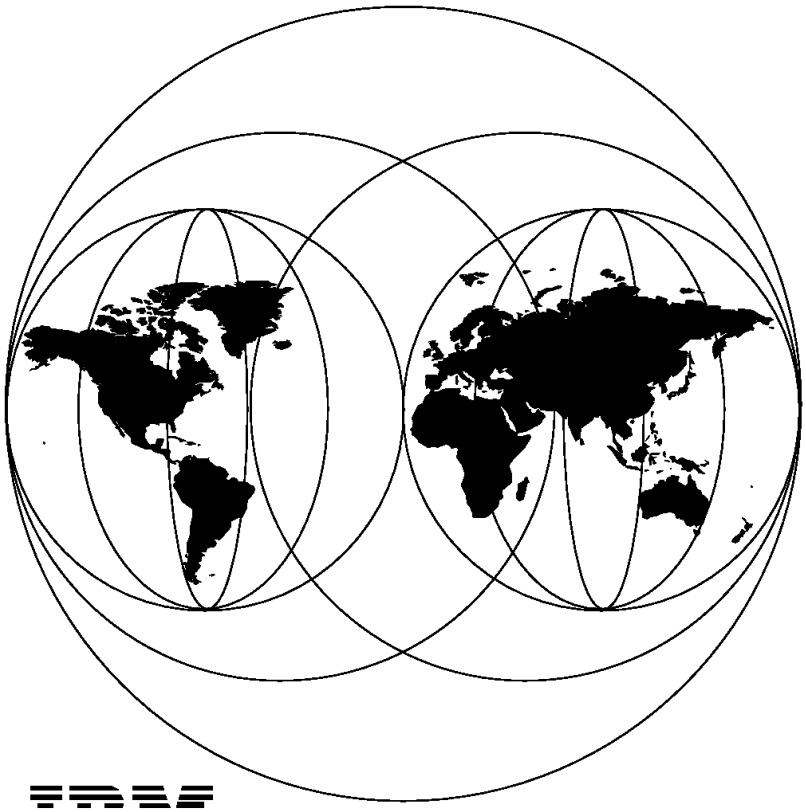
Getting Started With TME 10 User Administration 3.1

August 1997



IBM

International Technical Support Organization
Austin Center

International Technical Support Organization

SG24-2015-00

Getting Started With TME 10 User Administration 3.1

August 1997

Take Note!

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

First Edition (August 1997)

This edition applies to Version 3, Release 1 of TME 10 User Administration for use with UNIX, Windows NT, NetWare and RACF.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. JN9B Building 045 Internal Zip 2834
11400 Burnet Road
Austin, Texas 78758-3493

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Figures

Tables

Preface

In a distributed and heterogeneous environment, managing user and group accounts and maintaining consistent user name and passwords across various platforms is time consuming and a heavy task.

This redbook describes a tool, part of the Tivoli Management Environment (TME) framework, that helps systems administrators manage a large number of user and group accounts from a single point. This tool is TME 10 User Administration.

This redbook describes the TME 10 Framework with a specific focus on the user and group administration application within that framework. After describing user and group management concepts on various platforms (UNIX, Windows NT, NetWare, and RACF), information is provided on how to deploy TME 10 User Administration in a customer environment. Planning, installing and using TME 10 User Administration are described in this redbook. Technical issues are highlighted as well as hints and tips.

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 Austin Center.

Yves Bex is an Advisory Systems Engineer at the International Technical Support Organization, Austin Center. He writes extensively and teaches IBM classes worldwide on all areas of Symmetric Multiprocessing, Migration from AIX V3.2.5 to AIX V4, Windows NT and systems management in general. Before joining the ITSO two years ago, Yves worked in an IBM Branch Office in Toulouse, France. He was in charge of large customers in the aerospace industry as a UNIX Systems Engineer. He has a strong field experience.

Marco Mangravitti is a Systems Management Specialist at IBM Italy. He has one year of experience in C and C++ software development and one year of experience in systems management. He has worked at IBM for one year. His areas of expertise include TME 10 Systems Management, Windows NT and UNIX operating systems. He has written extensively on Windows NT and UNIX users and groups management.

 is a Certified Solutions Architect in Sweden. He has 20 years of experience in the security field. He has worked at IBM for 30 years. His areas of expertise include Security and Large Systems. He has written extensively about RACF users administration.

 is a Security Program Manager in IBM Global Services (IGS) in Australia. He has eight years of experience in the security field and has worked at IBM for 10 years. He has worked for a number of years as a security systems programmer and as the team leader for the security administration group within IGS, Australia. He has written extensively on RACF user administration.

Thanks to the following people for their invaluable contributions to this project:

Rick Fafard
Tivoli Systems

Dan Martilloti
Tivoli Systems

Cees Kingma
IBM ITSO Pougkeepsie

John Dayka
IBM Poughkeepsie

Nancy Ball
Tivoli Systems

Pat Griffin
Tivoli Systems

Tim Little
Tivoli Systems

Gary Cole
Tivoli Systems

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 (cross-ref to the Evaluation form) to the fax number shown on the form.
- Use the electronic evaluation form found on the Redbooks Home Pages at the following URLs:

  For Internet users `http://www.redbooks.ibm.com`
  For IBM Intranet users `http://w3.itso.ibm.com/redbooks`

- Send us a note at the following address:

  `redbook@vnet.ibm.com`

Chapter 1. Introduction

This chapter gives an overview of user administration issues in a truly distributed environment. It presents Tivoli's approach in managing users and groups and provides an overview of TME 10 User Administration.

1.1 Issues in Managing Users in a Distributed Environment

The growth of client/server computing, and the recent move to network computing, has resulted in an explosion in the number of servers, databases, and applications that users must access in order to perform their jobs. This causes headaches for end-users as they struggle to keep up with the various user IDs and passwords (both of which usually vary by platform) that they need to access these resources.

It also causes even more severe headaches for administrators as they struggle to keep up with learning the various administrative systems for each resource and then expend effort in tracking users as they join an organization and change jobs.

User administration is the process of enabling and controlling end-users' access to information by creating, modifying, and deleting user accounts and access privileges on various resources throughout the enterprise. It is very common to find customers whose users require 10-30 different user IDs and passwords to access everything from LAN servers to relational databases to client/server applications to mainframe-based applications. In a corporation with tens of thousands of users, the multiplier effect generally leads to a situation in which the complexity of user management is simply becoming unmanageable.

In order to properly control users' access, administrators must understand the information requirements of the user (typically based on a user's department or group affiliation), the various ways in which the user may be represented across different resources, and the corporate security policies that might impact how and when access is granted. Since information is usually a company's most critical competitive weapon, it is even more important to have the ability to ensure that a user's access has been disabled or deleted when that person leaves his/her position in the company.

Many customers are looking for a consistent, integrated approach to managing user accounts and access privileges across this diverse spectrum of resources. Unfortunately, the current situation is largely characterized by islands of management/automation in which separate tools are required to manage user access across servers, databases and applications. This leads to an environment where efforts are repetitive and time-consuming, with many errors occurring along the way.

1.2 User Administration Approaches

There are three approaches commonly found to solve the user administration problem:

Re-Hosted

Vendors using this approach have provided very good “mainframe” security tools in the past. These tools were generally designed to manage many users on *one* system (that is the mainframe). With the proliferation of client/server solutions, these vendors have seen the opportunities to provide extended user administration; however, their approach is to “re-host” or port their mainframe based solution over to the distributed servers or resources. This solution, which takes a mainframe approach (many users for one system) to solve a distributed or network computing problem, doesn’t work very well in that it doesn’t really hide the complexity of the user information.

LAN-Centric

Some vendors approach this problem from the other side of the fence. They have good LAN-based tools to solve management of LAN systems (including user administration) and they are trying to “grow-up” these solutions to fit the network computing environment. As they look at the complexity of the environment they are trying to solve, they usually limit their support to only addressing “system” accounts and not user accounts.

Directory

Many vendors are touting “directories” as being the answer to the user administration problem. The dilemma here is “which directory?”. There are many existing directories out there, no standards yet for these directories and they usually don’t work together. Thus, the applications need to be changed to fit the directory standard, and then the administrators have to understand the specifics of each of these “point” solutions that don’t work together!

Note:

An INFO WORLD article (from 11/25/96) talks about an effort to consolidate or integrate directory information (Microsoft, Netscape, Novell, IBM, Lotus, Banyan, Worldtalk, and Zoomit). The effort is called “Lightweight Internet Person Schema” and it will be presented to the Internet Engineering Task Force (IETF). It defines a common set of attributes in enterprise directories (such as length, placement, and naming of e-mail and URL data and it complements the Lightweight Directory Access Protocol (LDAP) which is currently under construction from the IETF.

1.3 The Tivoli Approach

The Tivoli approach is one that focuses on shielding the administrator from having to understand in great detail all the different platforms he has to deal with. Instead, it focuses the administrator on the tasks that he needs to perform. With Tivoli, the administrator does not have to understand all the details of adding a user to UNIX, Windows NT, NetWare, Resource Access Control Facility (RACF), and (DCE) Distributed Computing Environment (available through the santix

offering which extends TME 10 User Administration with the capability to managed DCE) systems.

The object-based architecture of TME 10 provides increased scalability to your administrators and operators. It allows you to define high-level polices for user administration and then delegate to junior administrators the tasks you want them to perform across the enterprise. You can also schedule changes to your systems to occur when you want them to occur and, with the Tivoli solution behind you, know that these changes will be completed successfully, or in the case of an error, that the systems will be rolled-back to their prior state ensuring that your users will not be affected.

With this capability to define high-level policies for your user administration needs (and then also define more detailed policies based on organizational needs), you can be assured that the security policies (or user administration policies) are being followed.

1.4 The Tivoli Solution: Single-Action Management

Normally, when you add a user into your company, you have to access each system the user will be using, understand the syntax of those various systems and then manually give the user access to each of the required resources.

Tivoli is the only solution that gives the administrator single-action management! With a single action, the administrator can add, change, and delete users across UNIX, Windows NT, NetWare, RACF, and DCE systems. Support for additional platforms will be added later on.

In addition, a senior administrator can set up default policies for your various users in their policy regions so that when a new user joins your sales or engineering group, with a single point and click, you can generate the default user IDs, passwords, working directories and so on for each of the various systems and resources that this user needs access to.

You can also designate certain systems (for example, if they only need access to HP-UX and NetWare systems and not AIX, Solaris, and Windows NT).

When a user changes jobs or leaves the company, you simply need look at your user database to quickly and easily determine which systems that user had access to and change/remove access as needed.

1.5 TME 10 User Administration: Features at a Glance

TME 10 User Administration allows you to manage the Windows NT and NetWare user attributes and many of the UNIX attributes. Since UNIX systems have some differences, Tivoli's approach is to allow you to manage all of the common UNIX attributes.

These attributes include:

- Approximately 20 Windows NT user attributes, including information such as login, password, profile, groups, and so on. In addition, TME 10 User Administration supports both domain user accounts and local user accounts.
- Approximately 60 NetWare attributes, including support for login, password, context, groups, and so on. Both NetWare 3.x (which has Bindery support) and NetWare 4.x (with its NetWare Directory Service (NDS) support) are supported.
- Approximately 30 common UNIX attributes, such as group ID, user ID, password, and home directory.
- RACF attributes including the base segments.
- Many DCE attributes through DCEmgmt/Security Manager from santix, such as principles, accounts, groups, organizations, and so on.

1.6 Easing Day-to-Day Operations

In addition to capabilities of adding users, deleting users, and changing users's attributes, there are some major actions provided by TME 10 User Administration. These actions include:

Populate

There is a very high chance that you are not implementing TME 10 User Administration from scratch. All your existing systems probably have users already defined. You are probably using many different tools to manage these users. TME 10 User Administration is able to gather your current user information and create your initial user database. This operation is called populate. Once all your user information is retrieved and stored into the TME 10 User Administration database, user administration operations such as adding, changing, deleting a user can be performed by using this unique user administration tool.

Distribute

Many companies have similar departments and groups that probably share some high-level and detailed characteristics. In these cases, you would like a tool that allows you to use definitions that you have set up in one place in another.

With TME 10 User Administration, once you have created your initial user database and your user administration policies, you can use this information to set-up user management policies for other policy regions. You can do this by using the “distribute” capabilities of TME 10 User Administration. This function allows you to take many of your current definitions that you are using and redistribute them out so that you can quickly and easily set-up another policy region within your enterprise.

Verify

While you can (most of the time) safely delegate responsibilities to junior administrators, there are times when you need to be able to verify that your user policies are still in place and that accurate and up-to-date information is available. With the “verify” function (actually "Check Policy" function) of TME 10 User Administration, you can easily verify that remote sites have followed your user

policies. This function is also useful to consolidate all of your user administration information into a central place (if so desired).

Synchronize

What happens when you find out that your policies have not been followed? What if you have a rogue administrator out there who has granted system access to users who really didn't have a need to know (maybe they just didn't ask the right questions when another user came asking for access to that new Windows NT system). With TME 10 User Administration, you can easily "synchronize" a central user database from your endpoint data file (system files), enabling you to quickly reestablish control of your enterprise users.

1.7 santix DCEmgmt Offerings

On August 5th, 1996, santix software (a leading German Distributed Computing Environment (DCE) and systems management consulting and products company) announced the DCEmgmt application suite, a truly integrated, scalable management solution for DCE. DCEmgmt is based on TME 10 and adds extensions to the TME 10 User Administration product. However, it is not part of the TME 10 User Administration product.

The DCEmgmt application suite consists of five modules, which will address all DCE management tasks, allowing customers to customize their own management solutions. These five modules are:

- DCEmgmt/Security Manager
- DCEmgmt/Event Manager
- DCEmgmt/Cell Manager*
- DCEmgmt/DFS Manager*
- DCEmgmt/Application Manager*

They are built on the TME 10 Framework and tightly integrate with other TME 10 applications. The DCEmgmt application suite is based on DCE 1.1 (1.0.3) and supports major UNIX platforms and Windows NT systems.

The DCEmgmt/Security Manager is a powerful extension of TME 10 User Administration for managing principals, groups, organizations, accounts, and security policies in a DCE Registry. The DCEmgmt/Event Manager permits correlation of DCE serviceability and audit events with other event sources in the TME 10 Enterprise Console. In addition, monitoring of DCE servers are also possible using TME 10 Distributed Monitoring.

Future support will include the other three modules. DCEmgmt/Cell Manager will provide common configuration management functions for DCE cells, such as cell attribute and server configuration. DCEmgmt/DFS Manager will perform management functions for the DCE Distributed File System, such as aggregate and fileset creation, fileset mounting and replication, as well as fileset backups.

1.8 TME 10 User Administration Key Advantages

TME 10 User Administration is the only solution that provides:

- Single-action management

  With a single action, you can add/modify/delete users across multiple systems (UNIX, Windows NT, NetWare, RACF, and DCE today).

- Administrator authority delegation

  You can centrally define user policies and then delegate specific authorities to junior administrators, ensuring that the actions you want performed are the only ones allowed by those administrators.

- Scalability

  If desired, you can manage every user in your enterprise from a single point or you can set-up several control points within specific management domains that allow you to manage every user from a single point in those domains.

- Security

  With a single action, you can easily determine what systems a user has access to and then once they leave the company, you can ensure that you have disabled their access back into your company.

- Integration

  With a TME 10 solution, you can use a common desktop for all of your system management applications. You have a single desktop that allows you to manage your users, as well as the other resources, and all of the applications that you need to perform from a single place. In fact, with a TME 10 solution, many times you are using multiple applications, but because of the ease-of-use of a Tivoli solution, you don't even realize you are using different applications (you just perform the tasks that you need to do).

1.9 Single-Action Management: Customer Relevance

What is the real benefit of implementing TME 10 User Administration? There are actually four main benefits that Single-Action Management gives you:

Saves Time and Money

With Single-Action Management, you can quickly execute multiple management operations in a single step. Thus, you can now set up user access to multiple systems with a single step. You can also consolidate your user accounts and set up default policies that will help reduce repetition and reduce mistakes. In addition, for any responsibilities that you have delegated out to junior administrators, you can easily incorporate changes that they have made back into one central repository.

Reduce Mistakes

With the capability to define a user policy (and defaults) from a central location, you can ensure that these policies are consistently performed/executed throughout your company. In addition, you have the capability to automate the distribution of those policies, all of which helps to improve user accuracy and to help reduce mistakes.

Creates "Peace of Mind"

Because you can efficiently and easily set up your user administration policies, delegate out responsibilities, and with one step remove user access, TME 10 ensures increased security for your enterprise.

Maximizes your Investments

Last, but not least, Tivoli helps you maximize the investments that you have already made. It minimizes the tools that you need to buy, works with tools and systems that you already have in place, and allows you to use a “single” model of the management environment and then leverage it across your management disciplines. And because the TME 10 desktop and management model is so easy to use, it helps reduce your administrator/operator training costs!

Chapter 2. Understanding TME 10 Framework

This chapter gives an overview of the Tivoli Management Environment as well as the Tivoli Management Framework (TMF) for readers that are not familiar with Tivoli products. If you are already familiar with the Tivoli TME 10 Framework and want to understand and implement TME 10 User Administration, you can skip this section and go to Chapter 4, “What Is TME 10 User Administration?” on page 65.

2.1 Tivoli Management Environment

Today’s computing environment relies more and more on distributed client/server setups for information system needs, where users at the client workstations perceive the network as one big server or service provider. Distributed computing or network computing ties people, information, and resources more closely together, but brings a challenge when considering the management of these systems. Managers face the complex problem of maintaining many different types of hardware and operating systems.

Tivoli Systems’ answer to managing a network computing environment is a set of management applications known collectively as TME 10, where TME stands for Tivoli Management Environment. TME 10 provides a way to manage network computing resources of many different types from a single location. TME 10 products provide a consistent interface to different operating systems and services. TME 10 allows administrators to control users, systems, and applications from one desktop and provides a streamlined way to automate and delegate routine, time-consuming tasks.

2.1.1 TME 10 Product Architecture

The TME 10 applications all share a common framework, called the TME 10 Framework. The TME 10 Framework is open and object-oriented and includes a set of managers, brokers, and agents that conform with the Common Object Request Broker Architecture (CORBA) specifications produced by the Object Management Group (OMG). This technology allows major differences between computer operating systems to be hidden from the TME 10 user and allows the encapsulation of key services in objects that can be used by multiple management applications. Basically, it allows for platform-independence, a unifying architecture, and the ability of third-party vendors to easily adapt to the TME 10 Framework.

2.1.2 TME 10 Disciplines and Products

The TME 10 products that allow you to manage your entire computing environment, including applications, fall into four distinct categories:

1. **Deployment management**
   Configuration and change-management activities. Example: Distributing new software and maintaining an enterprise-wide hardware and software inventory repository. The products that cover this category of management disciplines are:
   - TME 10 Software Distribution – Performs software distribution
   - TME 10 Inventory – Views and records software products installed on remote systems

2. **Availability management**
   Maintaining mission-critical service levels through proactive analysis of the entire computing environment, including centralized system and network monitoring, automated actions, and performance management. The products that cover this category of management disciplines are:
   - TME 10 Enterprise Console – Collects management messages and alarms and performs automatic responses
   - TME 10 Distributed Monitoring – Monitors system resources and services
   - TME 10 NetView
   - TME 10 Performance Management
3. **Security management**
   Protecting information and controlling access to resources. The products that cover this category of management disciplines are:
   - TME 10 User Administration – Performs user and group management
   - TME 10 Security Management
4. **Operations and Administration**
   Enabling day-to-day operation of managing thousands of applications through automated facilities for job scheduling, help desk, backup/restore, and output management. The products that cover this category of management disciplines are:
   - TME 10 Job Scheduler
   - TME 10 Remote Control
   - TME 10 ADSM (ADSTAR Distributed Storage Manager)
   - TME 10 Plus Modules for integration of third-party products – Modules designed for specific third-party applications that allow them to be integrated into the TME environment. An example of one of these modules is Tivoli/Plus for NetWorker. NetWorker is a product from Legato Systems, Inc., a third-party company, that performs backups and restores of different systems. If the Tivoli/Plus for NetWorker module is installed with the actual NetWorker software, you can then perform NetWorker functions from the TME 10 desktop.

The TME 10 Framework builds the foundation for all of the products listed above. In addition to the products that cover specific disciplines, there are several so-called multidiscipline products:

- TME 10 Framework

  The Framework is the foundation for other Tivoli and third-party management products. It provides a graphical desktop, object-oriented databases, and base services used by the other products. The TME 10 Framework is discussed in detail in section 2.2, “Tivoli Management Framework” on page 16.

- TME 10 Global Enterprise Manager (GEM)

  Unifies network computing management processes across mainframe data centers and distributed environments. An S/390 system becomes an element of the network computing environment – as a point of centralized management, as a peer manager or as a managed endpoint. The bidirectional Management Integration Services are GEM’s center-piece and provide:

- An exchange and update of management data between the management products on both environments
- A common view and collection of events from both environments with the possibility of performing a single action that executes a function on all platforms
- The ability to issue common commands from the S/390 interface or from the TME 10 interface

- TME 10 Net.Commander

  Manages Web servers, mail servers, news servers, and proxy servers.

- Tivoli Manager for PowerBuilder applications and a Tivoli Developer Kit for PowerBuilder applications
- TME 10 Module for SAP R/3
- TME 10 Module for Lotus Domino/Notes

Figure 1 depicts the layout of the TME 10 product structure together with the various integration and programming toolkits.

