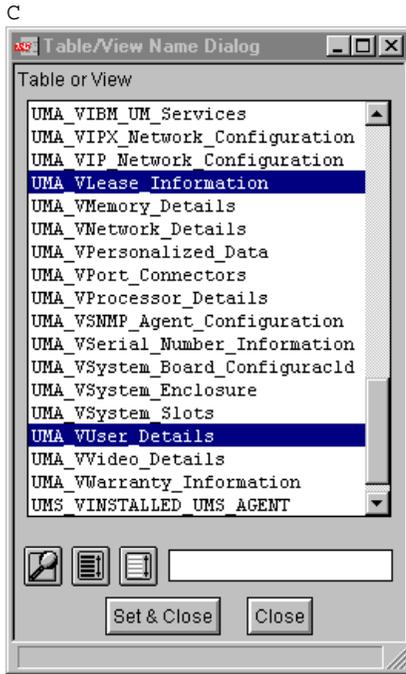
3. Click [...] in the Table/View Name section. Figure 124 appears:

C

Figure 124. Choosing a specific table

4. Highlight **UMA_Vlease_Information**. Hold the Ctrl key and highlight **UMA_VUser_Details.**

5. Click **Set & Close.**

6. From the Available Columns list box, select the following items and move them to the Chosen Columns list box.

   – UMA_VLease_Information.Lease_End_Date
   – UMA_VUser_Details.System_Location
   – UMA_VUser_Details.User_Name
   – UMA_VLease_Information.TME_OBJECT_LABEL
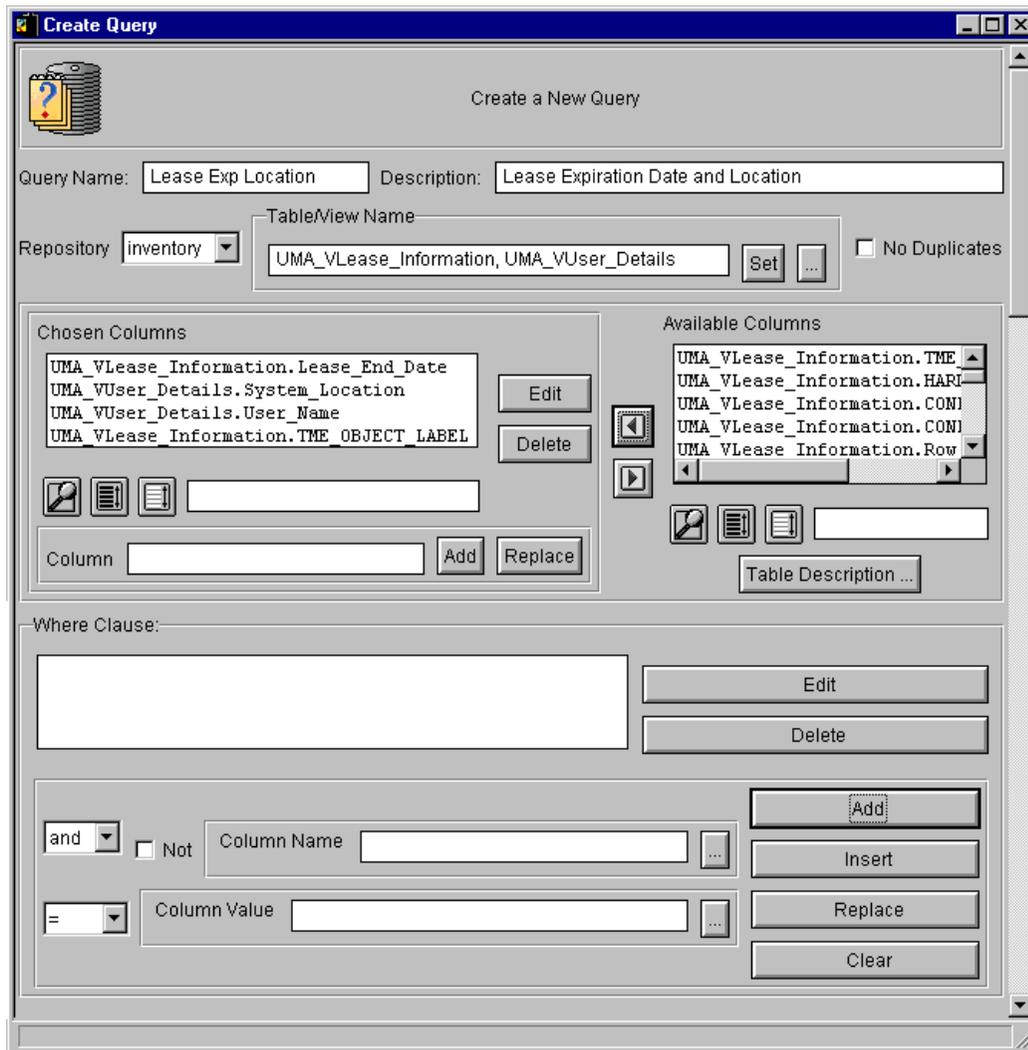
Figure 125. Moving an Available Column to a Chosen Column

7. Click next to Column Name and highlight
   UMA_VLease_Information.Lease_End_Date. We choose this field
   because it is the field that contains the value(s) we want to compare
   against the lease end date.
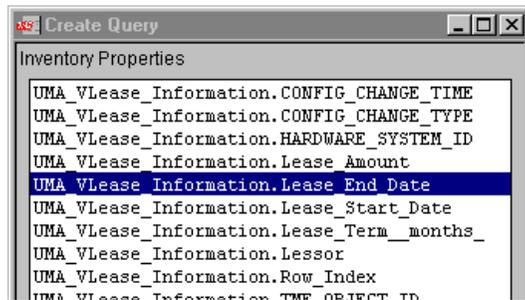
Figure 126. Specifying values

8. Click **Close**.

9. Click ⋯ next to the Column Value field and highlight a date. We have
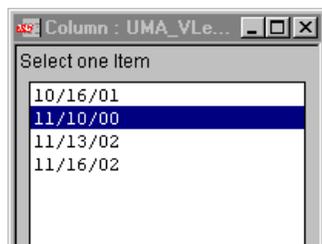   chosen **11/10/00**. Click **Close**.