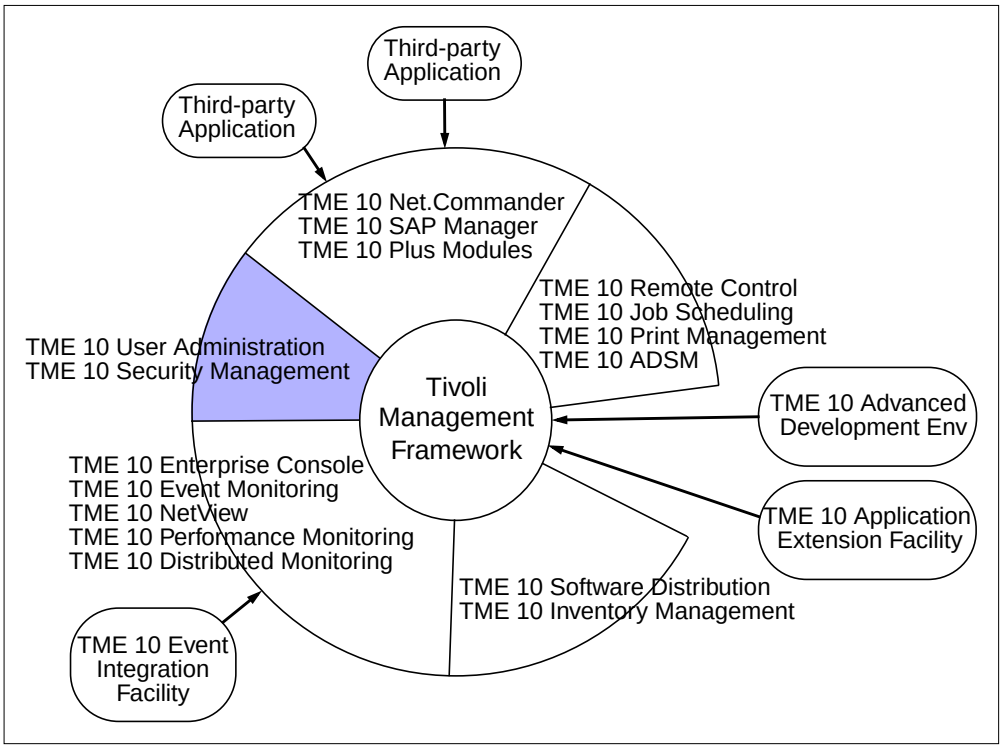


Figure 1. TME 10 Software Components

In addition, TME 10 provides toolkits that allow extension of TME 10 applications or development of new applications by using standard APIs. There are the three TME 10 Toolkits:

- ***TME 10 Application Extension Facility (TME 10 AEF)*** – Allows dynamic customization of TME 10 applications by adding site-specific behavior or values to standard applications. A typical AEF extension would be to create customized icons for your TME 10 desktop.

- ***TME 10 Event Integration Facility (TME 10 EIF)*** – Allows adaptation of events from other applications into the TME 10 Enterprise Console. An example of using the EIF would be to take events generated by Hewlett-Packard OpenView and integrate them into the TME 10 event console.
- ***TME 10 Advanced Developer's Environment (TME 10 ADE)*** – Has programming tools to create new applications on top of the framework.

Note that due to the merger of Tivoli with IBM, some product names have changed. For those who were familiar with Tivoli products before the merger, Figure 2 shows the pre-merger Tivoli products in which TME 10 products are rooted.

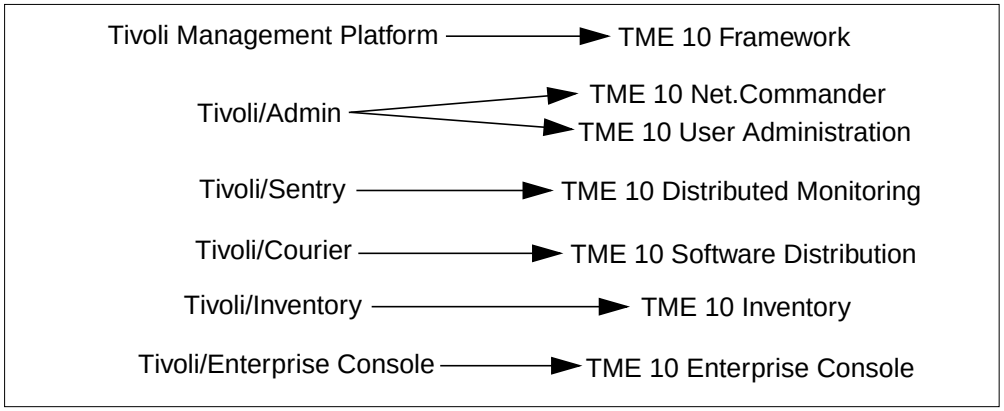


Figure 2. Summary of Product Name Changes

This list is not inclusive of all TME 10 products. For more information on TME 10, see the Tivoli Web site at `www.tivoli.com`.

2.1.3 Tivoli Management Environment

The Tivoli Management Environment or TME 10 Environment, refers in general to the set of TME 10 management applications, but can also refer specifically to the set of TME 10 products functioning at a particular site. TME 10 products are used in environments where businesses have many machines that must be managed; so it will be helpful to look at the layout of the TME 10 products in these situations.

2.1.3.1 TME 10 Servers and TME 10 Clients

The TME 10 environment consists of machines designated as either a TME 10 server or a TME 10 client. A *TME 10 server* runs software and a database that allows it to manage TME 10 clients. The *TME 10 clients* run software that allows them to interact with the server. A TME 10 client can only be configured to interact with one server.

2.1.3.2 The TME 10 Management Region

The basic unit of TME 10 functionality is the TME 10 Management Region (TMR). It consists of one TME 10 server and the clients that server is managing. The server for a TME 10 Management Region is normally referred to as the TMR server for a particular TMR and will hold the database for that TMR.

Depending on the size and requirements of an environment, there may be more than one TMR defined. If multiple TMRs are present, they can either stand on

their own or be linked together. Linking TMRs allows management functions to be exchanged between the regions. These connections can be of a one-way or two-way nature in terms of access permissions and exchanging information between TMRs.

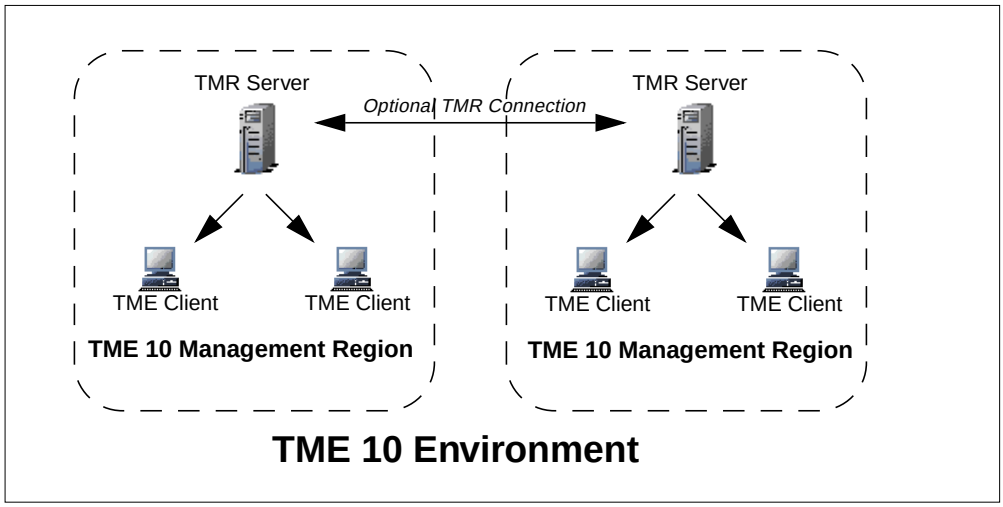


Figure 3. TME 10 Management Region Layout

2.1.3.3 TMR Design and Configuration

There are many criteria that should be considered when deciding how to divide an enterprise into one or more TME 10 Management Regions and then how to connect these TMRs.

Server Load

The performance of TMR servers will affect whether or not multiple servers are needed. Load will be caused by the processes used to contact client machines, by network traffic processing, and by the CPU and memory used by the server. If the load on a server becomes too high, it may be necessary to create multiple TMRs to aid performance.

Number of Clients

It is recommended that a single TMR server support no more than 200 clients. A client in this scenario does not include any PC clients running the PC agent software. For descriptions of these terms, please see section 2.2, “Tivoli Management Framework” on page 16. With a future extension of the TME 10 Framework architecture, the number of TME 10 clients in a TMR is drastically increased. This extension is known as the Light Client Framework.

Network Topology and Limitations

TME 10 uses TCP/IP, for the most part, for its communications. All direct traffic between clients and the server is TCP/IP. This should be taken into account during the planning of the TME 10 environment to assure that good connectivity and bandwidth is available for the operation of the TME 10 environment. A feature of the TME 10 that may be helpful in planning the network portion of the environment is the Multiplexed Distribution (MDist) service, which allows a distribution hierarchy.

Location of Administrators

The location of administrators is another consideration. If a company's administrators all work from one central location, one TMR may be sufficient. However, if there are three geographic locations, each having separate administrators responsible for their site's servers, multiple TMRs may make more sense.

Security

There are two issues to be concerned with for security: encryption levels and limited access.

At the time of the TME 10 installation, you must choose the level of encryption to be used for this TMR. The encryption level you choose will determine the security of the sensitive data stored by TME 10. Only one encryption level can be chosen per TMR; so if different levels of encryption are necessary, it may be necessary to have multiple TMRs.

Multiple TMRs will also allow you to limit administrator access to sets of machines.

Reliability

Multiple TMRs can provide some forms of reliability. If one TMR server goes down, other TMR servers can still function properly. Note that this will not provide redundancy for management of the clients located in the TMR of the down TMR server.

2.1.4 Common Concepts of Operation

Most of the TME 10 products operate under the same set of concepts. These concepts are described briefly below and in more detail in the chapters that follow.

- The communication within the TME 10 environment is performed by the oserv daemon or service, which runs on the TMR server and all of the managed nodes (not the PC managed nodes).
- The information relating to all objects in the TME 10 environment, along with the application-specific information, is stored in a distributed, object-oriented database.
- One graphical user interface, called the TME 10 desktop, provides a window into the TME 10 environment and access to all of the TME 10 applications.
- Most TME 10 functions are performed in the context of *profiles*. A profile is a collection of specific information that can be manipulated and distributed to machines in the TME 10 environment. The general concepts of creating and distributing a profile are common to all of the TME 10 applications.
- The operations in the TME 10 environment are all subject to *policies*, or rules for operation.

2.2 Tivoli Management Framework

The foundation of TME 10 is the TME 10 Framework. This base software is required to run any of the other TME 10 management applications. It provides some core TME 10 capabilities and services that are needed by other TME 10

applications as well as the graphical user interface (GUI), which lets the administrator view the environment.

The TME 10 Framework consists of the following features:

- ***Graphical User Interface (GUI)*** – The TME 10 desktop that allows administrators to view and control the TME 10 graphically. It provides standard logical layout of the TME 10 environment and keeps this standard throughout the addition of other TME 10 products.
- ***Command Line Interface (CLI)*** – This is used to run commands to view and control the TME 10 environment.
- ***oserv daemon*** – This is the service that runs continuously and coordinates communication within the TME 10 environment.
- ***Databases*** – This is the storage for information about objects in the TME 10 environment. TME 10 uses one database that is distributed among all of the machines running TME 10 Framework within a management region.
- ***Application Services*** – The core TME 10 capabilities and services that are needed by other TME 10 applications, such as profile managers and *MDist* for distribution. Also included are the task library, the scheduler and the bulletin board for notifications.
- ***Installation*** – This is the component used to install all TME 10 applications, locally and remotely.

2.2.1 TME 10 Framework Software

The TME 10 Framework is first installed on a machine designated as a TME 10 Management Region (TMR) server. Installing the TMR server installs each of the components listed above. Once the server is installed, you can create TME 10 clients by installing the TME 10 Framework on UNIX or Windows NT systems. You can perform this installation either remotely from the TMR server or locally on the TME 10 client machine. Following installation, the TMR server and each TME 10 client has an oserv daemon running locally. It is through these oserv daemons that the TMR server and its clients communicate and perform TME 10 management operations.

The TME 10 Framework also includes PC agents that allow the TME to manage PCs as well as UNIX and Windows NT systems. The PC agent is installed locally on these machines, either directly from the TME 10 Framework CD-ROM or from diskettes made from the CD-ROM.

Also included with the TME 10 Framework software package are two programming toolkits (TME 10 ADE and TME 10 AEF), the UserLink/DHCP service, which provides support for TME 10 UserLink and PCs running the DHCP (Dynamic Host Configuration Protocol), and PostScript documentation for these products. These products must be installed separately after the TME 10 Framework is installed.

2.2.2 Supported Platforms

The TME 10 Framework runs on the following operating systems:

- AIX
- HP-UX
- Solaris

- SunOS
- Windows NT

The TME 10 PC agent software runs on the following operating systems:

- DOS
- NetWare
- OS/2
- Windows 3.x
- Windows 95
- Windows NT

For specific information regarding operating system and maintenance level compatibilities and requirements, consult the latest release notes and installation manuals for the TME 10 Framework.

2.2.3 TME 10 Machine Roles

As explained in Section 2.1.3.2, “The TME 10 Management Region” on page 14, each TME 10 Management Region has one TMR server. The TME 10 Framework is first installed on this TMR server. Then TME 10 client software can be installed on remote machines. There are basically two kinds of TME 10 clients: those that can run the TME 10 Framework software and those that run the PC agent software.

The client/server relationships between the server and the two types of clients is shown in Figure 4 along with the supported operating systems. These relationships are discussed in the subsections immediately following.

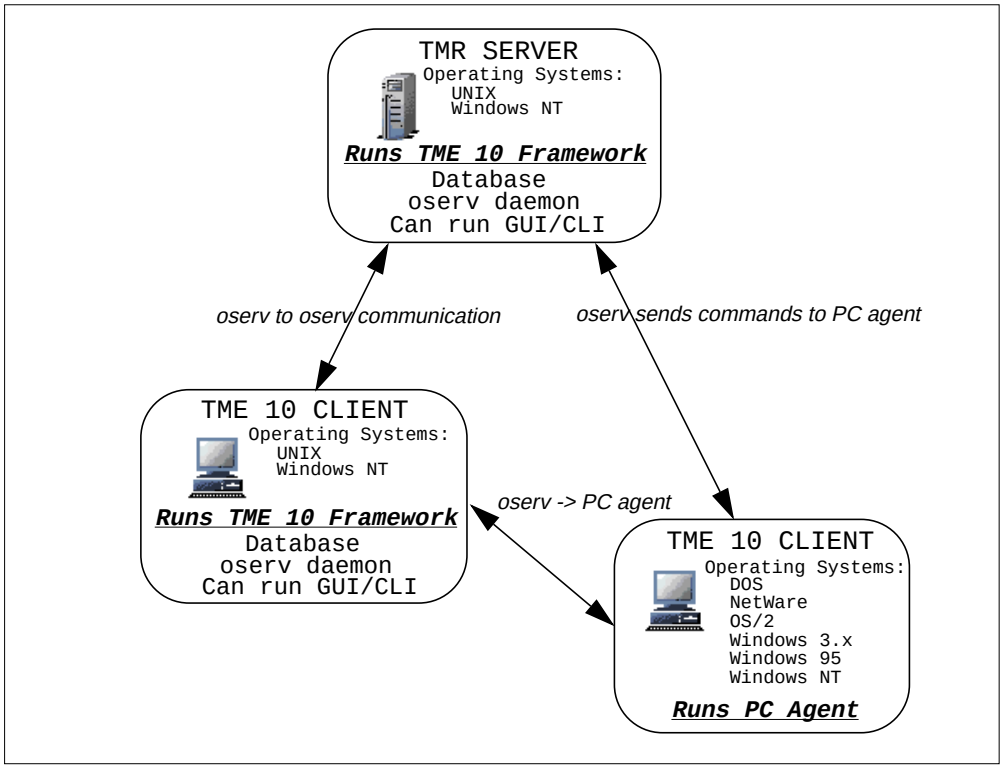


Figure 4. TMR Server and Clients and their Software Requirements

2.2.4 TME 10 Clients Running the TME 10 Framework

UNIX or Windows NT clients are able to run the TME 10 Framework. For a list of supported UNIX platforms, see section 2.2.2, “Supported Platforms” on page 17. These clients run an oserv daemon and have a local database that is integrated with the server’s database. You can run the TME 10 desktop from these systems, in which case the device is called a TME 10 management station. Management stations have slightly greater system requirements than clients that do not require the TME 10 desktop. Guidelines for sizing these and the other TME 10 machines can be found in the *TME 10 Framework Planning and Installation Guide*.

In some cases it may be beneficial to cascade the flow of information from the TMR server to its clients instead of having the default, flat distribution. Multiplexed Distribution (MDist) provides the functionality to do this by allowing TME 10 clients running the TME 10 Framework to be designated as repeaters that can resend information they receive from the server to other clients.

2.2.5 TME 10 Clients Running PC Agents

PCs can be managed without having to run a full TME 10 Framework. These "limited-function" TME 10 clients are called *PC agents*. They run the TME 10 PC agent software and are only used with the TME 10 Software Distribution and TME 10 Inventory products. A list of supported operating systems can be found in 2.2.2, “Supported Platforms” on page 17.

The PC agent software is available through the TME 10 Framework software package in two versions, one to communicate via TCP/IP and the other via the Internet Packet eXchange/Sequenced Packet eXchange (IPX/SPX), the latter being used only between a NetWare server and clients. When PC agents are defined to the TME 10 environment, they must meet one of two criteria:

- Have a TME 10 client or server running the TME 10 Framework to sponsor them and communicate with the TMR server on their behalf
- Be a client of a NetWare server running TME 10 NetWare repeater software. The NetWare repeater software allows a NetWare server to distribute software to its clients.

In order to support Windows machines that connect using the Dynamic Host Control Protocol (DHCP) addressing environment, you install a product on the TMR server called *TME 10 UserLink*, which is also included in the TME 10 Framework software package. The UserLink product provides additional capabilities for software distribution options.

2.2.6 Resources

An important concept of the TME 10 environment is that of resources. *Resources* are the TME 10 representations of actual elements in the enterprise. These resources may correspond to physical things, like computers, or to intangible things, like a set of rules governing a computer. Resources that are subject to certain sets of rules within the TME 10 environment are called *managed resources,* and the predefined rules are called *policies*.

Managed resources are contained within *policy regions*, which are special collections of managed resources that are subject to the same set of rules. As more products are installed in the TME 10 environment, more managed resources become available for use.

This section first discusses the resources found on the TME 10 desktop and then the different types of managed resources.

2.2.6.1 Resources Found on the TME 10 Desktop

This section discusses the resources found in the primary or top-level window of the TME 10 desktop (the administrator GUI), along with icons that represent them.

Administrator Collection and Administrator

The administrator collection is a container that holds the icons for all administrators defined for the TME 10 environment. It is represented by the icon shown above on the left. Within the administrator collection is an icon for each administrator, as shown on the right. The pop-up menus on the administrators' icons enable you to view and change information about the administrators, particularly their role assignments. The functions that can be performed using these resources are discussed in Section 2.2.9, "Administrators" on page 27.

Bulletin Board

This resource contains notices that are sent by TME 10 applications to inform the administrators of changes in the TME 10 environment. The icon for the bulletin board can appear in two different states, one showing there are no new notices to read, shown on the left above, and one showing that there are new notices, shown on the right. The notification facility is discussed in Section 2.2.10, "Notification (Bulletin Board) Facility" on page 28.

Policy Region

The policy region resource is a collection of managed resources that share one or more common sets of rules. Policy regions also represent administrative domains that can be assigned to administrators. They are discussed in Section 2.2.8, "Policy and Policy Regions" on page 26.

Scheduler

The scheduler resource allows tasks performed within the TME 10 environment to be automated. This feature is discussed in Section 2.2.13, "Scheduler" on page 33.

Generic Collection

The generic collection is a container on the desktop that can hold sets of resources, including other containers. Its function is to group and allow easy access to resources. The generic collection does not actually contain these resources, as policy regions do; it is only a set of pointers that link to resources located elsewhere in the TME 10 environment.

2.2.6.2 Managed Nodes

 TME 10 clients running operating systems able to support the TME 10 Framework are represented as *managed nodes*. Two icons are available for managed nodes, a server and a client icon. There is no difference in the way the different icons function; they differ for aesthetic purposes only and may be toggled back and forth at will. Managed nodes run the oserv daemon and maintain a local database. Managed nodes are UNIX or Windows NT systems and have the graphical TME 10 desktop capability.

The TMR server itself is configured automatically as the first managed node on the TME 10 desktop. Other managed nodes are defined and appear on the desktop when the TME 10 Framework software is installed on them. Communication is then established between the oserv daemons running on each system. Once the managed node icon appears on the desktop, the following menu options are available on a pop-up menu for that icon:

- **Open...** This menu option opens a window for the managed node and displays any relevant contents, such as local profile copies.
- **Properties...** This menu option displays physical system information such as RAM and allows changes to be made to some information, such as Internet Protocol (IP) interfaces.
- **Run xterm** This menu option opens an X-terminal session on that machine. This option is invalid for Windows NT managed nodes.
- **Toggle icon...** This option allows you to change between the server and client icon for the machine. This is for appearance only and does not change any of the functionality in the TME 10 environment.
- **Synchronize...** This option allows the synchronization of information stored in profiles with the corresponding system files. This will be discussed further in Section 2.2.11, “Configuration Management” on page 29.

This menu can be expanded as more TME 10 applications are installed. In particular, TME 10 User Administration adds host management options to it.

2.2.6.3 PC Managed Nodes

 A *PC managed node* is a representation on the TME 10 desktop of a TME 10 client running PC agent software. The actual PC managed node by definition is a UNIX or Windows NT managed node that relays and keeps object information in its database about a machine running PC agent software, as shown in Figure 5.

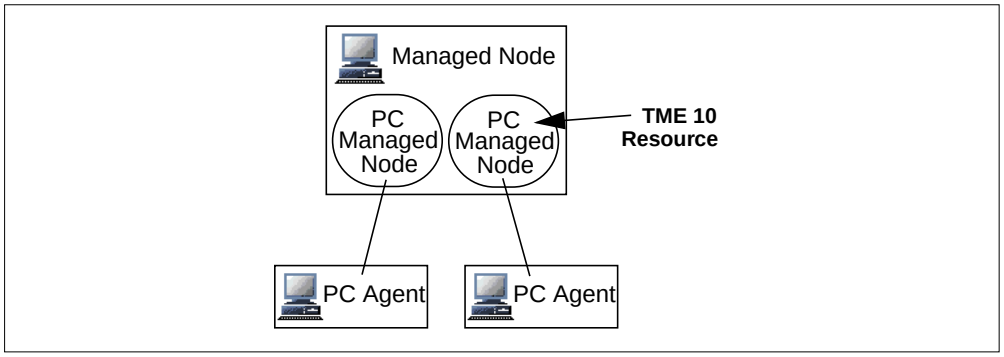


Figure 5. PC Managed Node/PC Agent Relationship

The icons for PC managed nodes are exactly the same as those of managed nodes. The label below it showing the machine's operating system will indicate what type of machine it is. As with managed nodes, there is no difference in functionality between the server and client icons; the icon used for a certain device is up to the user.

Icons for Windows NT

Machines running the Windows NT operating system can have different roles in the TME 10 environment. They can run the TME 10 Framework, in which case they would show up as managed nodes on the TME 10 desktop. They can also run the PC agent software and would then appear as PC managed nodes on the TME 10 desktop. Since the icons for managed nodes and PC managed nodes are the same, those Windows NT nodes running TME 10 Framework have a label reading *TMP/NT,* and those running the PC agent have the label *Windows NT*

When a PC managed node icon is added to the desktop, the following menu options appear as a pop-up menu for that icon:

- **Properties...** This displays physical system information about the PC.
- **Editable properties...** This option allows changes to be made to the icon name, operating system, and other fields.
- **Toggle icon...** This menu option allows you to change between the server and client icon for the machine. This is for appearance only and does not change any of the functionality in the TME 10 environment.

This menu can be expanded as more TME 10 applications are installed.

Note on PC Managed Nodes

The concept and usage of the *PC managed node* and *PC agent* terms can be confusing and often misleading. A TME 10 client running PC agent software can be called a PC agent machine. Sometimes it is also referred to as a PC managed node. In actuality, the PC managed node is a UNIX or Windows NT system that holds object information in its TME 10 database about a machine running PC agent software. Be aware that the term PC managed node is sometimes used to describe the PC client itself or the UNIX or NT system sponsoring that client as a proxy.

2.2.6.4 NetWare Managed Sites

The NetWare managed site (NWMS) resource icon represents a NetWare server and a group of NetWare clients. Multiple icons can be created for the same server if two different sets of clients are to be defined. The concept and terminology is the same for the PC managed node and PCs running the PC agent. The NWMS is a representation of the NetWare server and its clients. The actual object in the TME 10 database resides on a UNIX or NT managed node that acts as the liaison between the server and the NetWare server and its clients. This relationship is shown in Figure 6 on page 23.

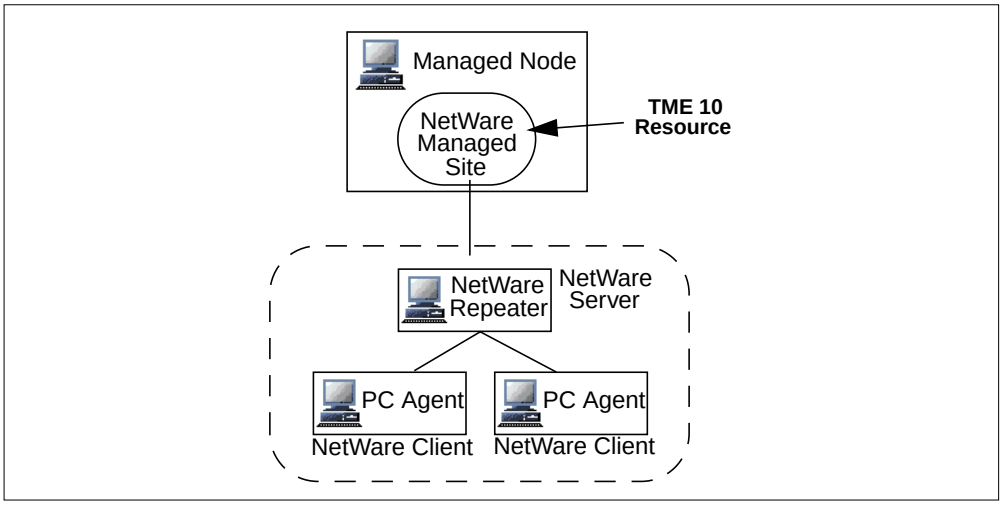


Figure 6. NetWare Managed Site

The NetWare managed site is used for software distribution.

2.2.6.5 Other Managed Resources

Managed resources are those resources subject to TME 10 predefined rules, called policies, and are contained within policy regions. Managed nodes, PC managed nodes, and NetWare managed sites discussed in the previous sections are the managed resources that represent computers. Other managed resources available with the TME 10 Framework are discussed below and are shown with their respective icons.

Policy Subregion

A policy subregion is a policy region located inside another policy region. A policy subregion has the same icon as a policy region. Policy subregions are discussed in Section 2.2.8, “Policy and Policy Regions” on page 26.

Profile Manager

A profile manager resource is a container for profiles. Managed resources, such as managed nodes, PC managed nodes, and even other profile managers, can subscribe to a profile manager. During a profile distribution, subscribers of a profile manager receive copies of the profiles (and their

contents) contained in the profile manager. Profiles and profile managers are discussed in Section 2.2.11, “Configuration Management” on page 29.

Task Library

 A task library is a managed resource that allows an administrator to create and store tasks and jobs, which are defined below.

Task

 A task is a resource that represents an action or operation that needs to be performed within the TME 10 environment. Tasks are discussed in Section 2.2.12, “Performing Tasks in the TME 10 Environment” on page 32.

Job

 A job is a resource representing a task that is executed on specific managed resources. Jobs are discussed in Section 2.2.12, “Performing Tasks in the TME 10 Environment” on page 32.

Query Libraries and Queries

 The query facility is represented by query libraries and queries that appear within the context of a policy region. A *query library* is a container for queries and is represented by the icon on the left. A *query* is a specific, predefined request for information from the TME 10 configuration repository, a feature of the TME 10 Inventory application. It is represented by the icon on the right.

2.2.7 Introduction to the Desktop

The TME 10 *graphical user interface (GUI)*, or *desktop*, is the administrator’s view of TME 10. The TME 10 desktop, or simply called the desktop, allows users to graphically access resources and perform tasks. TME 10 also provides a *command line interface (CLI)* to allow many of the functions that the desktop provides to be performed from a shell. There are some functions that can be performed from the CLI only. Some functions can be performed through the desktop only.

The TME 10 desktop can be started from any machine running the TME 10 Framework software. The desktop can be configured to start from any subset of servers and clients running the TME 10 Framework. There is also a product called *TME 10 Desktop for Windows* that can be installed on machines running Windows 95, Windows NT, or Windows 3.11. The TME 10 Desktop for Windows is a graphical client/server software comparable to the X-Windows architecture. The desktop functions are performed on the TME 10 Framework (managed node), but the display window is sent across the network and displayed under Windows. To the user it appears as if the TME 10 desktop GUI is local to his/her PC. See the *TME 10 Desktop for Windows User’s Guide* for more information.

The desktop has menus, icons, status lines, and other means to allow these activities. Most of the icons have been shown and defined in the previous sections on resources and managed resources. Figure 7 shows the initial view after the desktop is started. You can see that there are pull-down menu options at the top of the window. These are accessed by clicking the left-mouse button on the option you'd like to expand. Pop-up menus can be seen by clicking the right-mouse button on any of the icons shown in the icon area. These icons represent resources in the TME 10 environment. You can also double-click on any of the icons to open a dialog window that allows more detailed options relating to that icon. A search facility is provided in the center of the window. Operational messages are shown in the message area, and other information can be shown on the status line at the bottom of the window.

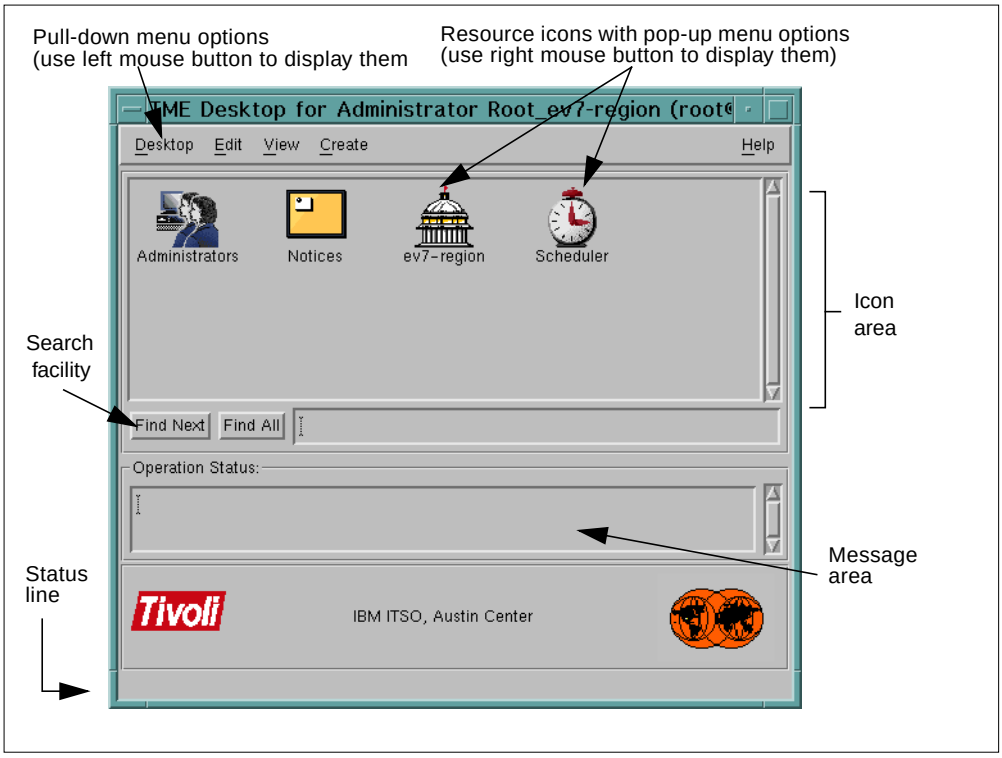


Figure 7. Initial Desktop View

There are five types of resources that can appear on the initial TME 10 desktop view: administrator collection, bulletin board, policy region, scheduler, and generic collection. The first four listed show up by default after the product's initial installation. Generic collections can be added if desired.

Many of the icons are presented in a hierarchical format, and layers of icons may be uncovered by opening new windows to reach information you may be interested in viewing. For example, policy regions can contain hierarchies of subregions within other subregions. The *desktop navigator* function of the GUI provides an alternate method of moving through the hierarchy.

The status line at the bottom of the desktop is a very helpful feature. When you place the mouse pointer over any of the icons, a brief description of that icon's function is given in the status line.

2.2.8 Policy and Policy Regions

In the TME 10 environment, a *policy* is a set of rules that are applied to managed resources. Policies enable you to control the default values of newly-created resources (*default policy*) and to maintain the guidelines when administrators modify or operate on resources (*validation policy*). A specific rule in a policy is referred to as a policy method. A default policy method can supply a constant value or run a shell script or a program that generates a value, whereas a validation policy method usually runs a program or shell script to verify values supplied by the administrator. Administrators can define and maintain policies.

An example of a TME 10 policy is a rule requiring user login names to be eight characters or less. The administrator can create a script that takes the full user name and constructs a user login name that is filled in as a default value (default policy method). He/she would also create a validation script that checks the length of a user login name before the profile is saved (validation policy method).

Policy regions are containers for resources that use the same set of policies. Administrator permissions or roles are assigned to administrators on the basis of policy regions. Therefore, policy regions help to organize the managed resources in the desktop and can be helpful in defining and limiting administrator access to these resources.

The categories of managed resources (managed resource types) and their instances (managed resources) that belong to a certain policy region are defined by the administrator. Before a managed resource can be added to a policy region, its resource type must be added. The types available to be defined to a policy region depend on the TME 10 applications installed. The managed resource types available through the TME 10 Framework software are:

- Managed nodes
- PC managed nodes
- Task libraries
- Profile managers

Policy regions can be arranged hierarchically by creating policy subregions. Each policy subregion has its own subset of resources. When the subregion is initially defined, it has the same policies and managed resource types as its parent. After the initial definition, these things can be changed and are not at all dependent on the parent's definitions.

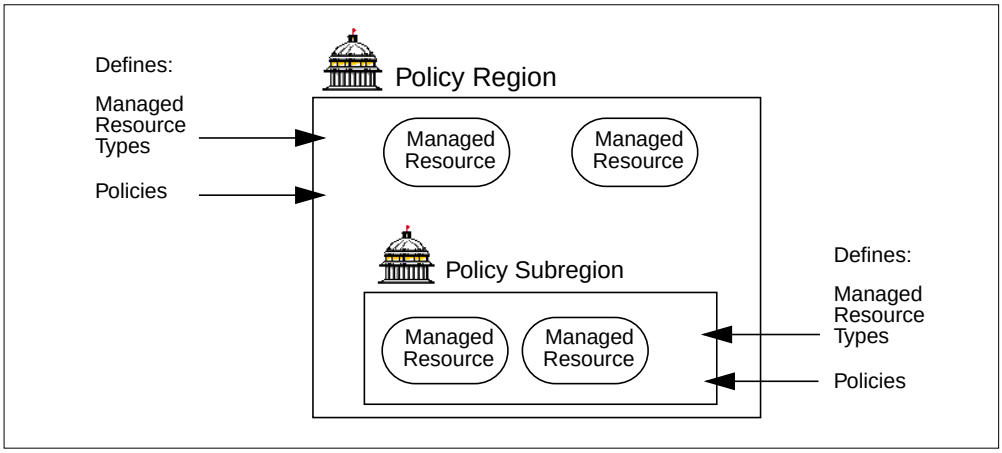


Figure 8. Policy Region with Policy Subregion

The only icons that can appear inside of a policy region's window are those for the managed resource types defined for that policy region and its policy subregions. The policy region's or policy subregion's pop-up menu has the following options:

- **Open...** This option opens the policy region to show the TME 10 managed resources assigned to that policy region.
- **Region Properties...** This option displays a window that lets the administrator change the name of the policy region.
- **Managed Resources...** This option allows the administrator to view and change the types of managed resources that are defined for that policy region.
- **Managed Resource Policies...** This option allows the administrator to change the policy for the different managed resource types within that policy region.

As initially mentioned, policy regions and subregions are collections of resources for which the same set of policies apply. Different criteria can be used to build these entities, such as administrator locations, administrator permission hierarchy, geography, departments, machine types, and so on. The product is so flexible that it can be laid out to reflect each company's individual structure and policies.

2.2.9 Administrators

A TME 10 administrator is someone who has been given authorization to perform management tasks in the TME 10 environment. The TME 10 administrator facility provides a senior administrator the ability to create administrator accounts and assign them the authority to perform tasks. Each administrator then has his or her own TME 10 desktop that reflects the access and control he or she has been given.

2.2.9.1 Authorization Roles

A major concept in TME 10 security is that of *authorization roles*. Authorization roles are predefined names for sets of management task abilities. These roles are discrete, not hierarchical, meaning that each role has specific functions it can perform, and these functions cannot be performed by any of the other roles. The

role or roles given to an administrator will define what that administrator can do to a particular set of resources.

Following is a list of the TME 10 authorization roles and their meanings:

- ***super*** – Allows the administrator to configure the TME 10 environment. Example: Connecting and disconnecting TMRs
- ***senior*** – Allows the administrator to create and define all of the TME 10 resources. Example: Creating a new policy region
- ***admin*** – Allows the administrator to perform day-to-day operation, configuration, and policy tasks. Example: Distributing a set of files to TME 10 clients
- ***user*** – Allows read-only access to the TME 10 environment. This role is required to run the graphical desktop. Example: Displaying configuration of a client machine
- ***backup*** – Allows the administrator to backup the TME 10 databases
- ***restore*** – Allows the administrator to restore TME 10 databases
- ***install_product*** – Allows the administrator to install applications into the local TMR
- ***install_client*** – Allows the administrator to install managed nodes within policy regions that support the managed node resource type
- ***Query_edit*** – Allows the administrator to edit existing queries within a query library
- ***Query_execute*** – Allows the administrator to perform queries using the query facility
- ***Query_view*** – Allows the administrator to view query libraries and queries defined in the query facility

These authorization roles can be delegated for the entire TMR and also for individual resources. Most often, roles are delegated specifically for policy regions. For example, an administrator could be given a senior authorization role in one specific policy region so that he/she could make various changes to that specific group of resources. The same administrator could be given user authorization for the rest of the TMR so that he/she would only be able to view TME 10 configuration, but not make any changes.

2.2.10 Notification (Bulletin Board) Facility

The notification facility provides a way to keep track of what system administration activities are happening. Notices are posted to a graphical bulletin board on the TME 10 desktop.

A *notice* is a message telling the administrator that something has happened or changed in the TME 10 environment. As notices are generated, they are sent to a notice group. A *notice group* is a grouping where notices sharing common types of information are stored. For example, there is a notice group called *TME Authorization*, where notices are sent regarding additions, deletions, and changes to TME 10 system administrators.

Access to the different notices groups is given to each administrator using the administrator facility itself. Each administrator is accessing his/her own

information; so an administrator performing functions on his/her notices and notice groups will not affect the other administrators.

System administrators can read these notices and then save, delete, and forward them as desired. The notices have a time stamp, severity, administrator, identification number, and subject, and they can be filtered, combined, and sorted by many of these fields.

When the TME 10 Framework software is installed, four notice groups are set up:

- *TME Administration* – This group contains notices concerning general TME 10 functions, such as creating and removing resources and installating new applications.
- *TME Authorization* – This group contains notices related to TME 10 administrator creations, deletions, or changes and authorization errors.
- *TME Diagnostics* – This group contains notices generated by TME 10 maintenance activities.
- *TME Scheduler* – This group contains notices concerning the TME 10 scheduler.

The number of notice groups available expands as more TME 10 applications are installed. Installation of applications adds other notice groups. User Administration adds User Management, Group Management and NIS Domains. Notices can also be observed as they are generated by running `wtailnotif`.

2.2.11 Configuration Management

Profiles and profile managers make up the configuration management portion of the TME 10. Together, these two organize, create, and distribute information to remote systems.

2.2.11.1 Profiles

A collection of information corresponding to a system resource is called a *profile*. It contains information that is specific to a certain application and a certain profile type. A profile is stored centrally in a profile database and can be distributed to numerous locations. An example of a profile is a *user profile* in the TME 10 User Administration application or a file package in TME 10 Software Distribution. The TME 10 User Administration user profile is used with UNIX-based systems, Windows NT systems and NetWare systems. It contains information about users, such as the user name, user ID, and user group for each user. This profile is stored on one TME 10 machine in a platform-independent manner. The information contained in the user profile can then be distributed to the machines of different types.

Note About Profiles

The TME 10 Framework provides the profile managers and the distribution capabilities. Profile types are added as additional products are installed in the TME 10 environment. The user profile mentioned above is part of the TME 10 User Administration application and is discussed in Section Chapter 4, “What Is TME 10 User Administration?” on page 65.

Profiles are subject to the default and validation policies defined for them. Profiles are created and maintained in the context of profile managers. Profiles can be changed without immediately putting the changes into effect on the managed machines. The editing and distribution of the profile are two separate functions.

After profiles are created, they can then be copied or cloned. Copying a profile creates an exact copy of the profile. Cloning creates a new profile that contains the same policy definitions, but does not replicate the information contained within the profile.

2.2.11.2 Profile Managers

A profile manager provides a place to create and organize groups of profiles and link recipients to them. A profile manager can contain multiple profiles of the same type, or it can contain profiles of more than one type. Profile managers also control the distribution of profiles and help organize resources.

Profile managers can be managed by creating new profiles, editing existing profiles, and by subscribing and unsubscribing profile endpoints and other profile managers.

2.2.11.3 Subscribers

A *subscriber* is a profile endpoint or another profile manager that receives profile records from the profile manager. A *profile endpoint* is a system that is the final destination for a profile. Examples of profile endpoints can be managed nodes, PC managed nodes, or Network Information System (NIS) domains. In the case of PC managed nodes, the profile would be distributed to the UNIX or NT system sponsoring that PC, which would then distribute to the PC running PC agent software. The same situation would be true for NetWare managed sites. The profile would be distributed to the NetWare server, which would then distribute to its set of clients. Profile endpoints can subscribe to more than one profile manager. Subscribing to a profile manager is the equivalent of subscribing to all of the profiles contained within that profile manager.

Profile managers can also subscribe to other profile managers, thereby creating a subscription hierarchy. When a profile manager is a subscriber, then all of its subscribers become distribution endpoints for the top-most profile manager. This subscription hierarchy yields more flexibility options and control over definition of resources within the profile manager. An example of this hierarchy is shown in Figure 9.

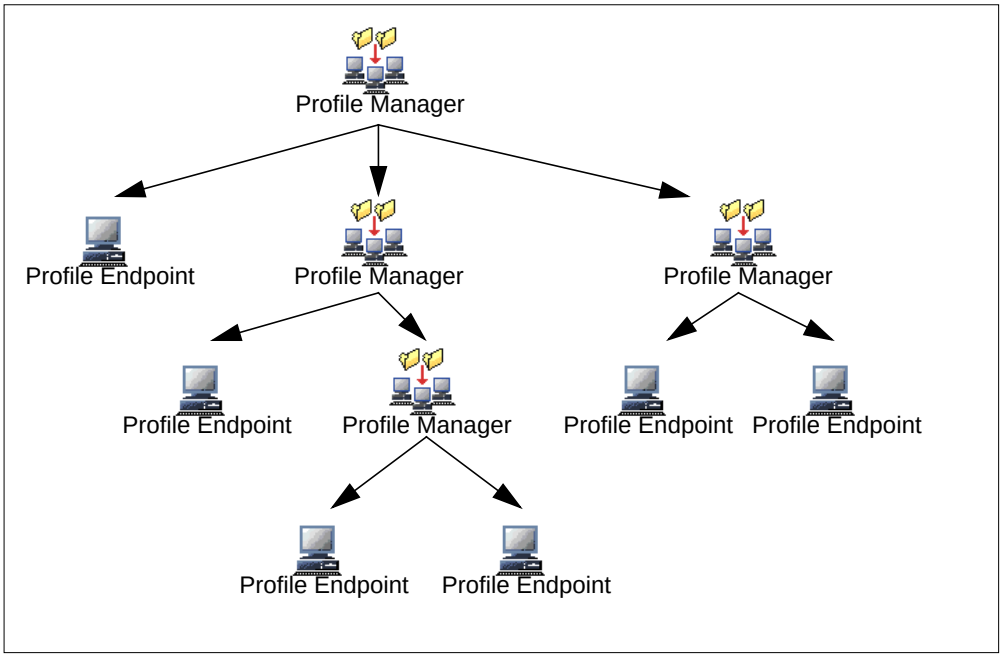


Figure 9. Profile Manager Hierarchy

Note that this subscription hierarchy is the key for simplicity in managing your environment. By creating specific profile managers containing, for example, no profiles but all machines of the same type in a department as subscribers, you build a group of machines subject to distribution of the same information. You then add this profile manager as a subscriber to another profile manager that contains profiles to be distributed. If changes occur in the network, machines can be added to and deleted from this "grouping" profile manager easily and without affecting other TME 10 operations.

2.2.11.4 Distributing Profiles

System configurations on the endpoints are only changed when the profile is distributed to these machines. When profiles are distributed to other profile managers, all that is changed are the profile databases, unless you explicitly distribute to all levels.

When distributing the profile, you can choose whether the distribution will stop at the first level of subscribers or whether it will be distributed to all levels of subscribers. Figure 9 shows a hierarchy of profile managers. If the distribution is stopped at the first level, it would only be distributed to one profile endpoint and to two profile managers; both are the initial level of subscribers of the top-level profile manager. If the distribution is sent to all levels of subscribers, each profile endpoint and profile manager would receive a copy of the profile and systems files would be updated.

The option is also given when distributing a profile of whether to keep or to overwrite local modifications. The option to preserve modification will incorporate local changes made to "downstream" profile copies into the newly distributed information. The option to overwrite will erase any previous information and replace it with the profile's information.