Figure 127. Choosing a date for the query

10.Click **Add**. You should now see the Where Clause field populated.
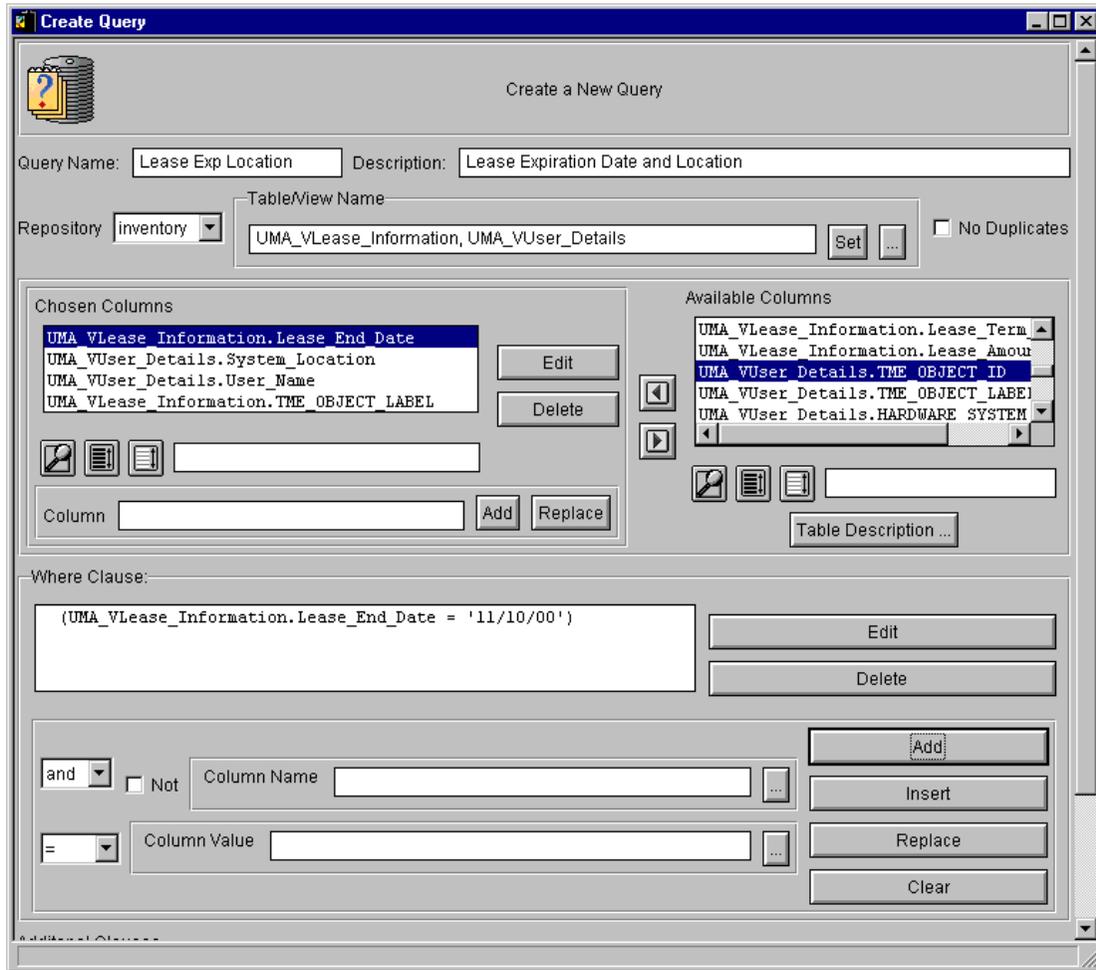
Figure 128. Where Clause window

11. In the Additional Clauses section (scroll to the bottom of the window — see Figure 129), type in the following:

    UMA_VUser_Details.TME_OBJECT_ID=UMA_VLease_Information.TME_OBJECT_ID
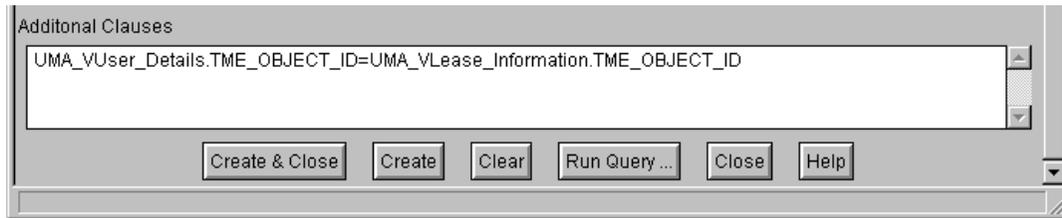
Figure 129. Additional clauses

Notes:

- This is case sensitive.
- If we do not insert this additional clause we will receive two or more occurences of each record because we are joining two tables.
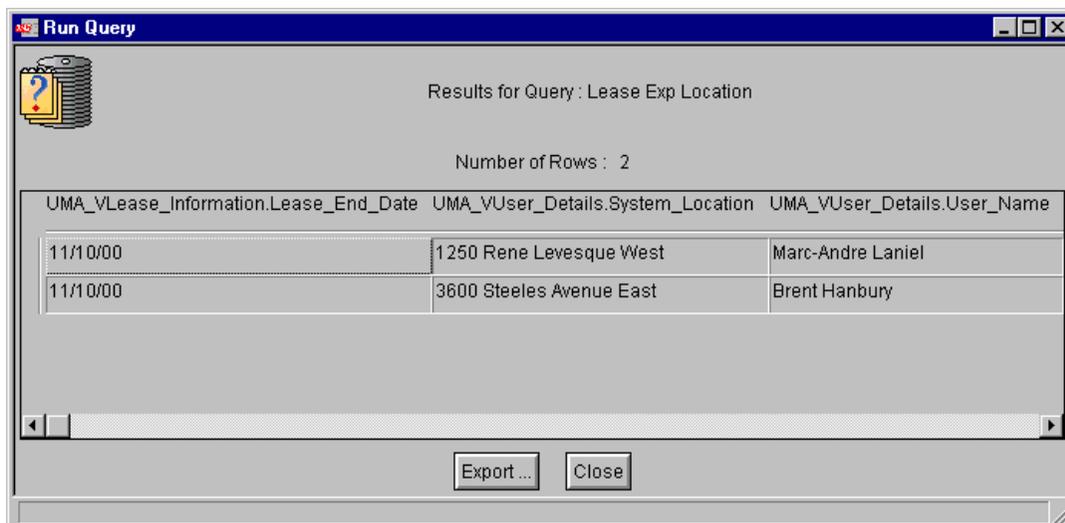
12.Click **Run Query** to get a preview of the query.

Figure 130. Preview of query

13.Click **Close**.

14.Click **Create & Close** if you are satisfied with your query.

15.You will now find a new query named **Lease Exp Location** in the UM Services Inventory Queries window (Figure 119 on page 152).

16.To run the query, right-click the query and choose **Run Query**.

Chapter 7. Implementing a complete Asset ID solution

What does an organization plan for in terms of Asset ID? In information technology, it is commonly accepted that "best practices" comprise technology, processes and people.

Think of each component as a leg on a stool. If any of these legs are missing, the stool will not be able to stand. Each component of people, processes and technology must work in harmony for success. The common factor for these three components is planning.

In this chapter, we briefly explain how processes, people and technology affect an Asset ID implementation. We then provide some hints and tips for the crucial planning stage. Lastly, we run through an end-to-end Asset ID scenario from the time the PC is received to the time it is retired.

- **Technology**

  There is no question that Asset ID is the technology component.

  Asset ID is the core technology enabler that lets you build and implement better solutions by automating manual tasks, simplifying processes and providing useful asset information. If the technology is leveraged correctly, you will build better processes and utilize your people more effectively.

- **Process**

  The Asset ID solution in an IT environment is only as good as the process that surrounds it.

  For example, you have just deployed new PCs in departments A, B, C in locations X, Y, Z. You have also electronically tagged each machine's location by using Asset ID. Six months later, departments A, B, C all move to new locations in different buildings. At this point you must have provisions in your Move, Add, Changes (MAC) process to change the data in Asset ID to properly reflect the new move.

  If you don't, the data will be incorrect the next time an inventory collection is performed, which defeats the purpose of using Asset ID in the first place. At every stage there must be well-documented procedures. And more importantly, these procedures must be followed.

  In the following sections, we provide some ideas that you may want to include and document in your process.

- **People**

  Even with the proper processes, you still require the right people to follow through on the processes to manage your IT effectively. These people

© Copyright IBM Corp. 2001 **161**

must have a good understanding of the process and technology. This understanding comes from training, experience and involvement.

In addition to the process and technology, people will either make or break a successful solution. For example, your organization had decided to implement Asset ID and you give the Symbol PDT 6100 and HID AMH100 to one of your IT staff to immediately start tagging machines at the dock. For this person to be productive, he or she should have an understanding of the task and how to use the technology first.

Technology and processes can reduce the number of people and their skill level but it will never fully replace them.

7.1 Planning

Some of the questions that have to be asked are:

1. What do we want to achieve in terms of benefit?
2. What do we need to achieve this benefit?
3. Do we have the time and resources?
4. Where and when do we pilot this?
5. What will our long-term gain be?

All these questions will guide you in your planning process. Here are key items and suggestions specific to Asset ID that you should consider when planning.

7.1.1 Reading and writing to the Asset ID area

How do you plan to read and write to the Asset ID area? There are many ways to do this and each will have its own set of requirements:

- RFID
- LCCM or DOS utilities
- IBM Director, Netfinity Director, UMS, Tivoli

7.1.1.1 RFID

To use RFID, you need to consider the following:

- One or more copies of the RFID software

If you are using RFID, you will need the appropriate hardware and software, such as the QueTel Asset ID Starter Kit as described in 3.1, "QueTel Asset ID Starter Kit" on page 16. Depending on the number of machines, you may need more than one copy of the Asset ID Starter Kit, especially if the PCs are geographically separated or there is a large number of systems to scan.

- RFID-capable systems

  Are the machines you have or plan to purchase RFID enabled? Without the RFID antenna and EEPROM in the client system, RFID integration simply will not be possible. As a good rule of thumb, any NetVista PC with the letter "P" at the end will have RFID (for example, A40P and S40P). The "P" denotes that these machines have the IBM *Promise of Value,* which includes RFID. The ThinkPad T2x and A2x systems also have the Asset ID EEPROM, but normally do not ship with antennas that must be purchased separately.

  Refer to 2.4, "Supported systems" on page 10 for more information.

- Where is the RFID data initially written?

  Where will the initial writing of the RFID data to the EEPROM take place? While the machine is in the box? At the end user's desk? If the data is written while the PC is in the shipping box, the box will have to be labelled for its destination (for example "Sarah Brown's office").

- Print barcodes before you start

  Use preprinted barcodes to expedite the process. It is a good idea to have preprinted barcodes of the data you want to input into Asset ID because it will offer you these advantages:

  - It will save you time and errors in keying in the information on the very small PDT keypad. When creating the barcodes, the information may be ported over from another existing source.

  - The barcodes can also be reused to label the shipping box or PC and its destination. For example, peel the barcode off its sheet and place it on the box. We will now know that particular machine is slated for Sarah Brown's desk in cubicle 123.

  - Barcodes can be permanently put in rooms. When machines move, you will need to rescan in its location. It will be very handy to have the room barcodes readily available.

7.1.1.2 LCCM or DOS utilities

This section really refers to the AIAREAD and AIAWRITE utilities that are supplied with LCCM that can be used natively in LCCM or put on a DOS boot disk. LCCM remotely boots clients using DOS.

Be aware of the following:

- You may be forced to use LCCM. For example, the NetVista S40P does not ship with a diskette drive, so booting from diskette is not possible. This

means that you will not be able to write to the Asset ID area by using a diskette in the default configuration.

- Where will the input come from? You can manually enter the information or you can have the information specified in a text file for the various groups that AIAWRITE writes to. The latter is less prone to error.

- Will you be using the information from Asset ID to write to a file on the hard drive? If this is the case, remember that DOS cannot natively see NTFS partitions. DOS will be able to see FAT32 partitions with the FAT32.EXE TSR supplied with LCCM.

  If you have a requirement for NTFS and need to write to the drive with AIAWRITE, here are our suggestions:

  - Leave the drive as FAT16 or FAT32 (Win2000) and then run the `convert` command upon first boot.

  - Make another partition FAT16 or FAT32 and write the data to this partition.

- AIAWRITE is an excellent utility if you want to write the exact same information to many machines (one to many) such as the lease dates. For example, you can predefine the lease dates in a custom LCCM profile. You would then drag and drop all the machines for that lease period into that profile and then click **Process**. This is a procedure that is best done at the time of initial image load.

- For Asset ID support on NetVista A40P systems, you will require a version of AIAWRITE and AIAREAD more recent than that supplied with LCCM 2.5.1 SP4. These are available from

  `http://www.pc.ibm.com/us/desktop/lccm/house2.html`

7.1.1.3 IBM Director, UMS, Tivoli, Upward Integration Modules

Be aware of the following points:

- If you are using Netfinity Director 2.12, you should apply the Asset ID patch or upgrade to a more recent version. See 5.2, "Netfinity Director 2.12 patch" on page 112 for information.

- With Netfinity Director 2.12, you will only be able to write to a single client at one time. However, you can read the Asset ID data from multiple clients at a time with the View Inventory feature.

- With the UMS upward integration modules you will only be able to write to a single client at a time. However, you can use the inventory viewer for the enterprise product to view all the Asset ID information.

- IBM Director and UM Services simulate Asset ID for systems that do not support Asset ID through hardware (EEPROM). These systems will lose any Asset ID settings when the ASSETCI.DAT file is erased. See 5.3, "Asset ID support in IBM Director" on page 115 for details.

7.1.2 Testing

Successful implementations are preceded by successful testing. Microsoft suggest a large amount of testing before implementing Windows 2000. Tivoli suggests a large amount of testing before implementing a Tivoli Management Environment (TME). Similarly we suggest thorough testing before implementing Asset ID.

Testing will identify any pitfalls you may experience. From our experience, thorough testing identifies problems early on where they can be corrected. Thorough testing reduces the number of potential problems once machines are deployed. The extra time testing will repay itself many times over.

We strongly recommend that you test Asset ID with the following considerations:

- Use a staging area or a test lab where the production LAN will not be affected.
- Document everything.
- Try as many different scenarios as possible including ones that will cause Asset ID to fail. For example, hold the AMH100 RF Reader so that it is out of range of the Asset ID antenna on the PC.

7.2 Full Asset ID integration scenario

IBM and QueTel were making many improvements and enhancements to the various products associated with Asset ID at the time of this writing. We will run through a scenario where Asset ID can be used fully to deploy and manage ThinkPads from the time the ThinkPad is received to the time it is deployed. We will provide the general steps involved.

7.2.1 Preparation

The preparation in this section involves the processes that are required before you actually receive any new machines.

1. Determine which model your organization has standardized on. For example we chose a ThinkPad T20 with the Intel mini-PCI Ethernet card

and the RFID antenna option. For this testing you will only need one T20, but two or three would be optimal to allow different stages of testing.

2. Create a staging area that closely resembles your production environment including similarly configured production PCs.

3. Install LCCM with Service Pack 4 and Netfinity Director 2.12 or IBM Director in this staging area. For Netfinity Director 2.12, install the Asset ID patch.

4. Start your initial planning to include other processes such as for moves, adds, and changes.

5. Install and configure the Asset ID Starter Kit. If you plan to print barcodes (which we recommend), purchase and install that software and print some test barcodes.

7.2.2 Initial setup

Do the following:

1. Create a master image as described in 4.1, "LANClient Control Manager" on page 50 with the following change: In your final master "Sysprepped" image or in your LCCM process you may want to copy some System Migration Assistant (SMA) automation scripts so that data and user migration will be easily facilitated. In your master/final image ensure that there is some UM enabler for reading and writing to Asset ID, such as IBM Director or UMS.

   Note: Updated versions of AIAWRITE and AIAREAD (post LCCM 2.5.1 SP1) are available for use with NetVista systems from:

   `http://www.pc.ibm.com/us/desktop/lccm/house2.html`

2. From a similarly configured production machine, automate the SMA capture so that the desired settings and data are saved to a network resource.

3. Print out some sample barcodes that peel off with the information you want to enter in the Asset ID area, namely the computer name, domain name, user name and user's department.

4. Install the antennas in the ThinkPad T20s.

5. Write to the Asset ID area using the Asset ID Starter Kit and the preprinted barcodes. To enable the LCCM autostart feature, ensure that the Image Profile date field has a 00/00/0000 or null date value and the Profile field has exactly the same name as the LCCM Profile (for example, `W2K with Asset ID Deployment`). You can check/change these values via the option

RFID View/Modify on the PDT as described in 3.1.2, "Viewing and updating the Asset ID data" on page 22.