Another means of distribution is to have an endpoint request it to happen. The endpoint will initiate a request to get a new copy of a profile. This will cause the profile to be distributed from the profile manager located one level higher in the hierarchy.

2.2.11.5 Synchronizing Profiles

Sometimes system files and databases of a profile endpoint are changed without using the TME 10 functions, and it may be desired that profiles are then updated to reflect these changes. This can be done with the Synchronize... option of a managed node's menu. The synchronize function works by profile type. Items that exist in the profile database, but do not exist in the system's files or databases, are removed from the profile database. Items that exist in both places, but contain different information, are altered in the profile database to reflect the actual system files or databases residing on that node. For items that exist in the actual system files but not in the profile database, a prompt is given in order to choose the profile to which the items should be added.

2.2.12 Performing Tasks in the TME 10 Environment

A *task library* is a resource that allows an administrator to create tasks and jobs. A *task* is an operation or set of operations that needs to be done within the TME 10 environment routinely. A *job* is a task that is executed on specific managed resources.

2.2.12.1 Task Library

The task library allows tasks and jobs to be created and also provides a place for the storage of binaries, scripts, or programs to be run in the TME 10 environment. Task libraries are created within policy regions, and more than one may be created in any given policy region. They can be arranged arbitrarily, perhaps to accommodate different types of tasks, different types of machines, or another configuration.

2.2.12.2 Tasks

A task that must be performed is defined and stored within a task library, and therefore it can be used repeatedly without having to redefine it. It is also useful to define tasks that grant authority to administrators to perform certain high-level functions without giving them high-level access to the system itself. When a task is created, you must define the following aspects:

- Executables to be run
- Administrator role required
- User ID and user group under which the task will be executed

Different executables may be specified for different platforms, which allows one task icon to perform work on many different operating systems. The executable files can reside on any managed node.

To execute the task one time without creating a job, the following must be defined:

- Task endpoints – The machines on which the task will run
- Format and destination of output
- Execution parameters – Example: time-out value
- Execution mode – Whether the job will run serial, parallel, or staged

After the task has been defined in the task library, it may then be edited or deleted.

2.2.12.3 Jobs

A job is simply a task that is executed on a specific set of managed resources. The task must exist before the job can be created. Several jobs can be created to run the same task, but with different sets of managed resources as task endpoints. When defining a job, the same things must be defined as when executing a task a single time: task endpoints, format and destination of output, execution parameters, and execution mode. Other than the task definitions, the job definitions contain specific target and execution parameters. Once a job is created, it may then be edited or deleted.

2.2.13 Scheduler

The scheduler can be thought of as a service within the TME 10 environment that will perform one-time or periodic scheduling of user-defined jobs as well as other functions, such as a profile distribution. The scheduler is helpful when you have tasks that must be performed on a regular basis or at times when administrators are not available to start the functions themselves.

When scheduling a job to be executed, you must specify the following:

- Start date and time
- If and how the job should be repeated
- Notification that should be performed when the job is complete
- Conditions for cancelling a job
- Scheduling retries if a job fails

After the job has been scheduled, you can edit or delete it from the scheduler.

2.2.14 Light Client Framework: A Glimpse Into the Future

In versions 3.1 and earlier, we have two types of TME 10 clients:

1. TME 10 client running the TME 10 Framework (managed node)
2. Limited-function TME 10 client running a PC agent

The full-function TME 10 clients possess some of the same capabilities as the TMR server, and they maintain a TME 10 database. In all, these clients have a fairly large footprint, and their maintenance and synchronization are expensive for the TMR server. A TMR server can therefore only support approximately 200 full-function clients or managed nodes.

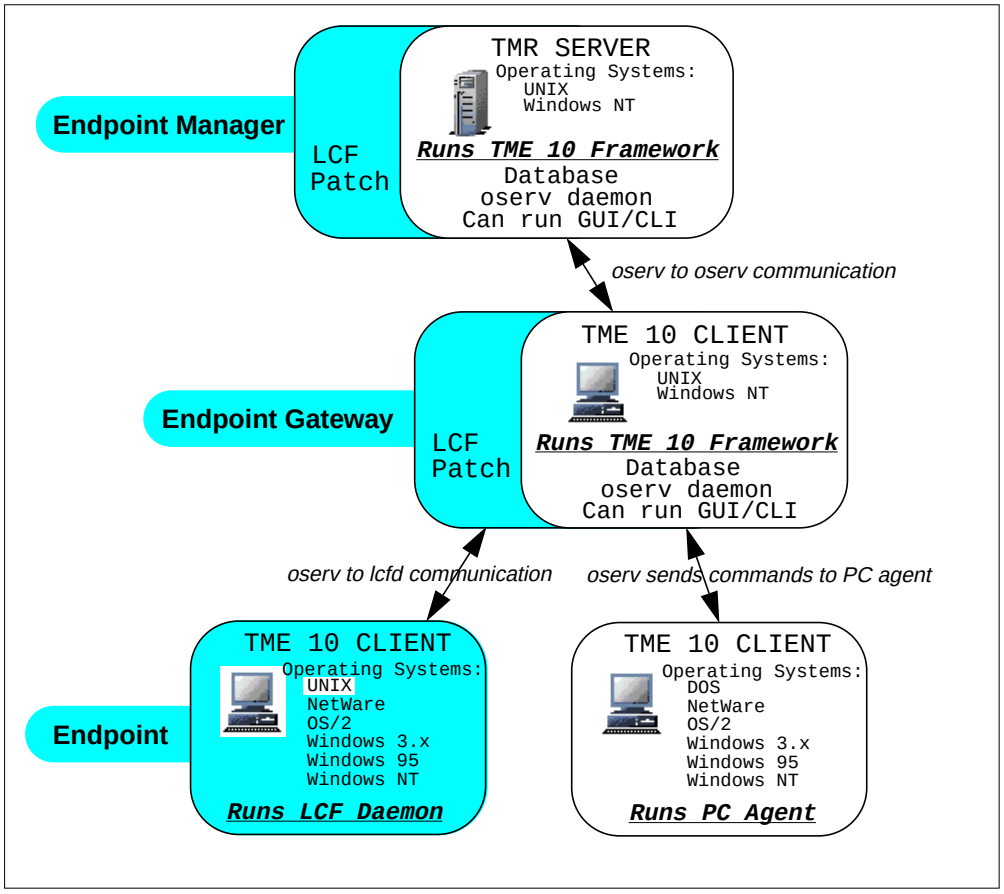


Figure 10. Light Client Framework

The current TME 10 Framework will be extended with a Light Client Framework (LCF) architecture. Figure 10 shows how the LCF elements (shaded) will be added to current TMR configurations. Compare this new environment also with the current basic configuration of a TMR as shown in Figure 4 on page 18.

The new LCF architecture elements are:

- ***Endpoint*** – A workstation running the LCF daemon, which extends TME 10 Framework functionality into PCs, thus eliminating the need for having to split the personality of a PC into a PC managed node and a 'dumb' PC agent. In addition to adding CORBA intelligence, the new endpoints will receive a more dynamic behavior and require less manual configuration. A machine not involved in the daily operations of managing a network computing environment is an endpoint, including UNIX platforms, which is new.
- ***Endpoint Gateway*** – Basically, a managed node as it exists in the current Framework with added functions to support dynamic configurations of endpoints and to take over all endpoint communications, thus relieving the TMR server from some of its control functions. An endpoint gateway is automatically configured as a repeater whose range includes all its assigned endpoints.
- ***Endpoint Manager*** – Is installed on the TMR server and assigns endpoints to endpoint gateways, either when the endpoints first log in to the TME 10 environment or when their assigned gateways become unavailable. The

endpoint manager also maintains an endpoint list that contains information about each endpoint, including a unique identifier, the *odnum*, and the gateway to which it is assigned. In a small environment, the endpoint manager can also be defined as an endpoint gateway.

By extending into the endpoints, the object-oriented Framework becomes three-tiered. The LCF daemon is a small subset of the CORBA runtime that provides sufficient functionality to implement methods, such as the TME 10 Software Distribution filepack methods and the profile endpoint methods. Other parts of the LCF allow endpoint-initiated operations required for applications like TME 10 Distributed Monitoring and TME 10 Inventory.

The endpoint has no database. The information it needs is stored in its proxy managed node's database. A new endpoint logs in to the TME 10 environment with a broadcast message which is routed to the endpoint manager. The endpoint manager configures the new endpoint into the endpoint list, assigns an endpoint gateway, and informs both the endpoint gateway and the endpoint of their new relationship. From then on, all communications between the endpoint and the rest of the TME 10 environment go through that gateway.

The endpoints initially do not have any methods. When a method is called, the LCF daemon checks its cache, and if the method is not there, it is downloaded from the associated gateway.

The main benefit of the new LCF architecture extension will be:

- An huge increase in scalability. The number of managed nodes will still be limited to 200. However, the number of TME 10 clients with managed node-like functionality in a TMR can now be in the tens of thousands.
- Endpoints need not be statically configured anymore. Strong support for DHCP-connected (Dynamic Host Configuration Protocol) clients and dynamic creation and configuration of endpoint definitions.

From a TME 10 application point of view, the new architecture will not change a lot in the way they work. For instance, the TME 10 Software Distribution or TME 10 Inventory will work the same way with the endpoints as they do with PC managed nodes now. What changes is the TME 10 Framework underneath. With the introduction of endpoints, which can be considered dataless managed nodes, we will see two major differences:

- Profile distributions to subscribed endpoints will be dataless, meaning that no local profile copy is created in the endpoints as is the case with *real* managed nodes. The actions related to the profile, however, will be performed like on managed nodes.
- More TME 10 applications will be able to run on the PC platform, such as the TME 10 Distributed Monitoring and the TME 10 Enterprise Console event adapters.

While TME 10 applications will be enhanced to support the new LCF clients, we will see a transition period in which some applications need the current PC managed node/PC agent configuration and others the endpoint functions. Mixed environments will be supported until PC managed nodes, and also NetWare managed sites, are no longer required.

Chapter 3. User and Group Management Concepts

This chapter introduces terminology and concepts used in each specific environment: UNIX, NIS, Windows NT, NetWare NDS, and RACF. It is important to understand these concepts before implementing TME 10 User Administration on any of these platforms.

3.1 UNIX User and Group Management

This section gives a description of user and group management in AIX. Note that this information might slightly differ from one UNIX system to another. At the end of this section, we will highlight some differences with other UNIX platforms in terms of user and group system configuration files, default system users and groups. For more details on the different flavors of UNIX systems, you can refer to the following publication: *Essential System Administration,* Aeleen Frisch, O'Reilly & Associates, Inc. - ISBN 1-56592-127-5.

3.1.1 Logon Process

A user must be authenticated to the UNIX operating system by entering a valid user name and, optionally, a valid password which is never echoed in clear text when the user authenticates. The user ID is checked against entries in the /etc/passwd file, and the password is checked against the /etc/security/passwd file on the local system.

However, UNIX allows authentication via remote databases such as Network Information System (NIS) and Distributed Computing Environment (DCE).

Once a login session is granted, the user's environment is created. The system sets up a global environment, then proceeds to set up the user's private environment. The global environment is usually created from the /etc/profile and the /etc/environment files that are systemwide files. These files are used to set environment variables for most users on the system. They can also be used to set read-only environment variables that a user cannot modify or remove.

A user's private environment comes from the user's .profile file and other files usually contained in the user's home directory.

3.1.2 User Identification and Authentication

Each user on a UNIX system is identified by a unique user identifier number or UID and a primary group identifier or GID. These numbers are automatically set by the system, but can be set manually by the system administrator.

Users typically use their user name even though the system tracks all ownerships and access rights by the user UID. The translation is performed by way of the /etc/passwd file, as people tend to remember names while the system tends to work with numbers, or UIDs.

After successful login, UNIX assigns to the user a Login User ID (LUID) which for audit reasons never changes, an Effective and Real User ID (EUID and RUID), and an Effective and Real Group ID (EGID and RGID) as well as secondary groups.

A user can switch to another user with the su command. This command cannot change the LUID to keep track of the original user that logged into the system.

The possibility for another user to su to a user can be disabled by the system administrator or by the security administrator.

3.1.3 Access Control Lists (ACLs)

Once a user has been authenticated, authorization must be granted to a single object resource (file or directory) by the subjects (users or processes). UNIX provides permissions for owner, group, and others that are Read (r), Write (w), and Execute (x).

In addition, some UNIX systems also allow for the use of a B3 security feature, the Access Control Lists or ACLs, to further define access permissions to files and directories. In general, these ACLs are used to specify individual users in a more granular method. ACLs allow a user to define specific permissions to a list of discrete users, beyond that provided by the regular User-Group-Others permissions methodology.

The commands to deal with ACLs are usually included in the operating system. For AIX, these commands are `aclget` to get the ACL of a file, `aclput` to set the ACL, and `acledit` to get and set the ACL. However, the use of ACLs is strictly optional and is not global in nature. That is to say, one directory can use ACLs while another may use the standard Owner-Group-Other permissions. The base AIX operating system does not use ACLs, by default, to control access to system files.

3.1.4 Users and Groups

Each user on the system is a member of at least one group. These groups are comprised of users that require similar access rights and permissions. By using the group permissions, access to a file or directory can be granted to a group of users so that many people can access that file easily. The default group used for most users is called the `staff` group. System administrators can create groups and assign users to groups as needed. Also, an individual user can simultaneously be a member of several groups.

In all UNIX systems, there are standard system groups and users that are predefined when the system is installed. These groups and users might be slightly different from one system to another.

3.1.4.1 Built-In Groups

This is a list of predefined groups in AIX:

- `system` is used by system administrators. User root is a member of this group by default.
- `staff` is the default user group. User daemon is a member of this group by default.
- `bin` is a system group. Users root and bin are members of this group by default.
- `sys` is a system group. Users root, bin and sys are members of this group by default.

- `adm` is a system group. Users bin and adm are members of this group by default.
- `uucp` contains the uucp user.
- `mail`: members of this group can use the `mail` commands. This group does not have any members by default.
- `security` is used by security users. User root is a member of this group by default.
- `cron` is used for scheduling activities. User root is a member of this group by default.
- `printq` is used for printer administration. This group does not have any members by default.
- audit is used for auditing the system. User root is a member of this group by default.
- `ecs` is used for IBM connection facilities.
- `nobody`. User nobody and lpd are members of this group by default.
- `usr`. User guest is a member of this group by default.
- `perf`. This group does not have any members by default.

3.1.4.2 Built-In Users

This is a list of predefined users in AIX:

- `root` is the owner of all resources.
- `daemon` owns the system daemons.
- `bin` owns the system executable files.
- `sys` owns the system devices.
- `adm` owns the system utilities.
- `uucp` owns the `uucp` program.
- `guest` is the guest account.
- `nobody` is a user used, for example, by NFS when a root user tries to access to a file mounted via NFS. It has the same rights as others.
- `lpd` owns the printer spooler utilities.

3.1.4.3 System Administrator (root)

The system administrator, commonly referred to as the root user or the super user, is the master user of the system. The administrator has most of the responsibility for securing the system. For the most part, the root user is not screened from issuing any commands or operations.

In fact, one of the first access-permission-related checks is to see if the user issuing a command/request is the root user. If it is, then no further permission checking is performed, such as checking Owner-Group-Others access permissions. The command is performed no matter how adverse it may be to the overall system health and safety, although some commands do have the occasional verification step included. For the most part, however, it is assumed that the root user knows what he or she is doing.

Note

One of the most vital security-related tasks for a system administrator is to secure and protect access to the root account. Many “hacker attacks” are centered around becoming the root user so that any trace of the attack can be hidden.

3.1.4.4 Account Policy

The Account Policy comprises the following functions. This list is not exhaustive and can differ from one system to another.

- Expiration date
- Allowed login times
- Number of failed logins before user is locked
- Login authentication grammar
- Valid TTYs
- Days to WARN USER before password expires
- Maximum password age
- Minimum password age
- Minimum password length
- Minimum alphanumeric characters
- Minimum other characters
- Maximum repeated characters
- Minimum different characters
- Password uniqueness
- Disconnect remote users when logon hours expire
- Account lockout
- Workstation lockout

3.1.4.5 User Profiles

At the creation of a user, a profile is created in the user’s home directory (.profile file). This file is executed each time the user logs in. Variables can be set in this file, and specific applications can be started.

3.1.4.6 Home Directories

At the creation of a user, a home directory must be specified. All a user’s personal data will be stored by default in this directory. This directory is local to the system on which the user logged in, but can be remote if accessed through NFS or DCE/DFS.

3.1.5 Main User and Group Related Files

UNIX uses several files to manage and maintain security aspects of the operating system, user and groups accounts. Most security-related files can only be accessed by the operating system or by the administrative user. Below is a list of the most frequently used files:

- **/etc/passwd**

  This is the master users list. This file can normally be viewed by any user on the system, but cannot be modified by non-privileged users. It contains one line for each user of the system. A sample line may look like:

  ```
  joeuser:!:200:200:Joe the User:/u/joeuser:/bin/ksh
  ```

  Each line is a list of attributes as follows, separated by colons:

  - The user login name (joeuser), limited to eight characters.
  - Password attribute: An asterisk indicates that the password is invalid, and the exclamation point indicates that the password is in the /etc/security/passwd file.
  - The UID of the user.
  - The primary group ID (GID) that the user is a member of. The primary group is the default group for newly created files and directories.
  - The GECOS field. This is a free-form field that usually contains identifying information such as the user's full name.
  - The home directory for this user. This is the user's private directory.
  - The user's default shell, although the user can normally execute other shells if so desired.

- **/etc/security/passwd**

  This is the password file. It is a stanza-based file that contains one stanza per user. A sample entry may look like this:

  ```
  joeuser:
      password = DD1cQ1OctBCn.
      lastupdate = 818269778
      flags = ADMCHG
  ```

  - `Password` is the encrypted password for that user.
  - `lastupdate` is the last time the password was changed. This is used in cases where password aging has been enabled.
  - `flags` are additional flags turned on by the system. In this case, the `ADMCHG` flag is on, indicating that the system administrator has set the user's password. The user will be automatically prompted to change it the first time he or she logs onto the system.

  Note: The user may be disabled from issuing certain commands on that system until the `ADMCHG` flag is removed by changing the password.

- **/etc/group**

  This is the list of groups defined on the system. A sample entry may look like:

  ```
  staff:!:1:rick,John,yvesbex,notes
  ```

  Each line is a list of attributes separated by colons.

  - The group name
  - The group ID (GID)
  - The list of users belonging to that group

- **/etc/security/group**

  This file contains additional information for each group with the adm and adms flags. The adms flag lists the users that have administrative authority on the group, and the adm flag determines if the group is an administrative group or not. Below is an example of a /etc/security/group file.

```
staff:
        admin           = false

sys:
        admin           = true

usr:
        admin           = false

uucp:
        admin           = true

webusers:
        admin           = true

tivoli:
        adms = root
```

There are other files in the /etc/security directory that control what the default attributes of a new user will be and how they are created. In addition, certain files that track invalid login attempts are stored in the /etc/security directory as well as backup copies of important files like /etc/password and so on.

Notes:

- Passwords stored in the /etc/security/passwd file are encrypted.
- Access to the /etc/security directory is limited to the administrative user and to the security user only.

3.1.6 User and Group Configuration Files

User and group configuration files vary from one UNIX flavor to another. You will find in Table 1 a summary of the user and group configuration files for each flavor of UNIX supported by TME 10 User Administration. For more information on the format of these files, you can refer to *Appendix A Configuration Files and System Directories* in *TME 10 User Administration User and Group Management Guide Version 3.1*.

Table 1. User and Group Configuration Files

Platform	File
AIX V3.2.5 , V4.1, V4.2	/etc/passwd
	/etc/group
	/etc/security/passwd
	/etc/security/group
HP-UX 9.0	/etc/passwd

Platform	File
	/etc/group
	/.secure/etc/passwd
	/.secure/etc/group
Solaris	/etc/passwd
	/etc/shadow
	/etc/group
	/etc/group.secure
SunOS 4.1.x	/etc/passwd
	/etc/group
	/etc/security/passwd.adjunct
	/etc/security/group.adjunct

3.1.7 Standard User and Group Accounts

The standard system user and group accounts vary from one UNIX platform to another. It is very important to be aware of those differences if you are using TME 10 User Administration in an heteregeneous environment. You will find in Table 2 a summary of the user and group accounts that are created by default on a UNIX system at installation time. For more information on these users and groups such as the users' roles, and the default members of these groups, you can refer to *Appendix A Configuration Files and System Directories* in *TME 10 User Administration User and Group Management Guide Version 3.1*.

Table 2. Standard System User and Group Accounts in UNIX (Part 1)

Platform	User Accounts	UID	Group Accounts	GID
AIX V3.2.5, V4.1, V4.2	root	0	system	0
	daemon	1	staff	1
	bin	2	bin	2
	sys	3	sys	3
	adm	4	adm	4
	uucp	5	uucp	5
	nobody	4294967294		
	lpd	9		
HP-UX	root	0		
	daemon	1		
	bin	2		
	adm	4		
	uucp	5		

Platform	User Accounts	UID	Group Accounts	GID
	lp	9		
	hpdb	27		

Table 3. Standard System User and Group Accounts in UNIX (Part 2)

Platform	User Accounts	UID	Group Accounts	GID
Solaris	root	0	root	0
	daemon	1	other	1
	bin	2	bin	2
	sys	3	sys	3
	adm	4	adm	4
	lp	71	uucp	5
	smtp	0	mail	6
	uucp	5	tty	7
	nuucp	9	lp	8
	listen	37	nuucp	9
	nobody	60001	staff	10
	noaccess	60002	daemon	12
			nobody	60001
			noaccess	60002
SunOS	root	0	wheel	0
	nobody	65534	nogroup	65534
	daemon	1	daemon	1
	sys	2	kmem	2
	bin	3	bin	3
	uucp	4	tty	4
	news	6	operator	5
	ingres	7	uucp	8
	audit	9	audit	9
	sync	1	staff	10
	sysdiag	0	other	20
	sundiag	0		

3.2 Network Information System (NIS)

Network Information Service (NIS) is a useful UNIX tool to assist in administering a large number of systems. The main purpose of NIS is to distribute up-to-date information from UNIX files used for user management, system management, and network management. NIS can also be used to distribute information from your own files.

NIS is most commonly used to keep user names, user IDs, passwords, group names and group IDs consistent across many systems. This is a way to centrally manage users and groups in a distributed UNIX environment.

3.2.1 NIS Maps and Servers

NIS does not distribute the actual files containing the data. It uses the information in the files to build an NIS *map,* which is really a database file created and accessed by NIS clients. NIS uses the dbm database supplied as standard with NIS. Note that dbm is a very simple database and is not designed to provide the facilities, robustness and performance of commercial Relational Database Management System (RDBMS) products.