Tip: You may want to shorten the LCCM profile name if you plan to use the autostart feature.

6. Start the LCCM scan on your LCCM staging server. See 4.1.2, "Scanning clients into LCCM" on page 58. You want to change the default client name (common name base) from CLNT to TP. This will indicate and mark the machines in this scan differently.

7. Connect the ThinkPad T20s in your staging area network.

8. Turn on the ThinkPads and boot them to the network (Press F12 when prompted during POST to boot via the Intel Boot Agent).

9. Let LCCM scan them in. The ThinkPads will be automatically powered off.

10. Assign the image you created in step 1 to these machines and click **Process**. This step is unnecessary if you used the autostart feature of LCCM. See step 5 on page 166.

11. Power on the ThinkPads either remotely via LCCM (wake clients) or power the machines on manually.

12. Allow Windows 2000 Sysprep to perform its functions.

13. Verify that the ThinkPad is imaged as designed.

14. If you are using Windows 2000 to push applications down, test this aspect. For example, if you are using Windows 2000 Server to push down MSI packages to your Windows 2000 Professional clients, you will want to ensure that the packages are correctly delivered and more importantly that they function correctly. This would be an excellent time to test the functionality of these applications.

15. Test both the final image and the process. This includes:

    - All applications in the image (for example, Microsoft Word, Lotus Notes, etc)
    - The ability to read and write information from Asset ID remotely (for example, IBM Director)
    - The Asset ID is ported up successfully to your management system

16. Sign off on your final staging area image.

7.2.3 Pre-pilot

At this point you should be ready for a pre-pilot. By pre-pilot we are referring to mini-pilot of a few users before a full pilot. The full pilot will be followed by

the actual rollout. Here are the steps you would take during this pre-pilot phase:

1. Make any required modifications to the master image that you signed off in step 16 on page 167 so that it will function correctly in your production domain. For example, there may be some specifics in the production domain that one of the application requires. If you have used IBM System Migration Assistant, many of these situations can be eliminated.

2. Image the new ThinkPad and provide this newly imaged machine to someone who will not be seriously impacted, such as yourself or a fellow IT colleague. Possibly provide similar images and machines to a few people.

3. Use this new ThinkPad as your production workstation and verify that all applications and tasks function as expected.

4. Once you are satisfied, sign off on this image.

7.2.4 Image delivery location and timing

At some point you have to determine where and when the master/final image is installed on all the new ThinkPads. This can be in one of three locations:

- **User's desk (final location)**

  Benefits:

  - One time and direct delivery to user's desk from shipping dock.
  - Image can be pushed down after hours directly to the PC when LAN traffic is minimized.
  - After imaging, the PC can be powered on for the first time so its computer account will be added to the domain automatically, since this will be on the production LAN.

  Drawbacks:

  - Will use network bandwidth to push down the image. May cause excessive LAN traffic if done during the day.
  - User will not be productive during the time the image is being pushed down if done during the day.
  - Leaving ThinkPads on unattended desks overnight may pose a theft risk.

- **Your staging area**

  Benefits:

  - LAN traffic is localized.
  - Multiple machines (especially desktops) can be imaged at the same time with only a power cable and LAN cable attached. In other words

you can stack the machines. You must ensure that the error startup sequence is set to Network in the configuration utility.
- Machines can be scheduled to be imaged overnight.
- Little to no user impact.
- Assuming your staging area is secure, the ThinkPads are also more secure during the imaging process.

Drawbacks:

- If the staging area LAN is totally isolated, you must perform its first power-on while attached to the production LAN to add the computer account to the domain. If you used System Migration Assistant, you may have to pull the SMA files from the production network.
- The machines will have to be moved two times: from the shipping dock to the staging area and then to their final destinations.

• **Your Business Partner or IBM**

You provide the master image to your Business Partner or IBM.

Benefits:

- Plug and go. All you require is to scan in the Asset ID information. You will, however, have to modify the first boot process so that Sysprep picks up the correct attributes from the Asset ID area. In 4.1.5, "Writing Asset ID data using LCCM" on page 68 we used LCCM to change this.
- Direct delivery to final destination.
- You will save imaging time and LAN bandwidth.
- The Business Partner or IBM may also be able to insert the RFID antenna for the ThinkPads. You will be able to immediately scan once the machine is received.

Drawbacks:

- There is a cost associated with these type of services.
- You will still need to initially register the machine into the LCCM database if you plan to use LCCM in the future for these machines. This process takes little time, however.

7.2.5 Piloting

As a pilot, we have decided to use the staging area scenario as a means to deliver the image. We have chosen this option because it will best illustrate our process and it does not require a change to our LCCM process defined in 4.1, "LANClient Control Manager" on page 50.

1. Choose a department or area where the pilot will have little impact.

2. Determine how many people in this area will be part of the pilot. We will use 10 people in our example.

3. Perform all the administration required, such as notifying the appropriate people of the new machines.

4. We recommend that you use System Migration Assistant (SMA) to ease the system and user migration. Since we are using IBM PCs, SMA is available at no additional charge and is part of the System Installation Tool Kit.

5. Print out the required barcodes for these 10 machines (individuals).

6. Once you received your 10 new ThinkPads, take them out of the box. Install an antenna in each system if you haven't had your Business Partner or IBM install them prior to delivery.

7. Using the Asset ID Starter Kit and barcodes, write the appropriate information into the Asset ID area.

8. Peel off and place the barcode for username on the underside of the notebook.

9. Plug in the new notebooks into your staging area LAN.

10. Start the LCCM scan. It could be an advantage to have your LCCM server on your production LAN at this time so future reloads will be easier, in addition to all the other benefits LCCM offers.

11. Power-on all the notebooks and boot to the network (press F12 to use the Intel Boot Agent). You could also use Wake on LAN to do this if you collected the MAC addresses in your RFID scan process.

12. Once all the notebooks are scanned in by LCCM, stop the scanning process.

13. Drag and drop all your newly scanned clients into the LCCM profile for your master image. This step is not required if you populated the Profile group with a null date and the profile with the exact name as the LCCM profile. See step 5 on page 166 for more information.

14. If your staging area LAN is attached to your production LAN (which we suggest), power-on the machines to allow Windows 2000 to do its first Sysprep boot. If your staging area LAN is not attached to the production LAN, do not power-on the machines until they are on a production LAN.

15. Deliver the machines to the 10 recipients.

16. Plug the machines into the LAN and power on the machines for the first time if applicable.

17. Run SMA if required. This may be part of a login script.

18. Regularly check back with the 10 users on how their new machines are functioning.

19. Ensure the Asset ID fields such as location are correctly populated.

20. Make modification to the image or process as required.

21. If your team is satisfied with the new ThinkPads and image, document a detailed process, since others will mostly likely be involved for the rollout.

22. If there are some processes or bugs to still work out, you may want to run another pilot. Remember, do thorough testing because this is your last chance before the rollout.

7.2.6 The rollout

You would follow the same steps as the pilot but this time the number of machines, users and departments will be much larger. You will need to mutually agree on a rollout schedule for all those involved. Once the machines are rolled out you will follow up to ensure that machines are operating as intended. At this time you would use the discovery tools, such as IBM Director or Tivoli, to populate your centralized database of assets.

7.2.7 Post rollout

Once the rollout is complete, there is still maintenance work to be done to keep your environment well managed.

7.2.7.1 Moves, adds, changes, and inventory

During your initial planning stages, you have hopefully put processes in place for moves, adds and changes. For example, if machines are moved, users leave, new hires arrive, etc., you will have a process outlining the steps to be taken, which may include rewriting to the Asset ID area whether it be through the Asset ID Starter Kit, IBM Director, or Tivoli.

At certain predefined intervals, run an inventory collection to determine any configurations that may have changed. If your process for moves, adds and changes is in place and followed, the changes in Asset ID should be reflected in your centralized database. You may want to perform a physical inventory if you do not have a centralized database. Similarly you may want to do a physical inventory to complement the discovery tools. With QueTel RFID products you can quickly inventory machines that are detached from the network (for example, in a storage room) without the hassle of looking for its serial number and model number. You now have the ability to port this information to other tools, including QueTel Asset TraQ.

7.2.7.2 Reloading of machines

At some point, the machines may have to be reloaded. With LCCM on your production LAN, this should be a straightforward process.

LCCM has a utility to search for machines in its client database including user name. Assuming the user name field in Asset ID has not changed since the client was first scanned in, you could easily find this client and remotely push the new image down. The LCCM process you have previously defined with your "master" image will allow you to push the image down. There is no customization required because our LCCM process will pull these variables out of Asset ID.

You create a new master image in the future to reflect a new operating system. Again you do not need to customize each machine, because your image will pull these variables from the Asset ID area.

As new machines are deployed, it would be wise to scan them into LCCM at that time even if they have been preimaged from a Business Partner or IBM.

7.2.7.3 Retiring machines

At some point the asset is usually retired. With the growing popularity of leasing, it is very advantageous to find your machines before the lease is up. Asset ID has fields for leasing information enabling you to be proactive. This information can now be queried in advance to determine when the leases are expiring and where the machines are located.

As an example, we are using ThinkPad T20s. Two years down the road, 10 mobile employees leave their current positions. Only eight of them return their notebooks. The barcode that you placed on the notebooks are long gone. The serial number is barely legible because of the wear and tear. How can you quickly determine who has returned their T20 ThinkPads even if the hard drive has been formatted? Use RFID to scan the information from these notebooks. If your process was implemented and followed correctly, you will be able to read the user and other information from the Asset ID area using RFID.

The above scenario is an example. You could use a similar method to determine the owners of the notebook and desktop systems coming into your area for reloading. For desktop systems coming into your reloading area you will have the ability to reload them remotely at their location without fear of theft.

If the machines to be retired come back to your area, securely dispose of the data using LCCM. Similarly, delete the data in the Asset ID area. Again this

can be done with LCCM. You will have to create a profile that writes null information to all the Asset ID groups.

7.2.8 Summary

The above end-to-end process for Asset ID may seem like a lot of work but really there are only a few extra steps performed from a non-Asset ID-enabled environment. Once you established your Asset ID process there are really only a few steps required. For example, a very fast deployment scenario could be as follows:

1. You receive your preimaged RFID machines from your Business Partner or IBM at your shipping dock.

2. While on the shipping dock, use the QueTel Asset ID Starter Kit to write to the Asset ID area.

3. Tag the shipping box for its destination.

4. Deliver the machines to its destination.

5. Set up the machine. Attach keyboard, mouse, LAN, power, and monitor.

6. Turn on the machine and boot to the network to scan the PC into LCCM.

7. Turn on the machine again.

8. Let Windows 2000 run its Sysprep.

9. Run System Migration Assistant.

10.The machine is now functional for work.

Appendix A. Special notices

This publication is intended to help customers, IBM Business Partners and IBM employees understand what Asset ID is and how to successfully implement it. The information in this publication is not intended as the specification of any programming interfaces that are provided by Asset ID and IBM workstations. See the PUBLICATIONS section of the IBM Programming Announcements for more information about what publications are considered to be product documentation.