The information in the NIS maps is kept on a *master server*, which controls the information. Additional *slave servers* can hold copies of the information controlled by the master server; so performance and availability of information is improved.

The availibility of this information is crucial since it can include such things as hostname to IP mapping (/etc/hosts), user names and passwords (/etc/passwd, /etc/security/passwd). If the master server is not available and there is no slave server, a network of systems can be completely disrupted, with no systems operational.

Figure 4 shows the NIS maps that are created from UNIX files and other information on the master server that can be administered by NIS.

Table 4. NIS Default Maps

Map	NIS Nickname	Files Used to Create Map
passwd.byname	passwd	/etc/passwd, /etc/security/passwd
passwd.byuid		
group.byname	group	/etc/group
group.bygid		
hosts.byaddr	hosts	/etc/hosts
hosts.byname		
ethers.byaddr	ethers	/etc/ethers
ethers.byname		
networks.byaddr	networks	/etc/networks
networks.byname		
rpc.bynumber		/etc/rpc
services.byname	services	/etc/services

Map	NIS Nickname	Files Used to Create Map
protocols.byname	protocols	/etc/protocols
protocols.bynumber		
netgroup		/etc/netgroup
netgroup.byhost		
netgroup.byuser		
bootparams		/etc/bootparams
mail.aliases	aliases	/etc/aliases
mail.byaddr		
publickey.byname		/etc/publickey
netid.byname		/etc/passwd, /etc/group, /etc/hosts, /etc/netid
netmasks.byaddr		/etc/netmasks
ypservers		(obtained from network broadcast)

Some NIS maps replace local UNIX files so that when NIS is running, the information in the NIS maps is used instead of the information in the UNIX files. Other NIS maps can be logically appended to local UNIX files. This allows private and local information to be held on the NIS client.

NIS's data and most NIS commands are stored in the NIS /var/yp, /usr/etc/var or /etc/yp directory, depending on the UNIX flavor. Each NIS map is stored in a subdirectory, <NIS_domain_name>, as a pair of NDBM files. NDBM is the format used by the DBM database: <map_name>.dir and <map_name>.pag.

For example, let's suppose we have an NIS domain called NISDomain comprised of AIX systems. The password maps will be stored as:

```
/var/yp/NISDomain/passwd.byname.dir
/var/yp/NISDomain/passwd.byname.pag
/var/yp/NISDomain/passwd.byuid.dir
/var/yp/NISDomain/passwd.byuid.pag
```

NIS maps can be built by running the `make` command located under the NIS directory. This command will use a predefined Makefile located in that directory. `make` will check for each system file (for example passwd), and if the file has been modified or is still up-to-date, it will generate the corresponding NIS maps.

3.2.2 NIS Domains

An NIS domain is a collection of NIS maps that are used by one or more NIS clients. A client can belong to a number of NIS domains.

NIS domains and Domain Name System (DNS) domains are two separate entities. However, if NIS is used for hostname-to-IP address mapping, there might be some conflict with an existing DNS that also maps hostnames to IP addresses. NIS can be set up to operate with DNS so that any hostname resolution is first tried using DNS, and if the hostname is not found, the request is passed to NIS.

3.2.3 NIS Clients

A client system can request information from any server that matches its domain (or domains). A client can belong to one or more domains. NIS client systems run the `ypbind` daemon. When the `ypbind` deamon starts, it broadcasts a request for each domain used by that client. The NIS server chosen continues to be used for that domain by the NIS client until the server is unavailable (the NIS timeout is reached). The NIS timeout defaults to 20 seconds and can be set to a different value with the `TIMEOUT` variable.

An NIS server can also run the `ypbind` daemon and be a client of itself. This is usualy the case; the NIS server runs both the server (`ypserv`) and client NIS daemons.

On the NIS client, local users and groups can be maintained. This is done by adding a + at the end of the /etc/passwd file and the /etc/group file. All users and groups defined before that plus sign are local to the system. Thus the NIS maps on the server will not be checked for these users/groups.

3.2.4 NIS Netgroups

In order to assist in managing groups of users and hosts, NIS supports `netgroups`. Netgroups are definitions that consist of defined users, hosts and domains. Netgroup entries have the form of:

netgroup_name (host_name, user_name, domain_name) (host_name, ...)

Netgroups are used as a shorthand way to include host, user and domain information into NIS maps. Each NIS map only uses the information applicable to it.

3.2.5 NIS Daemons

NIS relies on daemons on both client and server systems.

Figure 5 shows where the NIS daemons are running and their purposes.

Table 5. NIS Daemons

NIS Daemon	Server or Client	Purpose
ypbind	Client (server can also be a client)	Used to obtain information from NIS server
ypserv	NIS master or slave server	Provides map information to clients
ypupdated	NIS master server	Prompts slave servers to update their maps
yppasswdd	NIS master server	Processes requests to change user's passwords
keyserv	NIS clients and servers running secure NIS	Provides security services for Secure NIS

3.3 Windows NT

This section provides an overview of the Windows NT security model, network models, global groups, local groups, and user accounts.

3.3.1 Windows NT Security Model Overview

The key objective of the Windows NT security model is to regulate access to objects. The security model maintains security information for each user, group, and object. It can identify access attempts that are made directly by a user, and it can identify access attempts that are made indirectly by a program or other process running on a user's behalf. Windows NT also tracks and controls access to objects that users can see in the user interface (such as files and printers) and to objects that users can't see (such as processes and named pipes).

Security in Windows NT has been included as part of the original design of the operating system. The main components of the security subsystem are:

- The Local Security Authority
- The Security Account Manager
- The Security Reference Monitor

Windows NT also offers components such as the logon process, Discretionary Access Control, Access Tokens and Access Control Lists.

3.3.1.1 Local Security Authority (LSA)

The LSA ensures that the user has permission to access the system. It creates access tokens during the logon process, manages the security policies, controls the audit policies, and logs audit messages to the event log.

3.3.1.2 Security Account Manager

The Security Account Manager (SAM) maintains the users/groups account database. This database contains information for all user and group accounts. It provides user validation services. These services are actually used by the LSA. SAM also compares the user input in the Logon Information dialog box (dialog box that appears on the screen when entering Ctrl+Alt+Del) with the SAM database.

When creating a user account, SAM provides a security identifier (SID) for the user and the SID of any groups the user is a member of. The SID is a 32-bit number generated by the system that is used to uniquely identify each account on the system (or domain). It is similar to the UNIX User ID (UID) number, but unlike UNIX, system administrators do not have the option of editing this number. The Windows NT SID is assigned by the system only, and it is unique. Two users on two different machines cannot have the same SID.

Note: If a user is deleted and then re-created later, the user will be given/assigned a different SID.

3.3.1.3 Security Reference Monitor

The Security Reference Monitor (SRM) is responsible for validating access to objects or resources (files, directories, printers, and so on). It protects resources from unauthorized access or modification and generates the corresponding audit messages.

In Windows NT, users cannot directly access resources. User requests for accessing a resource must be validated by the SRM.

3.3.1.4 Logon Process

In order to log into a system or a domain, the user must enter the Ctrl+Alt+Del key sequence to display the Logon Information dialog box. This key sequence prevents against any application running in the background, such as a Trojan Horse, that attempts to capture the user's logon information.

The user must then enter the username and password and specify whether or not to log on to the local computer or to the domain.

Note: At logon, a domain can be selected only if the computer participates in a domain.

The system first checks in the SAM database to see if the user exists and if the password is valid. It will reject the connection if one of the entries is invalid without saying if the user does not exist or if the password is incorrect (this is done intentionally).

If the user has an account and the password is valid, then the security subsystem creates an *access token*. This token represents the user. It contains information such as the user's Security ID (SID), the username, and the groups to which the user belongs.

This access token (or a copy of it) is associated with each process started by the user. The access token and process association is called a *subject*. When accessing a resource (file, directory and so on), the content of the subject is checked against the Access Control List of the object being accessed by an access validation routine.

3.3.1.5 Discretionary Access Controls

Discretionary Access Controls (DACs) allow the owner of a resource to determine who can access the resource and with which permissions (Read, Write, Execute, Delete, Change Permissions, and Take Ownership). Resources include files, directories, printers, network shares, and other objects.

3.3.1.6 Access Control Lists

ACLs are a form of Discretionary Access Control. ACLs work in conjunction with the file system. They allow the owner of a resource to specify who can share that object and who is denied access to that particular object. An ACL is associated with each object. The ACL contains Access Control Entries (ACEs). Each ACE grants or denies access to a group of users or to a specific user.

3.3.1.7 Access Tokens

When a user starts a process, an access token is created. This token contains the SID and a list of groups the user belongs to. The token is associated with the process. When the process tries to access a resource (for example, open a file), the content of the token is checked against the file's ACLs to see if the user is allowed to open that file. If ACLs include permissions for that user, the user will be able to access the object (open the file).

3.3.1.8 Rights Versus Permissions

Rights are operations that a group of users or a specific user is allowed to perform. For example, by default, a member of the built-in Administrators group can modify or delete a user account.

Permissions are operations that can be performed on a resource. For example, if a file has read permission for a specific group, members of this group will be granted only read access to that file.

3.3.2 Windows NT Networking Models

It is very important to understand that Windows NT can be networked in two models:, **workgroup** and **domain**.

In a workgroup environment, each computer maintains its own SAM database. When a user logs into a computer, SAM checks that the user exists in the user database on that computer. Maintaining a user database on each machine is quite a task when the number of machines grows and when users need to work on any machine.

A Windows NT domain allows for managing of a centralized user account database. Domain users and groups are defined in a centralized SAM database physically located on the Primary Domain Controller (PDC) as well as on the Backup Domain Controllers (BDC). The SAM database on the BDC is just a replica of the master SAM database located on the PDC. However, each computer that is part of the domain can have its own local SAM database. Thus, a user can log into a computer or log into the domain. If a user wants to log into the local computer, the local SAM database will be accessed. If the user wants to log into the domain, the centralized database will be accessed directly on the PDC or on the BDC if the PDC is down.

3.3.3 Users and Groups

3.3.3.1 Local Groups and Global Groups

All users in Windows NT are assigned to one or more groups. Grouping users simplifies the management of resource access since you can grant a group of users access to a specific resource.

The Windows NT security model supports three types of accounts:

- User Accounts
- Local Groups
- Global Groups

Local Groups can be defined on each machine. A local group is local to the machine, meaning that rights and permissions associated with these local groups work with local resources. Windows NT supplies some built-in local groups (listed below) on each machine.

If the machine is a stand-alone machine, only local user accounts can belong to a local group. If the machine is a member of a domain, the local group can contain local user accounts, domain user accounts, trusted domain user accounts, and global groups from the domain or from a trusted domain.

Global groups are defined at the domain level and can be exported to remote domains. Members of global groups are domain user accounts or trusted domain user accounts. A local group cannot be a member of a global group. Windows NT supplies several built-in global group accounts.

Built-In Local Groups

Windows NT Workstation and Server, when used as stand-alone systems (not part of a domain), have built-in local groups:

- **Administrators**

  Members of this group can fully administer the computer. The Administrator user is, by default, part of this group.

- **Backup Operators**

  Members of this group can bypass file security to back up files. By default, no users are part of this group.

- **Guests**

  This group contains users granted guest access to the computer/domain. The user guest is, by default, a member of this group.

- **Power Users**

  Members of this group can share directories and printers. No user is member of this group, by default.

- **Replicator (Windows NT Server only)**

  Members of this group support file replication in a domain. By default, no user is a member of this group.

Windows NT Server, when part of a domain, has some additional built-in local groups:

- **Account Operators**

  Members of this group can administer domain users and group accounts. This group has no members, by default.

- **Domain Administrators**

  Members of this group can fully administer the computer/domain. User Administrator and Domain Admin global group are members of this group, by default.

- **Server Operators**

  Members of this group can administer domain servers. This group does not have any members, by default.

- **Account Operators**

  Members of this group can administer domain users and group accounts. This group does not have any members, by default.

- **Print Operators**

  Members of this group can administer printers in a domain. This group does not have members, by default.

Special Groups

There are also some additional special groups that will not show up in the list of groups under User Manager or User Manager for Domain. These groups cannot be assigned to users by the administrators. They are automatically assigned to users by the system.

- **Network**

This group includes any user who is currently connected from another computer on the network to a shared resource on the local computer.

- **Interactive**

  A user who logs in locally is automatically included in the Interactive group at logon. Members of this group access resources on the computer on which they are directly logged.

- **Everyone**

  This group includes all users that access the computer, locally or remotely. This includes guests and users from other domains as well as interactive and network users. By default, when creating a network share, this share is accessible by all members of the group Everyone.

- **Creator Owner**

  This group includes the user account that created or took ownership of a resource.

- **System**

  This group refers to the system itself.

Built-In Global Groups

In addition, Windows NT Server, when part of a domain, has the following built-in global groups:

- **Domain Admins**

  This group contains designated administrators of the domain. User Administrator is a member of this group, by default. Members of this group can administer the Primary and Secondary Domain Controller.

- **Domain Guests**

  This group contains all domain guests users. User Guest is, by default, a member of this group.

- **Domain Users**

  This group contains all domain users. All global domain users are part of this group.

3.3.3.2 User Accounts

A user account comprises all information related to that user account: username, password, groups to which the user belongs, and rights and permissions.

The account security policy controls the way passwords are changed and assigned, and the user account policy controls the explicit rights that can be assigned to the groups of users and user accounts.

Account Policy

The Account Policy comprises the following functions:

- Maximum password age
- Minimum password age
- Minimum password length
- Password uniqueness
- Disconnect remote users when logon hours expire

- Account lockout
- Workstation lockout

Users Rights Policy
User Rights authorize a user to perform specific actions in Windows NT. When you log on to the computer using an account that has been granted the right to carry out an action, Windows NT will let you proceed.

For example, if you want to back up the partition, you need a ‘Back up files and directories’ right that is assigned to Administrators and Backup Operators.

User Profiles
A user profile is a file or directory with a collection of files containing information about the user’s environment. The user profile is loaded each time the user logs on. Modifications to the environment made by the user are saved in that profile when the user logs off.

There are actually different types of profiles: mandatory user profiles, personal user profiles, user default profile, and system default profiles.

A mandatory user profile can be set by the system administrator to users in a domain. This profile defines which environment settings must be set when a user logs on as well as which application must be started and which network drive must be connected. If a user makes any changes to the environment, these changes will not be saved when the user logs off.

A personal user profile (when assigned to a user) can be modified by the user, and changes are saved when the user logs off. The user will retrieve the previous environment after login.

The user default profile is the standard Windows NT default profile that is used when a user account has not been assigned a profile or when a user has never logged onto the system. Also, if a user profile cannot be accessed when a user logs in, the user default profile is assigned.

The system default profile is the one that appears when nobody is logged in (when the Ctrl+Alt+Del dialog box is displayed).

Home Directories
A home directory can be assigned to each user for storing personal files. The home directory is the default directory in which user files will be saved and from which user files will be opened.

Logon Scripts
A logon script is a batch file (.CMD or .BAT extension) or an executable file (.EXE extension) that is executed when the user logs in. Such a script can start a network connection, execute a specific application or configure the user environment. The script is executed after the user is logged in.

3.3.3.3 Users and Groups Management Interface
To manage users and groups, Windows NT provides the User Manager interface in Windows NT Workstation and in Windows NT Server when they are used as stand-alone systems. The User Manager for Domains interface is provided in Windows NT Server when part of a domain.

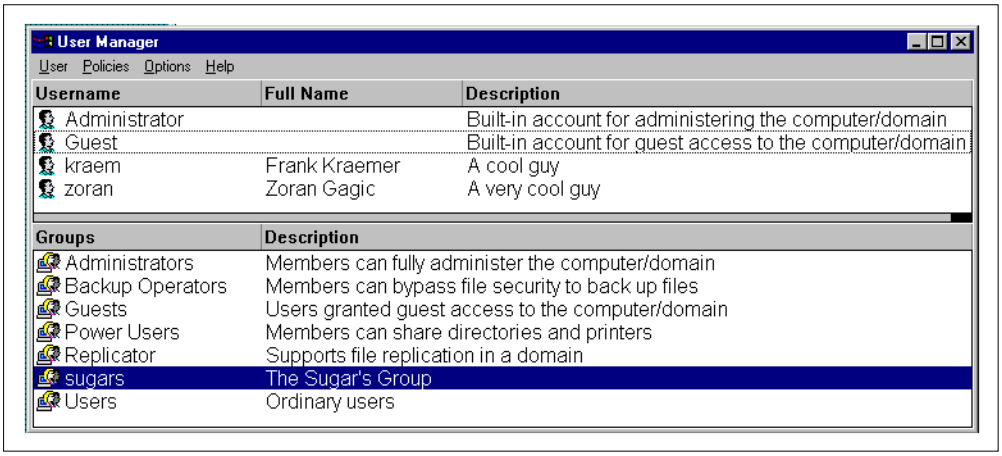


Figure 11. Windows NT User Manager

User Manager provides the facilities for managing users and groups such as create and modify user accounts, set account policies, set up auditing for users activities (logon/logoff, system object access and so on), create, delete, modify groups, grant user rights, create and modify trust relationships.

3.4 NetWare NDS

Novell Directory Services (NDS) is an information database service introduced in NetWare 4.0 that organizes network resources such as users, groups, printers, volumes and other physical network devices into a hierarchical tree structure. NDS has facilities for storing, accessing, managing and using information about network resources and provides global access to all network resources regardless of where they are physically located, forming a simple information system.

NDS treats all network resources, users, groups, printers, and volumes as individual objects in a distributed data base known as the NetWare Directory Infobase. The database organizes resources in hierarchical tree structure, independent of their physical location. Users and supervisors can access any network services without having to know the physical location of the server that stores the service. "Directory" means the global database provided by NetWare 4 servers.

The Directory replaces the bindery, which served as the system database in previous versions of NetWare. While the bindery supports the operation of a single NetWare server, NDS supports an entire network of servers. Instead of storing all the information in one server that can be a single point of failure, information is distributed over a global data base and accessed by all servers. NDS helps in managing directory resources such as NetWare users, servers, and volumes. Graphical and text tools provide administrative functions to manage the NDS and the file system.

It is very important to understand that the NetWare 4 directory structure and the file system (directories, files, applications) are separate, distinct hierarchical structures. Files and directories are not objects and are not in the NDS data

base. For example, trustee rights that are assigned in the directory to a Volume object do not flow down to directories and files in that volume.

Instead of logging in or attaching to individual servers, if NDS name context is properly set, users can log in to the network by typing:

```
LOGIN <USER_NAME>
```

instead of

```
LOGIN <SERVER_NAME>/<USER_NAME>
```

When a user accesses resources on the network, background authentication processes verify that the user has rights to those resources. Authentication allows a user to access any servers, volumes, printers, and so on in the network to which the users has rights. User trustee rights in the directory restrict the users's access within the network. Authentication is a means of verifying that a user is authorized to use both directory and file system resources. Aunthentication works in combination with the Access Control List (ACL) to provide network security.

3.4.1 NDS Objects

NDS is object oriented. Physical devices are represented by objects or logical representations of physical devices. Users and groups are logical user accounts and group accounts and are one type of NDS object. One of the benefits of working with an object-oriented system is that moving a device does not change the object's definition. This makes system administration much easier.

The key terms used in NDS are:

- **Objects**

  Objects, are logical objects, representations of physical resources, users and end user-related entries, such as groups. For example, a User object is one of over 20 different NDS object types; a Printer object is another type of NDS object.

- **Object Properties**

  Object properties are different types of information associated with an NDS object. For example, a User Login Script is one of 59 object properties associated with a user object.

- **Property Values**

  Property values are simply names and descriptions associated with an NDS object. For example, HP3 might be the property value for the printer name object property, which is in turn associated with the Printer Object.

3.4.2 NDS Tree Structure

We said that NDS uses a hierarchical tree structure to organize the various objects. Hence the structure is referred to as the NDS `tree`. The tree is made up of these three types of objects:

- The [Root] object
- Container objects
- Leaf objects

The location in which objects are placed in a tree is called the *context* or *name context* (similar to a pointer in a database). The context is of key importance. To access a resource, the User object must be in the same context as the Resource object. A user object has access to all objects that lie in the same directory and in child directories.

The [Root] object is the top of a given Directory tree. Branches are made up of container objects, within them are leaf objects. The [Root] object is created automatically when NDS is installed. It cannot be renamed or related. There can be only one [Root] object in a given NDS tree.

Container objects provide a way to logically organize other objects in the NDS tree. A Container object can house other Containers objects within it. The top Container is called the *Parent Object*. Objects contained is a container object are *Child Objects.*

There are three types of parents, or containers:

- Organization (O=)
- Organizational Unit (OU=)
- Country (C=)

There must be at least one *Organization object* within the NDS tree, and it must be placed one level below [Root]. The organization object is usually used to denote a company or main organization.

Organizational Units are optional. If they are used, they must be placed one level below an Organization level or below another Organizational unit. They can be used to denote divisions or departments within a company.

Organizational Units can be defined within Organizational Units to configure a deeper organizational structure. At a higher level, an Organizational Unit may represent a division of a company. Organizational Units contained in the divisional Organizational unit may represent departments within a division. An example is given in Figure 12.

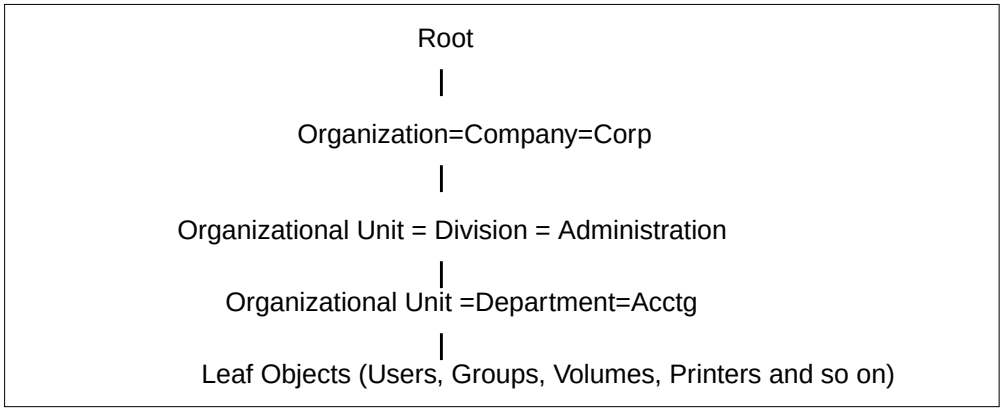


Figure 12. A Typical Company Tree

Because NDS is based on the CCITT X.500 specification, the use of *Country* container objects (C=) is also supported. Country containers are located below

[Root] and above Organization Container Objects. Country containers are useful for a multinational company.

Leaf objects are a single entity objects. They do not contain other objects. They correspond to actual physical entities such as users, groups, servers, and printers. A leaf object is denoted by CN= (Common Name).

Objects are either user-related or resource-related. Objects are all intended to provide users (user-related objects) with access to resources (resource-related objects). One Leaf Object is put in a container to provide access to another leaf object. Container objects are provided for the purpose of organizing Leaf objects.

Associated with each object is a set of *object rights.* Depending on the object rights assignment, a user may or may not have access to certain parts of the tree. Specifically, the user may or may not have access to network (resources such as printers in those parts of the tree. Object rights are NDS-based rights. When users are given access to a Volume object, they still must be granted file system trustee assignments, which are separate from NDS rights.

3.4.3 Users and Groups

We said previously that users and groups are objects in the NDS structure. Creating a user consists in selecting a container in which to create the user. User objects receive all the NDS rights and trustee assignments of the container in which they are created. Groups can be created to simplify user access to applications and data.

Users and groups are called *trustees* when they possess NetWare properties or values. Access rights can be assigned to users or to groups; when they are assigned, there are called *trustee* assignments. These assignments are called *direct* assignments if they are assigned directly to users or groups.

When a user is assigned to a group, the user receives indirectly the trustee assignments that were assigned to the group.

3.5 RACF

To visualize how RACF works, picture RACF as a layer in the operating system that verifies user's identities and grants user requests to access resources.

Assume, for example, that you have been identified and verified to the RACF protected system and now want to modify an existing RACF protected resource. After you enter a command to the system to access the resource, a system resource manager (such as data management) processes the request. The resource manager, based on what RACF indicates, either grants or denies the request.

Figure 13 on page 58 shows how RACF interacts with the operating system to allow access to a protected resource. The operating system interacts with RACF in a similar manner to identify and verify users.

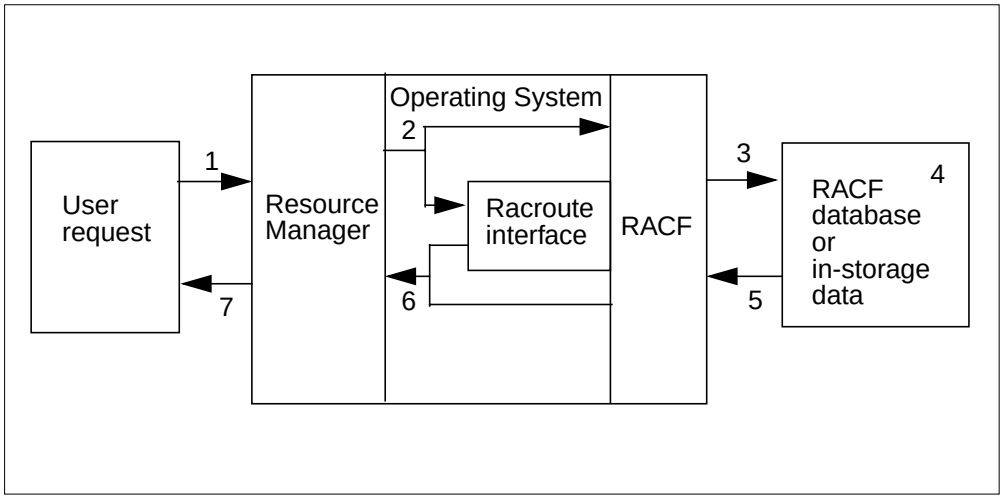


Figure 13. RACF's Relationship to the Operating System

1. A user requests access to a resource using a resource manager (for example, TSO/E).
2. The resource manager issues a RACF request to see if the user can access the resource.
3. RACF refers to the RACF database or in-storage data
4. It checks the appropriate resource profile.
5. Based on the information in the profile,
6. RACF passes the status of the request to the resource manager.
7. The resource manager grants (or denies) the request.

During authorization checking, RACF checks the resource profile to ensure that the resource can be accessed in the way requested and that you have the proper authorization to access the resource. The necessary user-resource requirements must match before RACF grants the access request to a protected resource.

Figure 14 on page 59 illustrates a conceptual model of how RACF checks profiles to ensure who (in a user profile) is accessing what and how (in a resource profile).

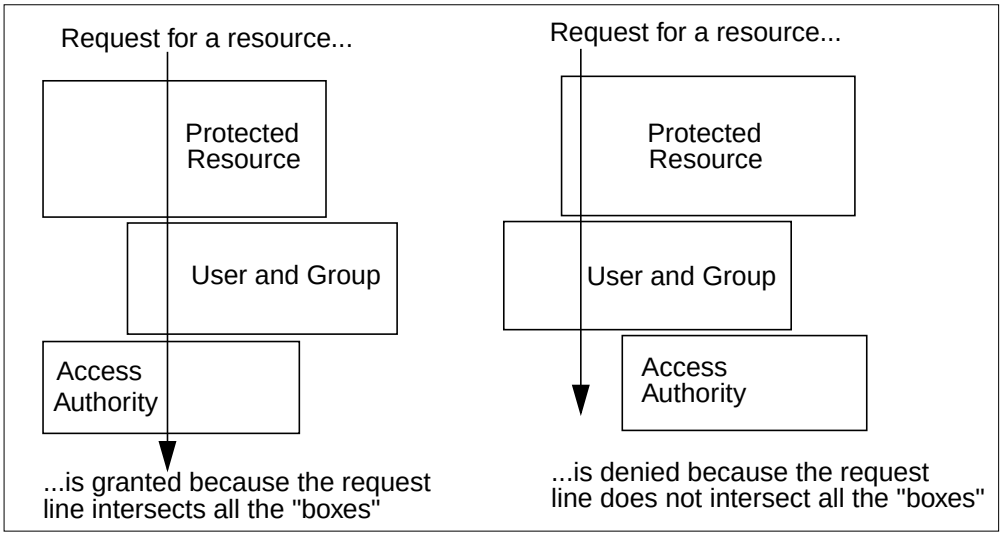


Figure 14. Conceptual Illustration of RACF Profile Checking

The "boxes" refer to the installation-assigned attributes and authorities for user and resources that determine which users can access which resources in what manner.

3.5.1 System Authorization Facility

The System Authorization Facility (SAF) is a part of the MVS operating system that conditionally directs control to RACF, if RACF is present, or to a user-supplied processing routine, or both, when receiving a request from a resource manager. SAF does not require any other product as a prerequesite, but overall system security functions are greatly enhanced and complemented if it is used concurrently with RACF. The key element in SAF is the SAF router. The SAF router is always present, even when RACF is not present.

The SAF router is a system service that provides a common focal point for all products providing resource control. This focal point encourages the use of common control functions shared across products and across systems. The resource-managing components and subsystems call the MVS router as part of certain decision-making functions in their processing, such as access-control checking and authorization-related checking. These functions are called control points.

3.5.2 The RACF Database

Information about all your users, groups, data sets, and other resources is kept in the RACF database. The records in the database that describe all these objects are called *profiles*. Hence we are talking about user profiles, data set profiles and so forth. A resource profile that is used to protect a single resource (a data set (file), a transaction, a cryptographic key, and so on) is called a *discrete profile,* and a profile that protects multiple resources is called a *generic profile*. User profiles and group profiles mostly have a relationship to one another in that every user is a member of at least one group. When a user belongs to a group, we say that the user is *connected* to the group**.**

Profiles that describe RACF protected resources also have an *access list* that tells which user IDs and what groups have the right to access the resource(s). This is to say that access to a resource is based on who you are or which group(s) you are connected to. Not only does the access list tell who is allowed to access the resource(s) but also at what access level (right) they are allowed to access.

There is a thing or two to remember from what has been said so far about RACF profiles. A RACF user profile is a description of one user as opposed to the user profiles described later in Chapter 4, “What Is TME 10 User Administration?” on page 65. There is also a difference in the way RACF groups are used within RACF and the way TME 10 terms and uses groups.

3.5.3 RACF User and Group Management Concepts

User administration in the OS/390 Security Server, as in most other systems for controlling user access to resources, should be based on a security policy. The policy sets out the principles of what resources should be protected, who is responsible for resources, and what the organization that takes care of security looks like. Based on this policy, you should build a structure that can fulfill the requirements set out in the policy. When building this kind of a structure, you should try to make it transparent for the users who do not try to bend the rules and at the same time design the administration to be as easy as possible.

The basic principle in user administration is to allow the users to access only the resources they need to carry out their job. You should also base access rights on a person's responsibilities or job role rather than on the individual's user ID. By sticking to these simple rules, you are making sure that you are not building a structure that will need constant administrative attention, but will only require attention when you introduce new resources or when people change job roles.

The OS/390 Security Server (RACF) allows you to meet the above objectives by building a RACF group structure that reflects the many job roles and responsibilities that your company has. The important thing is to start your security implementation by mapping job roles and responsibilities into RACF groups and then to connect your users to the groups that correspond to the job they are doing. Having done this, you will then have to look at your resources in order to decide what job roles or responsibilities should have access to the them.

Experience shows that if you spend time building a good group structure before you start protecting resources, you will not only have a well-designed security, you will also have a much easier administration. Failing to build a structure mostly implies that you will do ad hoc administration based on individual access rights. This kind of administration will increase as you protect more and more resources. Quite soon, you will also find out that individuals not only have access to those resources they need to do their job but also to all those resources that reflect previous jobs and responsibilities. Needless to say, the administration will increase as time goes by, and the audit of this kind of an environment will be hard indeed.

User administration also includes decisions about what applications users are going to have access to. Some of these access rights can be handled through group connections, but others have to be handled by defining user attributes or defining additional segments to the basic user profile. Basically, you will have to

give users different roles to play and to define for every role what applications and resources are necessary. RACF in itself does not allow you to define roles, but you can build user definitions that can serve as a model when adding new users to a given role.

Later on there will be a discussion about the TME 10 Security Management product and the facilities to define roles using this product. You will also find that for some time to come the definition of roles and the capabilities to handle all the RACF profile classes will not be possible with the TME Security Management product. However, there will never be a product that can create order out of chaos, and a good RACF structure will be equally necessary after the coming of the TME 10 Security Management product as it is today.

3.5.4 User Attributes

Looking at the users in a given system, there are the normal users, there are managers and there are administrators. In RACF there are a number of attributes that can give users special rights with respect to resources and with respect to what users are allowed to do with the RACF database. The four most interesting user attributes are:

- SPECIAL
- OPERATIONS
- AUDITOR
- REVOKE

SPECIAL as a user attribute means the user is a RACF administrator and has the right to do all the RACF commands and to define every kind of profile in the RACF database. Quite often this attribute is thought of as having the right to access all the resources on a system (equivalent to the UNIX user root) but this is not the case. The administrator could give himself the rights to access all resources, but that would then show up in the audit trail. So SPECIAL really means you have the right to manage the contents of the RACF database but with respect to the other OS/390 resources you are just another user.

OPERATIONS as a user attribute means the user can access all the datasets and a few additional resource classes in the system. The OPERATIONS user can also allocate datasets for any other user in the system. Given these kinds of rights you can easily understand that these rights should not been given lightly - as a matter of fact there should only be temporary user IDs which have this attribute and that could be opened in emergency situations. Given that you know which the OPERATIONS users are you can still stop them from accessing resources by excluding them using the access list. All it takes is knowing the user IDs of those that have the OPERATIONS attribute.

AUDITOR as a user attribute designates a user who is responsible for auditing the RACF database as well as the system itself (the access logs and system integrity). The AUDITOR attribute gives a user the right to look at all the profiles in the RACF database and also to change the audit attributes for the system and individual profiles. The auditor would also have to analyze the audit logs to follow up on violations as well as the utilization of certain protected resources.

Both the SPECIAL, OPERATIONS and AUDITOR attributes can also be given to a user as an attribute applied to one or more of the user's connect groups. This is

called GROUP-SPECIAL, GROUP-OPERATIONS and so on, and means you can only use the attribute as far as the scope-of-group extends. Scope-of-group includes all the resources that are owned by the group in which you have one of the special attributes or any resource owned by a subgroup owned by the group and so on.

GROUP-SPECIAL is normally used to enable distributed administration where a department or branch office is taking care of their own RACF administration. Distributed administration requires a well-built RACF structure in order for it to work.

The REVOKE attribute is a way of stopping a RACF defined user from using the system. REVOKE can either be caused by guessing one's password too many times, from not logging on to the system for a predetermined number of days or by an administrator revoking a user's profile.

3.5.5 RACF Segments

Segments for RACF profiles are optional extensions to the base profile where you store information that applies to a given application or a management function. Let’s take the user profile as an example. If you should be able to run Time Sharing Option (TSO), you need a TSO segment. To run Customer Information Control System (CICS), you need a CICS segment and so forth. Each of these segments contain information necessary for the particular application for which the segment is intended. Depending on your job role, you may need none or several segments added to your basic RACF profile.

3.5.6 Managing RACF Groups

RACF groups can be used to serve different purposes and the three most common uses are:

- Resource protection groups
- Administrative groups
- Functional groups

Resource protection groups are necessary when it comes to protecting data sets. There are two kinds of data sets: user data sets and group data sets. User data sets are the ones where the first-level qualifier is a user ID; all other data sets are basically group data sets. Before you can protect a group data set, the first level qualifier has to be defined as a RACF group. Before you can protect a data set like CICS41.LOADLIB, you would have to define a group with the name of CICS41. Only then can you define RACF data set profiles starting with CICS41 for your protection.

Administrative groups can be used for information purposes. One common way of using such groups is to build a structure that emulates your company organization with departments, divisions etc. and then to connect the users belonging to a department to the corresponding group. When you need to know who works at a given department, you can find it out by listing the group which represents that department. This kind of information comes handy when you want to know whom to inform about a security violation or just need to know where a given user works.

Neither resource groups nor administrative groups should be used to give users access rights.

Functional groups are the groups that represent job roles or responsibilities and are what you use to give users their access rights. Let's asssume there is an accountant job role and you create the RACF group ACCOUNT to represent this job role. The next step is to connect all the accountants to this group, assuming they have the same access needs in the system. That being done, you would then enter the ACCOUNT group onto all the access lists for thise resources to which accountants need access. Keep in mind that even if there is only a single person who has a given job role, you should still create a functional group for it. The idea behind the whole thing is that people tend to move, to quit and to die, but the job is still there and has to be done by someone. By simply connecting whoever has a specific task to do to the corresponding functional group, or removing those who are changing jobs, you will also have granted granted or removed access to the resources necessary to perform the job. Had you instead chosen to give the individual user ID those access rights, you would then have had to revise all access lists twice-- first removing the previous user ID and then adding the user ID of the successor.

The proper use of RACF groups and the management of those groups is a task that is key to the successful implementation of RACF based access control.

3.5.7 Role Based Security

As mentioned earlier, RACF does not support role-based security as such. What you can do is to build a structure of groups where the functional groups can be used to represent a given job role. A functional group is entered onto each resource access list that is necessary for someone in a particular job role. Each user is then connected to those functional groups that represent all the job roles and functions he/she is to perform. In other words one or more functional groups can be used to represent a role, but RACF in itself does not recognize roles nor does it treat one group differently from another. Therefore, it is up the the RACF administrator to build a structure that lends itself to defining the roles. RACF as a tool will allow for any structure that makes sense to you.

Whatever you do, you should never plan on allowing access based on individual user IDs. It is all too esay to say "just this once" but after a while, you will have created a structure that needs more and more revision every time a user changes jobs or moves to another department.

Chapter 4. What Is TME 10 User Administration?

Before implementing TME 10 User Administration, it is very important to understand the overall architecture and design of TME 10 User Administration, such as the platforms supported, the main functions of the product and the mechanisms used by the product in order to perform user administration tasks.

TME 10 User Administration is one of the applications that can be installed on top of the Tivoli Management Framework (TMF). It is a new release of the Tivoli/Admin application. It extends the capabilities of the Tivoli Management Environment (TME) and allows you to manage user accounts on the UNIX, Windows NT, NetWare, and OS/390 platforms from a single location. It also manages group accounts on UNIX and group memberships on Windows NT and NetWare.

In conjuction with the Tivoli Management Framework, TME 10 User Administration provides your distributed environment with the following features:

- Centralized and GUI-based control of user administration tasks
- Single-action user management including:
  - Creation, deletion, modification of user accounts
  - Synchronization of systems files with user profiles
  - Common login and password for all platforms
- Secure delegation of administrative tasks to other administrators
- Consistent administrative policy definition for user accounts
- Automation for repetitive administration tasks
- Parallel operations performed on many users and systems
- Configuration error reduction via profile-based administration methodology

Figure 15 shows the TME 10 User Administration product amid all the current TME 10 software components. This picture shows that TME 10 User Administration uses the TME 10 Framework as infrastructure.

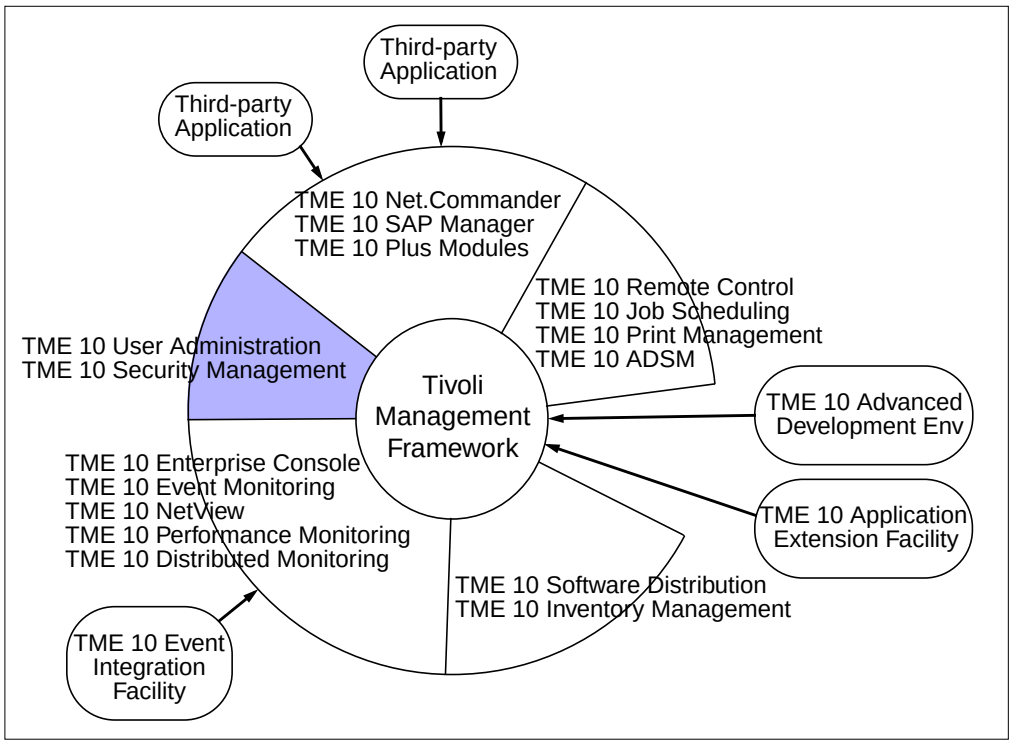


Figure 15. TME 10 Software Components

4.1 Supported Platforms

The TME 10 User Administration product supports user administration functions on the following managed nodes:

- AIX
- HP-UX
- SunOS
- Solaris
- Windows NT
- OS/390-RACF

In addition, the following platforms are supported as PC managed nodes:

- NetWare
- Windows NT

4.2 Product Information

The TME 10 Framework product (5697-FRA) is a prerequisite to the TME 10 User Administration product.

The TME 10 User Administration product (5697-UAD) consists of the following components:

- TME 10 User Administration
- TME 10 User Administration Filepack Utilities

The TME 10 User Administration product is required to manage user accounts on UNIX and Windows NT managed nodes. The TME 10 User Administration Filepack Utilities are required to managed user accounts on Windows NT and NetWare PC managed nodes.

In order to manage RACF accounts on an OS/390 system, additional products are required on the TMR server:

- TME 10 GEM OS/390 Connection Service
- TME 10 GEM User Administration Service

The TME 10 GEM OS/390 Connection Service allows an OS/390 Connection to be defined, which is a managed resource for TME 10 User Administration. The TME 10 GEM User Administration Service upgrades TME 10 User Administration to include new categories, subcategories and attributes that allow management of several segments of the RACF user profile.

On the OS/390 platform itself, the TME 10 Global Enterprise Manager (5697-B83) product is required and must be installed on the OS/390 platform. The OS/390 system must be running the OS/390 Security Server, which is the currently supported OS/390 security product for the implementation of TME 10 User Administration. For requisite software requirements on the OS/390 platform, refer to Section 5.4.3, “Installing TME 10 GEM User Administration for OS/390” on page 117, or refer to the appropriate TME 10 User Administration Release Notes Version 3.1.

4.3 Concepts and Architecture at a Glance

TME 10 User Administration is a profile-based application that runs on your TMR server. As a profile-based application, TME 10 User Administration works according to the *management by subscription* model. In this model, profiles contained in a profile manager define specific aspects of system configuration, such as user account or group information. A profile record (or entry) represents the actual configuration information about one user or group. In order to be eligible to receive this configuration information, managed nodes, PC managed nodes and OS/390 connections *subscribe* to the profile managers. Once data is stored in the profile or modified, you can *distribute* it to subscribers, thus updating their system information.

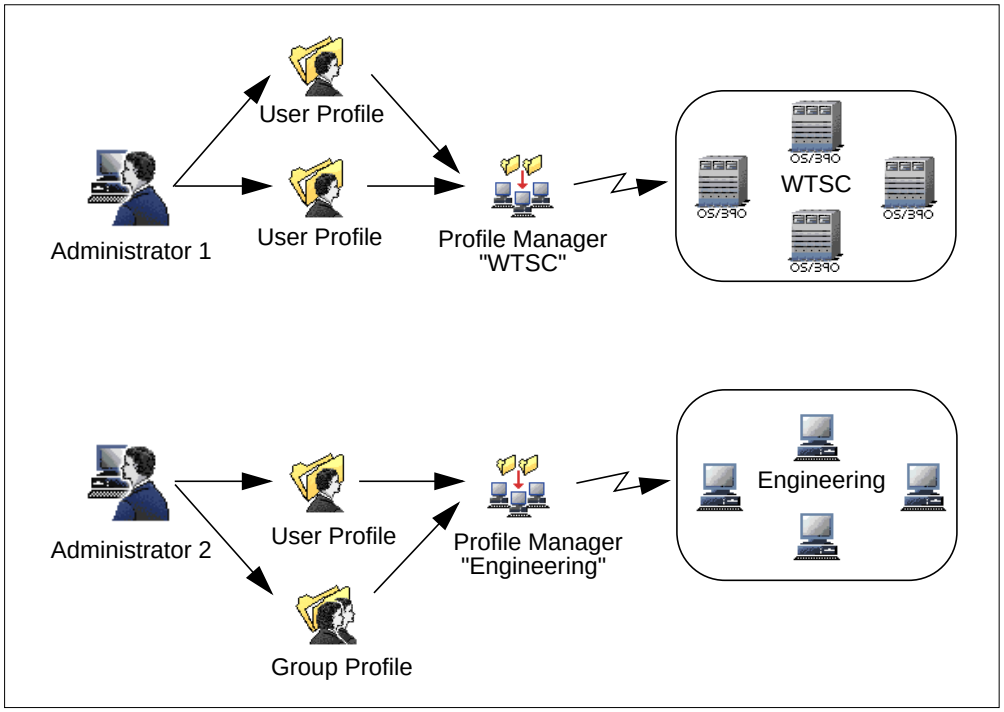


Figure 16. Relationship between Profiles, Profile Managers, and Managed Nodes

Figure 16 shows the relationship between profiles, profile managers, and managed nodes for user and group information as provided by TME 10 User Administration.