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 IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

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 the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) 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, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers

attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

e (logo)®	PC 300
Asset ID	Redbooks
DB2	Redbooks Logo
HelpCenter	ThinkPad
IBM ®	Wake on LAN
IntelliStation	Lotus
LANClient Control Manager	SmartSuite
Netfinity	Notes
Netfinity Manager	Tivoli
NetVista	TME

The following terms are trademarks of other companies:

Tivoli, Manage. Anything. Anywhere.,The Power To Manage., Anything. Anywhere.,TME, NetView, Cross-Site, Tivoli Ready, Tivoli Certified, Planet Tivoli, and Tivoli Enterprise are trademarks or registered trademarks of Tivoli Systems Inc., an IBM company, in the United States, other countries, or both. In Denmark, Tivoli is a trademark licensed from Kjøbenhavns Sommer - Tivoli A/S.

C-bus is a trademark of Corollary, Inc. in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

PC Direct is a trademark of Ziff Communications Company in the United States and/or other countries and is used by IBM Corporation under license.

ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States and/or other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

Appendix B. Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

B.1 IBM Redbooks

For information on ordering these publications see "How to get IBM Redbooks" on page 181.

- *Using LCCM Functions with Servers and Workstations*, SG24-5292
- *Universal Manageablity: Enterprise Management Integration*, SG24-5388
- *Migrating from Netfinity Manager to Netfinity Director*, SG24-6155

B.2 IBM Redbooks collections

Redbooks are also available on the following CD-ROMs. Click the CD-ROMs button at **ibm.com**/redbooks for information about all the CD-ROMs offered, updates and formats.

CD-ROM Title	Collection Kit Number
IBM System/390 Redbooks Collection	SK2T-2177
IBM Networking Redbooks Collection	SK2T-6022
IBM Transaction Processing and Data Management Redbooks Collection	SK2T-8038
IBM Lotus Redbooks Collection	SK2T-8039
Tivoli Redbooks Collection	SK2T-8044
IBM AS/400 Redbooks Collection	SK2T-2849
IBM Netfinity Hardware and Software Redbooks Collection	SK2T-8046
IBM RS/6000 Redbooks Collection	SK2T-8043
IBM Application Development Redbooks Collection	SK2T-8037
IBM Enterprise Storage and Systems Management Solutions	SK3T-3694

B.3 Other resources

These publications are also relevant as further information sources:

- *LCCM 2.5.1 Training and Procedures Guides*, available from
  http://www.pc.ibm.com/us/desktop/lccm/docs.html

B.4 Referenced Web sites

These IBM Web sites are relevant as further information sources:

Table 12. IBM product and support Web sites

Product	URLs
Asset ID	`www.pc.ibm.com/ww/assetid`
Forums and e-mail support for TCO products	`www.pc.ibm.com/ww/solutions/enterprise/support/`
Hardware support	`www.pc.ibm.com/support`
IBM Director and Netfinity Director	`www.pc.ibm.com/ww/eserver/xseries/systems_management`
LANClient Control Manager (LCCM) LCCM 2.5.1 post SP4 fixes	`www.pc.ibm.com/us/desktop/lccm` `www.pc.ibm.com/us/desktop/lccm/house2.html`
Software Delivery Assistant (SDA)	`www.pc.ibm.com/ww/software/applications/sda`
System Installation Tool Kit	`www.pc.ibm.com/ww/solutions/lcc/sit.html`
System Migration Assistant (SMA)	`www.pc.ibm.com/us/software/sysmgmt/products/sma`
UM Services	`www.pc.ibm.com/ww/software/applications/ums/index.html`

These IBM Business Partner Web sites are also relevant as further information sources:

QueTel	`http://www.quetel.com`
HID Corporation	`http://www.proxtrak.com`
Symbol Technologies	`http://www.symbol.com`

How to get IBM Redbooks

This section explains how both customers and IBM employees can find out about IBM Redbooks, redpieces, and CD-ROMs. A form for ordering books and CD-ROMs by fax or e-mail is also provided.

- **Redbooks Web Site** ibm.com/redbooks

  Search for, view, download, or order hardcopy/CD-ROM Redbooks from the Redbooks Web site. Also read redpieces and download additional materials (code samples or diskette/CD-ROM images) from this Redbooks site.

  Redpieces are Redbooks in progress; not all Redbooks become redpieces and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

- **E-mail Orders**

  Send orders by e-mail including information from the IBM Redbooks fax order form to:

	e-mail address
In United States or Canada	pubscan@us.ibm.com
Outside North America	Contact information is in the "How to Order" section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Telephone Orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	Country coordinator phone number is in the "How to Order" section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Fax Orders**

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	Fax phone number is in the "How to Order" section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

This information was current at the time of publication, but is continually subject to change. The latest information may be found at the Redbooks Web site.

IBM Intranet for Employees

IBM employees may register for information on workshops, residencies, and Redbooks by accessing the IBM Intranet Web site at http://w3.itso.ibm.com/ and clicking the ITSO Mailing List button. Look in the Materials repository for workshops, presentations, papers, and Web pages developed and written by the ITSO technical professionals; click the Additional Materials button. Employees may access MyNews at http://w3.ibm.com/ for redbook, residency, and workshop announcements.

181

IBM Redbooks fax order form

Please send me the following:

Title	Order Number	Quantity

First name _____ Last name _____

Company _____

Address _____

City _____ Postal code _____ Country _____

Telephone number _____ Telefax number _____ VAT number _____

☐ Invoice to customer number _____

☐ Credit card number _____

Credit card expiration date _____ Card issued to _____ Signature _____

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

Abbreviations and acronyms

AC	alternating current	MIF	managed information format
ASCII	American National Standard Code for Information Interchange	MSI	Microsoft Installer
		OEM	other equipment manufacturer
BDC	backup domain controller	OS	operating systems
BIOS	basic input output system	PC	personal computer
BSM	backscatter modulation	PCI	peripheral component interconnect
CAB	cabinet	PDC	primary domain controller
CD-ROM	compact disk read only memory	PDT	portable data terminal
CIM	common information model	POST	power-on self-test
COM	communications	PXE	Preboot eXecution Environment
CPU	central processing unit	RAID	redundant array of independent disks
CSV	comma separated variable		
DBMS	database management systems	RAM	random access memory
DHCP	Dynamic Host Configuration Protocol	RF	radio frequency
		RFID	radio frequency identification
DIMM	dual inline memory module	ROM	read only memory
DMI	desktop management interface	SCSI	small computer system interface
DOS	disk operating system	SDA	Software Delivery Assistant
EEPROM	electrically erasable programmable read only memory	SID	security identifier
		SMA	System Migration Assistant
IBM	International Business Machines	SMS	Systems Management Server
IDE	integrated drive electronics	SNMP	Simple Network Management Protocol
IE	Internet Explorer		
IIS	Internet Information Server	SP	service pack
IP	Internet Protocol	SQL	structured query language
ITSO	International Technical Support Organization	TCP/IP	Transmission Control Protocol/Internet Protocol
LAN	local area network	TMA	Tivoli Management Agent
LCCM	LANClient Control Manager	TME	Tivoli Managed Environment
LCD	liquid crystal display	TMR	Tivoli Management Region
LCF	Light Client Framework	TP	ThinkPad
LED	light emitting diode	TSR	terminate and stay resident
MAC	medium access control	UM	universal manageability

UMS	universal manageability services
UNC	universal naming convention
URL	universal resource locator
WAN	wide area network
WBEM	Web-Based Enterprise Management
WOL	Wake on LAN

Index

Numerics
08K6064   12

A
abbreviations   183
AIAREAD/WRITE fixes for NetVista   57
Alert on LAN   128, 134
AMH100   10
   tips for usage   11
antenna   3
   location on desktops   12
   operation   6
   option for ThinkPads   12
   power source   6
   removing from ThinkPads   12
asset group   6
Asset ID
   See also EEPROM
   See also groups
   browser interface   145
   bull's-eye label   10
   IBM Director, integration with   111
   implementing a solution   161, 165
   introduction   1
   LCCM, integration with   68
   partners   15
   SDA, integration with   87, 104
   sticker on shipping carton   10
   support   14
   supported systems   10
   updating using the Asset ID Starter Kit   22
Asset ID Starter Kit   16–35
   Asset ID data, updating   22
   Asset ID information, reading   24
   Asset TraQ, compared to   16
   barcodes   28
   building field   23
   Collect Handheld Data option   30
   Collect New Items option   27
   CSV file
      format of   33
      uploading to   29
   demonstration key   17
   EEPROM user area fields   25
   evaluation version   17
   installation   17
   inventory taker name   23
   location field   23
   options
      Collect Handheld Data   30
      Collect New Items   27
      RFID Only   22, 26
      RFID View/Modify   22
      Send Data to PC   29
      Update Tag   26
      User Info   25
      Utility Menu   29
      View/Modify Tag   24
   PDT initial load   19
   planning   162
   RFID Only option   22, 26
   RFID View/Modify option   22
   room number field   23
   Send Data to PC option   29
   Update Tag option   26
   uploading data   29
   User Info option   25
   Utility Menu option   29
   View/Modify Tag option   24
Asset TraQ   35–48
   Asset ID Starter Kit, comparing with   40
   database views   47
   installation   37
   LCCM, export to   43
   Send Data to PC option   41
   uploading to the PC   41
ASSETCI.DAT file   115

B
backscatter modulation   6
barcodes
   printing   23, 163
   scanning   28
boot sequence   59
booting a client from the network   58
browser interface   145
bull's-eye label   10
Business Partners, using   169

C
client images   168

© Copyright IBM Corp. 2001

185

IBM Redbooks review

Your feedback is valued by the Redbook authors. In particular we are interested in situations where a Redbook "made the difference" in a task or problem you encountered. Using one of the following methods, **please review the Redbook, addressing value, subject matter, structure, depth and quality as appropriate.**

- Use the online **Contact us** review redbook form found at **ibm.com**/redbooks
- Fax this form to: USA International Access Code + 1 845 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Document Number **Redbook Title**	SG24-6165-00 Implementing Asset ID
Review	
What other subjects would you like to see IBM Redbooks address?	
Please rate your overall satisfaction:	O Very Good O Good O Average O Poor
Please identify yourself as belonging to one of the following groups:	O Customer O Business Partner O Solution Developer O IBM, Lotus or Tivoli Employee O None of the above
Your email address: The data you provide here may be used to provide you with information from IBM or our business partners about our products, services or activities.	 O Please do not use the information collected here for future marketing or promotional contacts or other communications beyond the scope of this transaction.
Questions about IBM's privacy policy?	The following link explains how we protect your personal information. **ibm.com**/privacy/yourprivacy/

189

IBM

Redbooks

Implementing Asset ID

(0.2"spine)
0.17"<->0.473"
90<->249 pages

Implementing Asset ID

IBM ®

Redbooks

Explains how you can reduce your total cost of ownership

Helps you perform client rollout and inventory tasks

Describes the Asset ID technology and products

Asset ID is a radio-frequency identification technology that lets you read and write PC system data using RF devices such as handheld scanners. It can be considered the next generation of barcodes, but instead of actually having to find and scan the barcode then looking up a database to find the matching information, you simply hold the scanner near the system and all the system information is read in real-time, directly from the system.

Asset ID is available in recent models of the IBM PC 300PL, NetVista, and IntelliStation workstations, plus selected ThinkPad models.

Asset ID aids deployment by recording end-user information and software requirements on individual PCs without having to unpack them from the cardboard box. It also makes inventory reporting easier because you no longer have to open the system unit to determine what components are installed.

This redbook describes how to implement Asset ID. We describe what the components are and how the technology works. We explain how to use Asset TraQ and the Asset ID Starter Kit, two Asset ID solutions from IBM Business Partner QueTel Corporation. We then take a look at how to implement Asset ID with the following management products: LANClient Control Manager (LCCM), Software Delivery Assistant (SDA), Netfinity Director, and the Tivoli FrameWork.