It is important to understand that TME provides an environment to administer a number of heterogeneous platforms and that the TME 10 framework must cater for functions unique to each platform. This results in TME User Administration having objects that are unique to a specific platform. For example, in Figure 16 Group profiles only are applicable to UNIX platforms; *these group profiles do not relate to RACF groups in the OS/390 platform*. User profiles, profile managers and managed nodes are applicable to all platforms.

Profile entries can either be manually added one at a time, or they can be initially imported (*populated*) from one or more managed, PC managed nodes or NIS domains. The profiles are stored in the TME database of the TMR server.

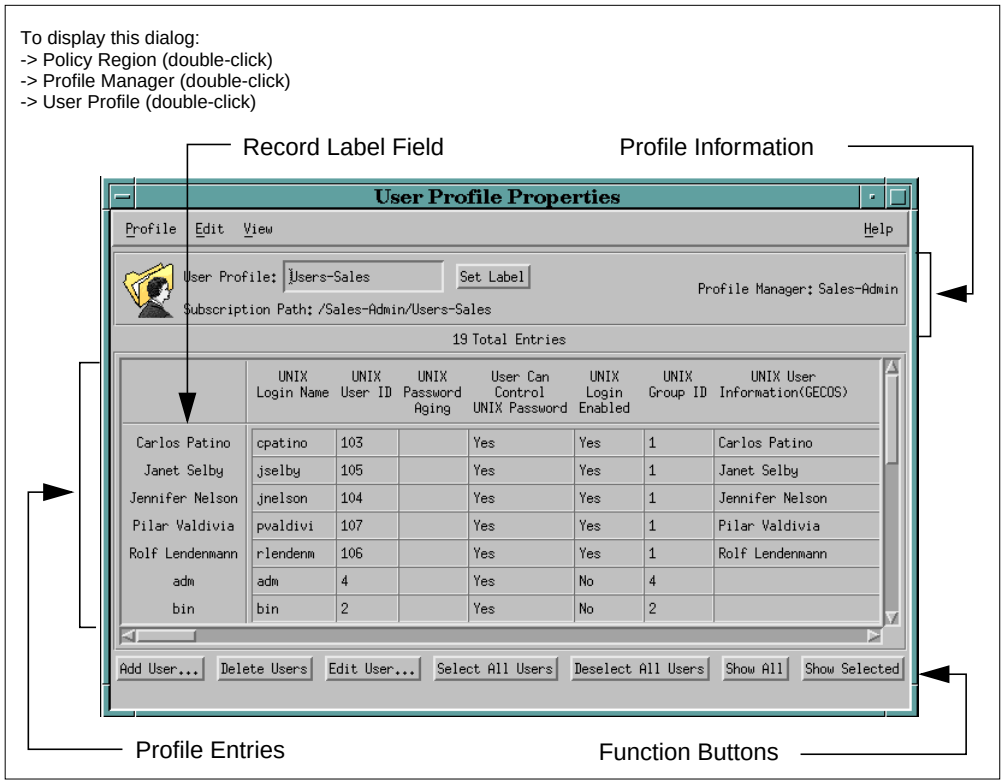


Figure 17. User Profile Properties Table

Figure 17 shows an example of a *User Profile Properties* window that already contains several records.

The Profile Information area displays information such as the profile's name, the profile manager that contains the profile, and the profile's icon. In this example, the User Profile displays all users of the Sales department. In particular the figure shows the UNIX attributes for the users. Each of the profile entries represents the information about a specific user and will create or maintain a single line in the corresponding system configuration file, the /etc/passwd file, of each workstation.

Any attribute contained in the profile can be designated as the record label. In this example, the *UNIX User Information (GECOS)* attribute was selected as a record label. Finally, the function buttons allow you to perform specific operations such as adding, deleting, or editing an entry as well as selecting or deselecting a set of entries.

In order to update system configuration files on the managed target machines, the profiles must be distributed to them. To be able to distribute profiles, an association has to be made between profiles and target machines (subscribers). This is done by using the profile manager's subscription list. Profile managers contain profiles and reside within an associated policy region in the TME desktop.

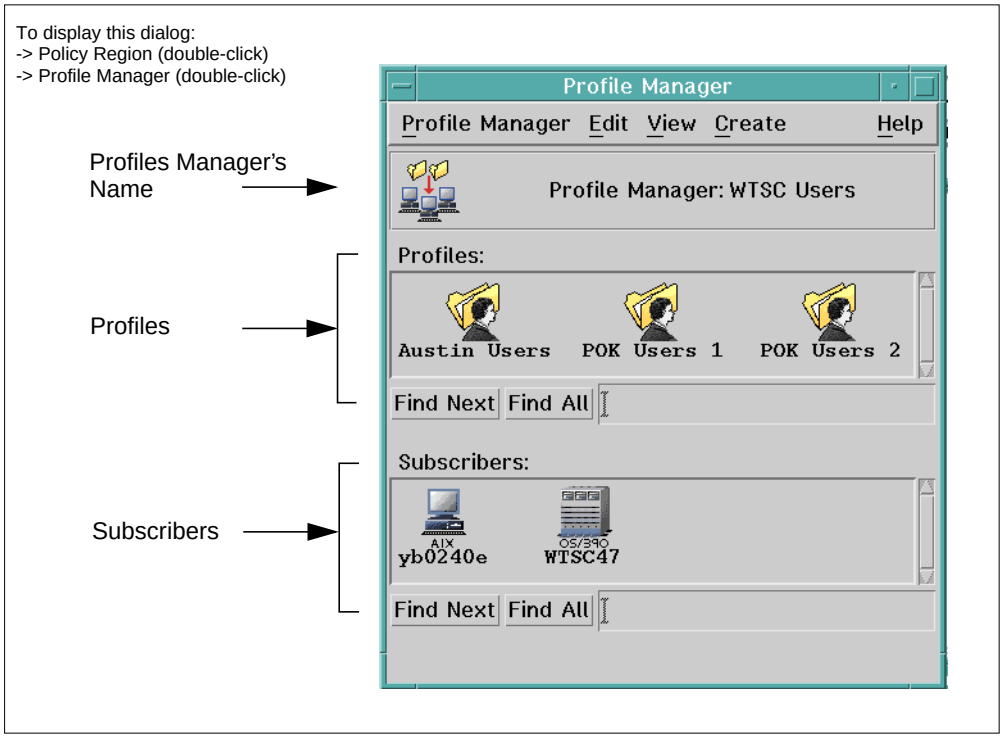


Figure 18. Profile Manager Window with Profiles and Subscribers

Figure 18 shows an example of a *Profile Manager* window. It is the WTSC Users profile manager, which contains all user and group profiles for the World-wide Technical Support Center as well as a list of subscribers. The Subscribers area displays the endpoints (managed nodes, PC managed nodes, NIS domains, or OS/390 Connections) or other profile managers to which the profiles may be distributed. When a distribution is initiated, the administrator can specify whether the profile(s) go to all subscribers or to particular subscribers only. In our example the profile manager has the following subscribers:

- yb0240e (AIX managed node)
- WTSC47 (OS/390 Connection)

Figure 19 summarizes the actions involved in defining and distributing system files using TME 10 User Administration. Remember that the following actions are performed within a *Profile Manager* window.

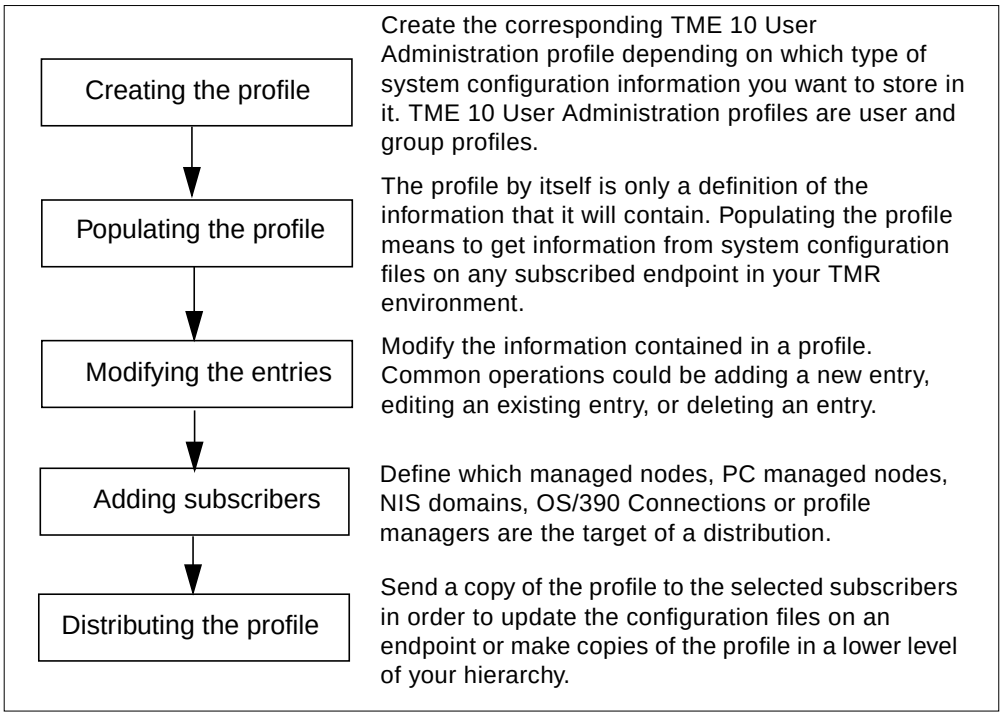


Figure 19. Tasks Involved in Customizing and Using TME 10 User Administration

4.3.1 Managed Resources

Like other TME applications, TME 10 User Administration is based on managed resources. A managed resource in this context is a set of centrally managed definitions or parameters to be enforced in a set of target machines. The managed resources added or extended by installing TME 10 User Administration are:

User Profile – Provides profile-based management of user account information. In a user profile each record is stored in a platform-independent format and contains information related to UNIX, Windows NT, NetWare and OS/390 RACF accounts, as well as the common login and common password for all the platforms. Example attributes that are stored include user name, user ID, password, home directory, and login shell. The profile resides in a profile manager and needs to be distributed to its subscribers to enforce the user account information on the managed nodes.

Group Profile – This resource is only supported for UNIX managed nodes. A group profile is a collection of UNIX group-specific information such as valid groups, group IDs, and membership list. This information is typically located in the /etc/group file. The profile resides in a profile manager and needs to be distributed to its subscribers to enforce the group information on the managed nodes

UNIX Managed Nodes – The UNIX host-management facility extends the management capabilities over all UNIX managed nodes in the TMR by adding the following functions to the pop-up menus of the UNIX managed node icons:

- Viewing and editing the properties and network interface information
- Run an Xterm session from the managed node
- Toggling the appearance of the icon that represents a managed node
- Enabling or disabling Internet services
- Viewing or signaling processes running on a managed node
- Editing local mail aliases
- Viewing or editing the remote authentication database
- Distributing or updating system configuration files

NIS Domain – The NIS map management facility allows you to manage NIS domains as policy region resources. The NIS master server must be a managed node. The following operations over NIS domains are provided:

- Discovering existing NIS domains
- Adding, editing, or removing NIS maps and map data
- Syntax of a map source file

TME 10 User Administration does not create NIS domains; it only creates objects that represent the domains that exist on managed hosts.

NetWare PC Managed Nodes - This provides the definition of NetWare systems managed by TME. The following functions are available from the pop-up menus of the NetWare PC managed node icons:

- Viewing the properties of the NetWare managed node
- Editing some properties of the node
- Toggling the appearance of the icon that represents a managed node

Windows NT Managed Nodes - NT managed nodes are defined by this icon. The following functions are available from the pop-up menu:

- Display members of the managed node
- Viewing and editing the properties and network interface information
- Toggling the appearance of the icon that represents a managed node
- Distributing or updating system configuration files

OS/390 Connections - The OS/390 Connection Service allows the creation of an OS/390 Connection, which is an end-point for TME 10. The following operations on OS/390 Connections are available from the pop-up icon:

- View OS/390 Connection profile subscriptions
- Edit properties of OS/390 Connections
- Issue RACF commands on the OS/390 server represented by the OS/390 Connection

4.3.2 Profiles and Profile Managers

A profile is a collection of information related to a specific application that lets you manage a particular type of resource. A profile also contains a list of subscribers (members of the list) to which the profile can be distributed in order to update system configuration information.

Note: User profiles have a record-level subscription list, which, if used, is a subset of the profile manager subscription list.

There is a strong relationship between profiles, profile managers, policy regions, and endpoints. Here are some key points about this relationship:

- Profile managers are created within a policy region.
- Profile managers contain profiles and a list of subscribers.
- Subscribers can be managed nodes, PC managed nodes, NIS domains, S/390 connections or other profile managers.

  Having a profile manager as a subscriber allows the administrator to distribute a user profile to that profile manager. Then another administrator can edit and customize that user profile before distributing it to the target machines. This is a way to delegate responsibility to other administrators within a region.
- Profile manager hierarchies are created when profile managers have other profile managers in their subscriber lists.
- Profile manager hierarchies allow you to manage your resources from a top-down approach in your organization.

For more information about profile policy, profiles, and profile managers in general, see the *TME 10 Framework User's Guide*.

There are two types of profiles, user profiles and group profiles. TME 10 User Administration user profiles can manage UNIX, Windows NT, NetWare, and OS/390 RACF accounts, whereas group profiles can only manage UNIX group accounts. However, when adding a user to a profile on Windows NT or NetWare, it is possible to specify an existing group for this user.

When an NIS domain subscribes to profiles, its master server will get the system files on a distribution, provided that it is a managed node.

4.3.3 Profile Policies

Policies are rules that users and groups must comply with. For example, the administrator might want that all user passwords have a minimum of five characters. These policies allow the administrator to keep all the user and group definitions (attributes) consistent across all platforms within a region.

There are two types of policies: default policies and validation policies.

- **Default Policy**

  Each profile has a *default policy* associated with it. The default policy determines the default values used when creating a new entry in a profile (when for example creating a new user in a user profile). These default values help you minimize the amount of data that you have to enter when creating a new record in a profile. They work as a template for each new record you add to the profile. Default policy provides a value if you don't fill in the blanks. A

default policy garantees that all users have a set of consistent default values for their attributes.

Note: Populating a profile does not run the default policy. Default policy can be run afterward though.

- **Validation Policy**

  Every time you modify or create a profile entry, it is checked against a set of *validation policies* that ensure that the data you are entering complies with the current policy. Validation is performed in the same way when populating a profile. This prevents you from creating or getting an entry that does not meet your specifications. You can also request a validation for a specific profile at any time.

The policies can be edited from the GUI or from the command line interface. Each policy attribute can be set to a constant, to a script, to a regular expression, or to none.

Default and validation policies are stored in the profile and can be set for any attribute on any profile or profile copy. This allows different policies on the top-level profile and on profile copies (at the managed nodes levels).

Figure 20 shows the *Edit Validation Policies* dialog for a user profile. This dialog allows you to edit the validation policies for a user profile. The attributes list allows you to select the attribute for which you want to define a validation policy. The *Subscribers can edit* radio button determines whether or not a Tivoli administrator can change the validation policy for the selected attribute in their local copy of the profile.

The Default Type list determines the validation type used to validate the attribute. Selected is Script, which requires you to provide shell script arguments (*Edit Script Arguments***...** button) and a shell script body (*Edit Script Body***...** button). Other values for the default type are: None, Constant, and Regular Expression.

In the same way as shown in Figure 20 for validation policies, administrators can edit default policies that implement rules for generating default values.

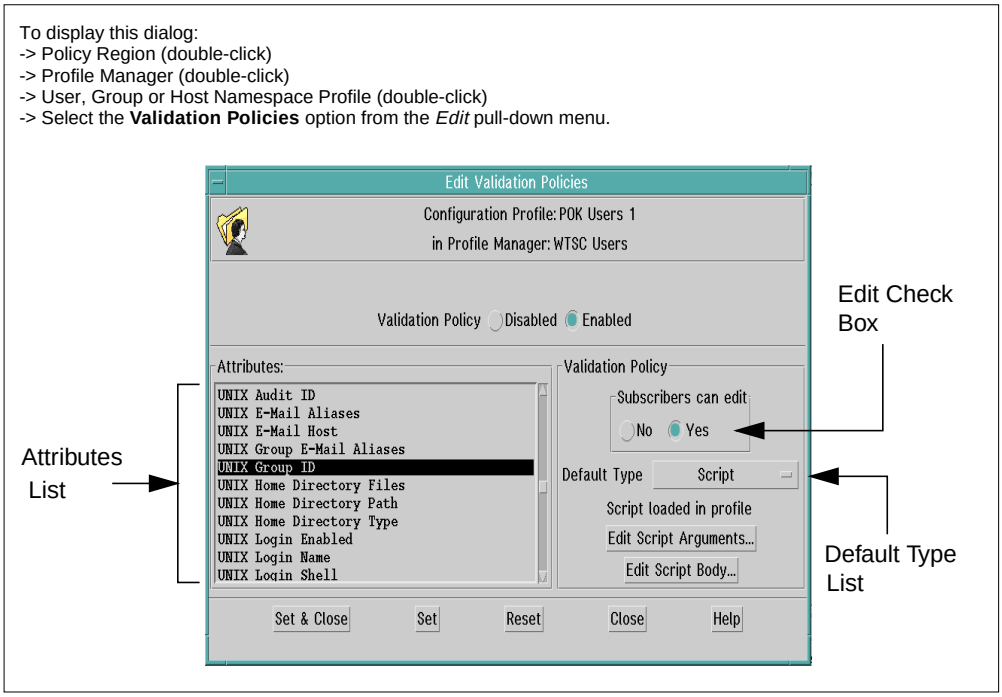


Figure 20. Edit Validation Policies Dialog

TME 10 User Administration as supplied by Tivoli includes default and validation policies for the following areas:

- General user information
- Windows NT user accounts
- NetWare user accounts
- UNIX user accounts
- UNIX groups accounts

For more information about user and group profile policies, refer to Appendix E in the *TME 10 User Administration User and Group Management Guide*.

4.3.4 Profile Population

Populating a user or group profile consists of gathering all user and group information from the system files on the managed nodes and PC managed node and adding that information as records to the profile.

TME 10 User Administration user and group profiles can be populated from any managed node, PC managed node (Windows NT or NetWare), or OS/390 Connection. Possible subscribers can be:

- Other profile managers
- Managed nodes
- NIS domains
- PC managed nodes (Windows NT, NetWare NDS trees, NetWare 3.X servers)
- OS/390 Connections

User and group profiles are managed resources, and each policy region maintains a list of managed resource types that are valid for that specific policy

region. In order for an administrator to create or manage a profile, the following must be true:

- The profile manager must be a managed resource of the policy region.
- The particular profile type, such as user or group, must be a managed resource of the policy region.
- The administrator must have the senior role to create profile managers.
- The administrator must have an administrator role to maintain the profiles in the policy region.

When populating a profile, the validation policy for that profile applies. This means that, for example, UIDs less or equal to 0 will fail the validation. In UNIX, users *root* and *nobody* will not pass the validation policy.

4.3.5 Profile Distribution

Once a profile is populated, by either a populate or by adding records, it can be distributed to the subscribers. The subscribers available to receive profiles are determined by the profile manager and can consist of the following resource types:

- NIS Domain
- Managed Node (UNIX or Windows NT)
- PC Managed Node (Windows NT or NetWare)
- Profile Manager

When distributing a profile, there are four options: Next Level, All Levels, Preserve local modifications, and Exact copy. It is extremely important to understand the differences between these options. These options are covered in great detail in Section 6.1, “General Operations” on page 135.

4.3.6 Profile Synchronization

If the system files and databases of a profile endpoint are changed directly without using TME, the profiles that the endpoint subscribes to may no longer accurately reflect the endpoint’s current configuration. That is, the users and groups defined in TME 10 profiles may not reflect the true definitions of the users and groups on the managed systems.

The synchronization function is available to reconcile any differences between the TME 10 profile databases and the current profile endpoint configuration (except for passwords).

When synchronizing profiles, TME 10 will first present a dialog titled Profile/System Discrepancies outlining the differences found. The following differences may be found:

Delete Record	Profile items that exist in the profile, but not in the endpoint’s system files
Add Record	Items that exist in the endpoint system files, but not in the profile
Change Record	Items that differ in the endpoint’s system files and in the profile

From the Profile/System Discrepancies dialog, you are able to commit or cancel the changes. If you commit the changes, the profile and the endpoint's system files will be synchronized. Synchronization is based on the endpoint's configuration files; that is, the profile is modified to reflect the current endpoint's configuration files. Modifications to existing records are merged on an attribute by attribute basis. The top level profile is not updated.

Note: Synchronization is not available for the OS/390 RACF environment.

4.3.7 The User Locator

The *User Locator* is a tool that allows you to locate any user in your TME. After you install the TME 10 User Administration product, this tool appears on the TME desktop. By double-clicking on the User Locator Icon, you can display the *User Locator* dialog, which lists all the users in the TME in alphabetical order.

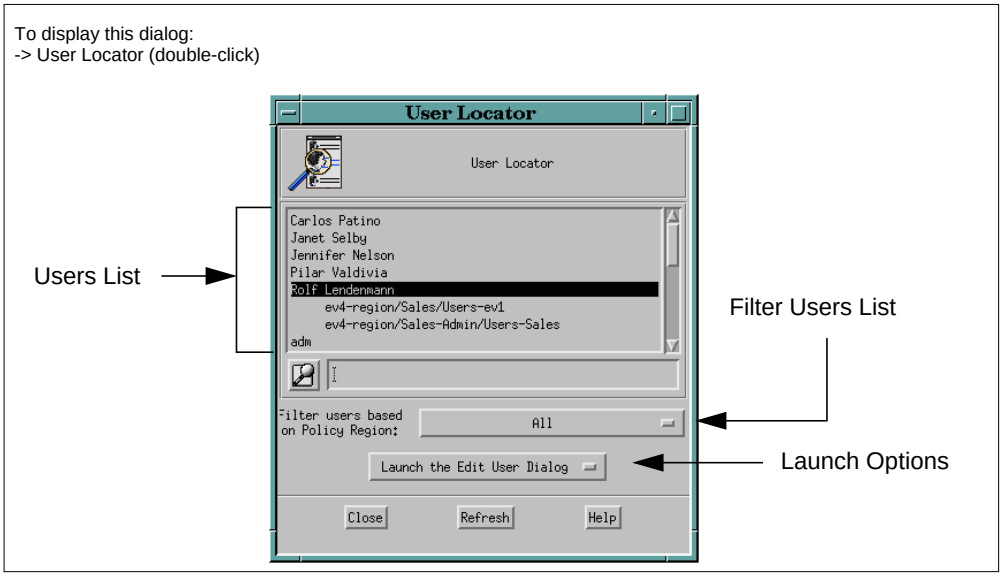


Figure 21. User Locator Dialog

The Users List panel lists all users in your TME. Each user in the *User Locator* dialog has an expandable view that lists all the profiles to which the user belongs. The nomenclature used to display the information is the following:

```
PolicyRegion/ProfileManager/Profile
```

The search of users can be limited (filtered) to a policy region, or you can search across the TME. Every time you change the search filter, the list of users in the Users List area is updated. The Launch Options feature allows you to determine which dialog(s) are displayed when you locate a user. Available options are:

- Display the *User Properties* dialog
- Display the *User Profile Properties* dialog
- Display both

4.4 TME 10 User Administration vs. TME 10 Security Management

TME 10 User Administration focuses on centralized administration of users and their system and application-specific representations in the form of accounts and user IDs. This includes user-centric security aspects such as password and login policy.

The focus of TME 10 Security Management is on centralized administration of secure access to the system and to applications by one of more accessors, where an accessor can be either individual users or groups of users. TME 10 Security Management manages the following:

Groups Collections of users
Roles The capabilities needed for a given job function
Resources The resources to which roles provide specific access rights

Note the concept of a group profile (refer to “Concepts and Architecture at a Glance” on page 67 and “Managed Resources” on page 71) is significantly enhanced between TME 10 User Administration and TME 10 Security Management.

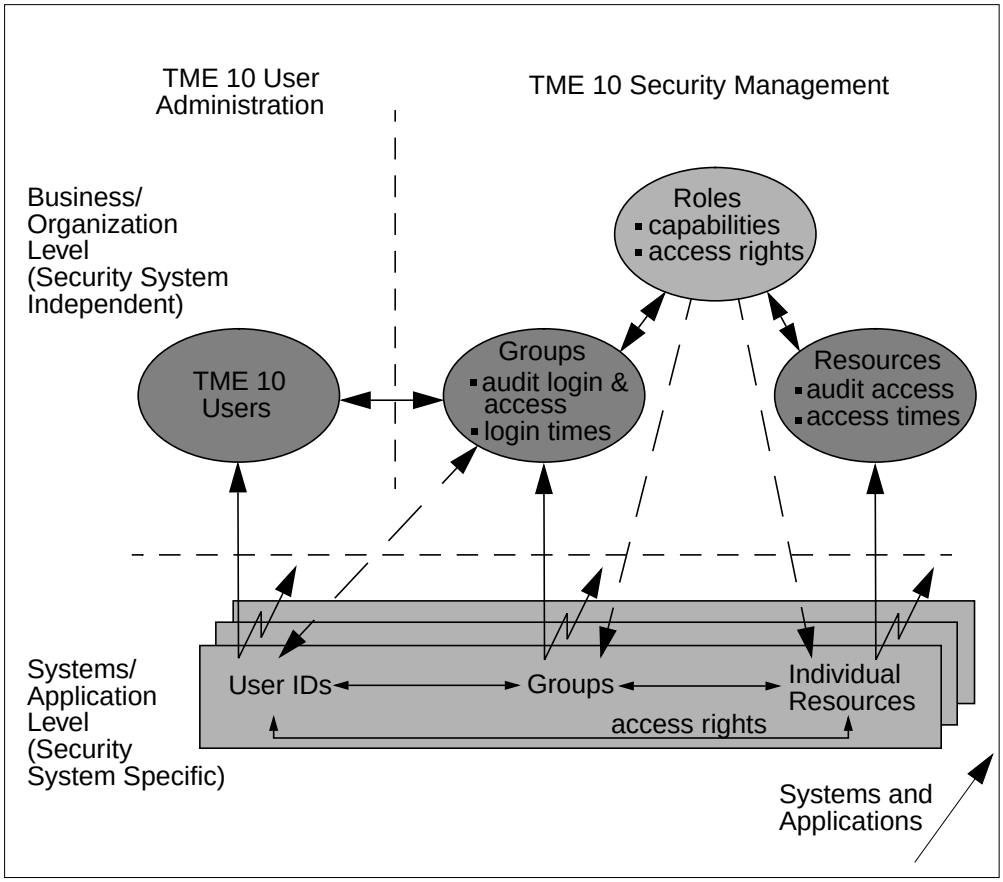


Figure 22. Relationship of TME 10 User Administration and TME 10 Security Management

TME 10 User Administration and TME 10 Security Management are not prerequisite products, rather they are complementary products. Figure 22 shows the relationship between the two products in the context of role-based access

administration. TME 10 Security Management cannot create user IDs. The dashed line in Figure 22 from the Groups balloon to the User IDs label is indicative of TME 10 Security Management being able to manipulate user IDs and groups. TME 10 Security Management is able to interface with TME 10 User Administration to automate user ID creation.

TME 10 Security Management also provides an enhanced level of administration for default enterprise security policies. TME 10 User Administration provides for user-specific security policies. TME 10 Security Management extends this to systemwide security policies.

In conjunction with TME 10 Enterprise Console and TME 10 Distributed Monitoring, TME 10 Security Management is able to provide security event auditing and security alarming.

Chapter 5. Planning and Installing TME 10 User Administration

This chapter describes the main steps required for setting up a TME 10 environment including TME 10 User Administration. As an example, a specific technical environment is also described in this document. This environment can be used as an example for setting up your own environment.

5.1 Planning

It is strongly suggested that any TME installation be carefully planned. The most critical factors to be considered when planning your installation are:

- The organization of the company.
- The type of machines in which the products will be installed (TME 10 Server, TME 10 Management Stations, Managed Nodes and PC Managed Nodes)
- The hardware and operating system configuration of these machines (disk space availability, memory, operating system type and modification level)
- Required systems resources (paging space)
- Software prerequisites (operating system fixes, TME patches and so on)
- Network topology and communications devices

TME 10 has a minimum set of hardware, operating systems and systems resource requirements. These requirements vary, depending on whether the system will be used as a TME 10 Server, TME 10 Management Station, TME 10 Managed Node or TME 10 PC Managed Node.

Before starting any TME 10 implementation, we strongly recommend that you read and understand the following document:

*TME 10 Framework Planning and Installation Guid*e

This document provides a comprehensive description of the TME 10 Framework and guidance in planning your TME 10 installation.

5.1.1 Planning Your Framework Installation

5.1.1.1 TME 10 Server

The machine used as a TME 10 server is the most critical part of your TME 10 installation. It should be a high-performance machine, very stable and with a few non-TME 10 applications running on it. The better choice is a dedicated machine. The following table describes some acceptable configurations for your TME 10 server.

Table 6. Typical Configurations for a TME 10 Server

System	RAM	Swap Space
Data General AViiON Series 530	64 MB	128 MB
HP 9000/735	64 MB	128 MB
IBM RS/6000	64 MB	128 MB
Intel 486 or Pentium running Windows NT 3.51	48 MB	128 MB
Intel 486 or Pentium running UnixWare 2.0	48 MB	96 MB
Motorola 88000 Series	64 MB	128 MB

System	RAM	Swap Space
NCR 3400/3500 Series	64 MB	128 MB
SPARC 10 or SPARC 20 running SunOS4.1x	48 MB	96 MB
SPARC 10 or SPARC 20 running Solaris 2.3	64 MB	128 MB

The type of machine to choose as a TME 10 server depends on the complexity and the size of the environment to manage. If your Tivoli installation has only a small number of machines to control, an entry level machine is acceptable. If you plan to manage an environment of (for example) hundreds of machines, a higher level machine is required.

Remember that a single server can manage up to 200 clients. If your environment is larger, you have to set up and configure another TME 10 server and perform a connection between the two regions (every TME 10 server controls one region).

Tivoli recommends limiting the number of clients (Managed Nodes) to 200 . No limitation exists for PC Managed Nodes.

5.1.1.2 TME 10 Management Stations

A TME 10 management station is a TME client machine from which an administrator can perform operations by using the Tivoli desktop. This machine must be able to run Win32 based or Motif applications and must have good networking performance (to provide fast, reliable communication with the TME 10 server). Even for these machines, there are minimum architectural requirements. These are listed in the following table:

Table 7. Typical Configurations for TME 10 Management Stations

System	RAM	Swap Space
Data General AViiON Series 530	48 MB	96 MB
HP9000/735	48 MB	96 MB
IBM RS/6000	48 MB	96 MB
Intel 486 or Pentium running Windows NT 3.51	32 MB	64 MB
Intel 486 or Pentium running UnixWare 2.0	32 MB	64 MB
Motorola 88000 Series	48 MB	96 MB
NCR 3400/3500 Series	48 MB	96 MB
SPARC 10 or SPARC 20 running SunOS4.1x	48 MB	96 MB
SPARC 10 or SPARC 20 running Solaris 2.3	48 MB	96 MB

5.1.1.3 TME 10 Managed Nodes

The TME 10 client (UNIX or NT) should have enough disk space to support the installation of the TME 10 client part and a configuration of 32 MB of RAM and 64 MB of swap space. TME 10 does not impose a heavy load on the client machines. This load increases when TME 10 operations are performed on the client. It could be useful to schedule the most demanding TME 10 operations during hours in which the machine is not too busy. For example, you may want to schedule the distribution of a new user profile made up of 100 users on your Windows NT server to occur during the night when users are not logged on the

machine. To perform the installation of a TME 10 client, you have to be able to access the client machine as Windows NT Administrator or UNIX root**.**

5.1.1.4 PC Managed Nodes

The minimum requirements for a TME 10 PC Managed Node are listed in the following table:

Table 8. Configurations for TME 10 PC Managed Nodes

Supported Platforms	Minimum RAM Requirements
NetWare	8 MB
OS/2	8 MB
Windows (WFW, W3.x, W95)	2 MB
Windows NT	8 MB

5.1.1.5 Communications Considerations

The basic requirements for all the TME 10 operations is a bidirectional TCP/IP line. If you have a line slower than 14.4 KB (for example a WAN line between two remote sites), you'll not be able to remotely install TME 10 clients. In this case the installation can only be performed locally.

You also have to check if every client is able to perform the mapping between IP addresses and hostnames (reverse mapping). Before installing a client, this mapping must be working on the client as well as the server in order to establish the initial connection.

To determine if reverse mapping is available on a machine, you can execute the following command:

`nslookup nnn.nnn.nnn.nnn` on a UNIX or NT system

or

`ping -a nnn.nnn.nnn.nnn` on a Windows NT system only

where `nnn.nnn.nnn.nnn` is the IP address of the system you want to check to see if you can do the reverse mapping. If this command returns you the name of the host that corresponds to the IP address, then your Domain Name Service is configured for reverse mapping. If you don't get the host name, you can do the following:

- Add the IP address to host name maps to DNS.

or

- Use the LMHOSTS facility on Windows NT or add the hosts to the /etc/hosts file and use the /etc/hosts file as a DNS fall-back.

In a TME 10 environment, IPX/SPX communications are supported between a NetWare server defined as a PC Managed Node and NetWare clients (PC Endpoints). However, only TCP/IP is supported between a TME 10 server and a NetWare PC Managed Node. You then must ensure that TCP/IP is properly configured on your NetWare server.

5.1.2 Planning Your TME 10 User Administration Installation

After planning your TME 10 Framework installation, you have to plan the installation of the TME 10 User Administration product.

TME 10 User Administration is both a product install and an upgrade from Tivoli Admin 3.0 to TME 10 User Administration 3.1.

Note

This document covers TME 10 User Administration 3.1, it doesn't cover upgrades from Tivoli Admin 3.0 to TME 10 User Administration 3.1. You may find lots of useful information about the product enhancements in *TME 10 User Administration Release Notes Version 3.1*

TME 10 User Administration can be installed on the following platforms:

- **IBM RS/6000 systems running AIX**

  AIX V3.2.5 with PTF U435001, V4.1 or V4.2

  Motif 1.2

- **HP 9000 systems running HP-UX**

  HP 9000/700 series running HP-UX 9.01, HP-UX 9.03, or HP-UX 9.05 and Motif 1.2

  HP 9000/800 series running HP-UX 9.00 and Motif 1.2

  HP 9000/700 series with PA RISC 1.1 architecture running HP-UX 10.01 or HP-UX 10.10 and Motif 1.2

- **Intel 486 or Pentium systems running PC operating systems**

  Novell NetWare 3.12 as PC Managed Node

  Novell NetWare 4.1.0 as PC Managed Node

  Microsoft Windows NT 3.1, 3.5, and 3.51 as PC Managed Node

  Microsoft Windows NT 3.51 and 4.0 as Managed Node

- **Sun SPARC systems running SunOS**

  Sun SPARC series running SunOS 4.1.2 and 4.1.3

  OpenLook with jumbo Open Windows patch 100444-62

  Motif 1.2

- **Sun SPARC systems running Solaris**

  Solaris 2.3 with jumbo kernel patch 101318-59

  Solaris 2.4 with jumbo kernel patch 101945-23

  Solaris 2.5 or 2.5.1

  OpenLook

  Motif 1.2

The following is a list of minimum memory and swap space requirements for TME 10 User Administration.

Table 9. Minimum Requirements for Installing User Administration

Platform	Management Server	Management Stations	Swap Space
AIX	64 MB	48 MB	32 MB
HP-UX	64 MB	48 MB	32 MB
Windows NT	48 MB		24 MB
Solaris	64 MB	48 MB	32 MB
SunOS	48 MB	48 MB	32 MB

The following table shows the minimum system requirements for PC Managed Nodes for installing User Administration.

Table 10. Minimum Requirements for Installing User Administration on PC Managed Nodes

Platform	RAM	Disk Space
NetWare 3.x	2 MB	.5 MB
NetWare 4.x	4 MB	.5 MB
Windows NT	16 MB	.5 MB

5.2 Environment Description

The following picture shows the technical environment used for conducting our installation and tests. This environment can be used as an example for your own environment.

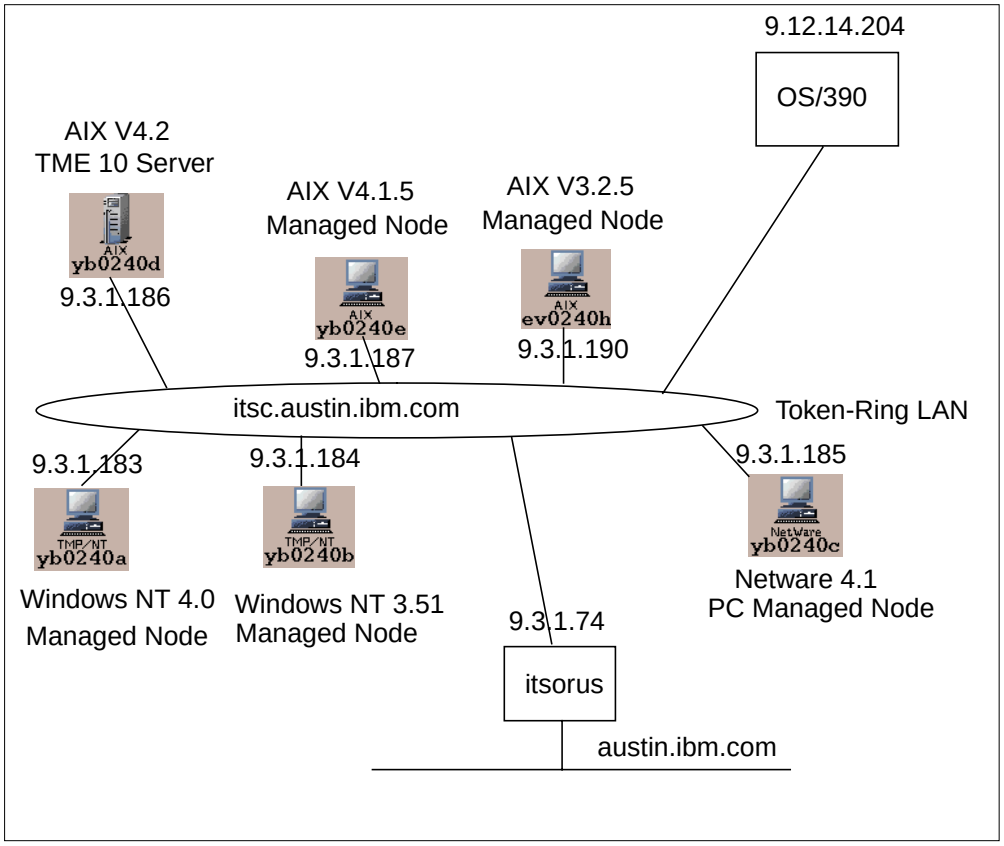


Figure 23. Technical Environment Description

- **TME 10 Server (yb0240d)**

  Machine type: RS/6000 with AIX V4.2

  Products installed:

  - TME 10 Framework Version 3.1
  - TME 10 Framework Version 3.1 Patch 3.1-TMP-0003 (required to install TME 10 User Administration Version 3.1)
  - TME 10 User Administration Version 3.1

- **TME 10 Managed Node (yb0240c)**

  Machine type: RS/6000 with AIX V4.1.5

  Products installed:

  - TME 10 Framework Version 3.1
  - TME 10 Framework Version 3.1 Patch 3.1-TMP-0003 (required to install TME 10 User Administration Version 3.1)
  - TME 10 User Administration Version 3.1

- **TME 10 Managed Node (ev0240h)**

  Machine type: RS/6000 with AIX V 3.2.5

  Products installed:

  - TME 10 Framework Version 3.1

- TME 10 Framework Version 3.1 Patch 3.1-TMP-0003 (required to install TME 10 User Administration Version 3.1)
- TME 10 User Administration Version 3.1

- **TME 10 Managed Node (yb0240b)**

  Machine type: Pentium system Windows NT 3.51

  Products installed:

  - TME 10 Framework Version 3.1
  - TME 10 Framework Version 3.1 Patch 3.1-TMP-0003 (required to install TME 10 User Administration Version 3.1)
  - TME 10 User Administration Version 3.1
  - TME 10 desktop

- **TME 10 Managed Node (yb0240a)**

  Machine type: Pentium system Windows NT 4.0

  Products installed:

  - TME 10 Framework Version 3.1
  - TME 10 Framework Version 3.1 Patch 3.1-TMP-0003 (required to install TME 10 User Administration Version 3.1)
  - TME 10 User Administration Version 3.1

- **TME 10 PC Managed Node (yb0240c)**

  Machine type: Pentium system Novell NetWare 4.1

  Products installed:

  - TME 10 PC TCP/IP Agent Version 4.005
  - TME 10 User Administration Version 3.1

5.3 Installing the TME 10 Framework

Since the TME 10 Framework (TMF) is a prerequisite for the installation of TME 10 User Administration, this chapter provides you with step-by-step installation instructions of the Framework on our technical environment. This can be used as an example to set up your own environment.

5.3.1 Installation Considerations

When installing the TME 10 Framework on a system, the binaries, libraries, and the TME database or the PC Agent software are installed on the system. These files take up disk space and system resources; so the initial planning is an important step in performing the TME installation.

By default, on UNIX machines, the main portion of the software is installed into two directories:

- /usr/local/Tivoli for the binaries and libraries
- /var/spool/Tivoli for the database

You may want to consider making separate file systems for installing these files. You may also choose to save some space by sharing directories between several systems with Network File Systems (NFS). These directories must be mounted before installing the client machines. The libraries, binaries, manual pages, X11 resource files, and message catalogs can all be safely shared within the boundaries of a Tivoli Management Region with the following exceptions:

- The libraries should be local to a UNIX TME server because the server's root user must have write access to that directory.
- The subdirectory with the task libraries and oserv.exe should always be local on Windows NT managed nodes.

The database (the files in /var on UNIX, the oserv directory on Windows NT) cannot be shared. This is true for the TME server as well as for all other managed nodes. If using NFS for sharing, simply mount the directories before the installation process begins.

Also on UNIX machines, two setup files are created after installation. These files contain shell script code that must be executed at user login to establish the correct paths and environment variables. The files are:

- */etc/Tivoli/setup_env.sh* for Korn shell or Bourne shell
- */etc/Tivoli/setup_env.csh* for C shell

Another consideration is that of host name to IP address conversion. Name lookups must be able to be performed from the server both ways (name to address, address to name) for all hosts that will be defined as clients in the TMR.

A license key is needed to install each TME server. This license key is normally provided along with the TME 10 Framework CD-ROM.

The TME server may either be a UNIX or Windows NT system. Instructions for installing the TMF on your TME server is the next topic for discussion.

5.3.2 Installing the UNIX TME 10 Server

To install the Tivoli Management Framework on UNIX systems, use the following steps:

1. Make sure you are a root user in a Windows environment and that your `DISPLAY` variable is properly set. You can check this value simply by entering the following command:

   ```
   echo $DISPLAY
   ```

   By default this value should be set to `:0.0`. If the environment variable is not properly set, enter the following command:

   ```
   export DISPLAY=:0.0
   ```

2. Mount the CD-ROM containing the TMF software for UNIX.

3. Create an installation directory called /usr/local/Tivoli/install_dir and then change to that directory. It may be necessary to create lower-level directories first.

   ```
   # mkdir /usr/local/Tivoli/install_dir
   # cd /usr/local/Tivoli/install_dir
   ```

4. The following command will copy some installation software onto disk:

   ```
   # /<cdrom_path>/<mgmtplatform_path>/WPREINST.SH
   ```

   `cdrom_path` is the mount point for the CD-ROM, and `mgmtplatform_path` is the path to the TMF software on the CD-ROM. We mounted the CD-ROM on the /cdrom directory, and the wpreinst.sh is found on the top-level directory there. Run the following command:

   ```
   # /cdrom/WPREINST.SH
   to install, type ./wserver -c /cdrom
   ```

5. Start the installation with the following command:

   ```
   # ./wserver -c /cdrom
   ```

6. This will bring up a window to start the installation (shown in Figure 24). The top portion of the window allows you to change the directories in which the Tivoli software will be installed, if desired. There are also three options at the bottom of the window that allow you to decide whether or not the directories you have chosen will be created automatically and to set the startup characteristics of the oserv daemon.

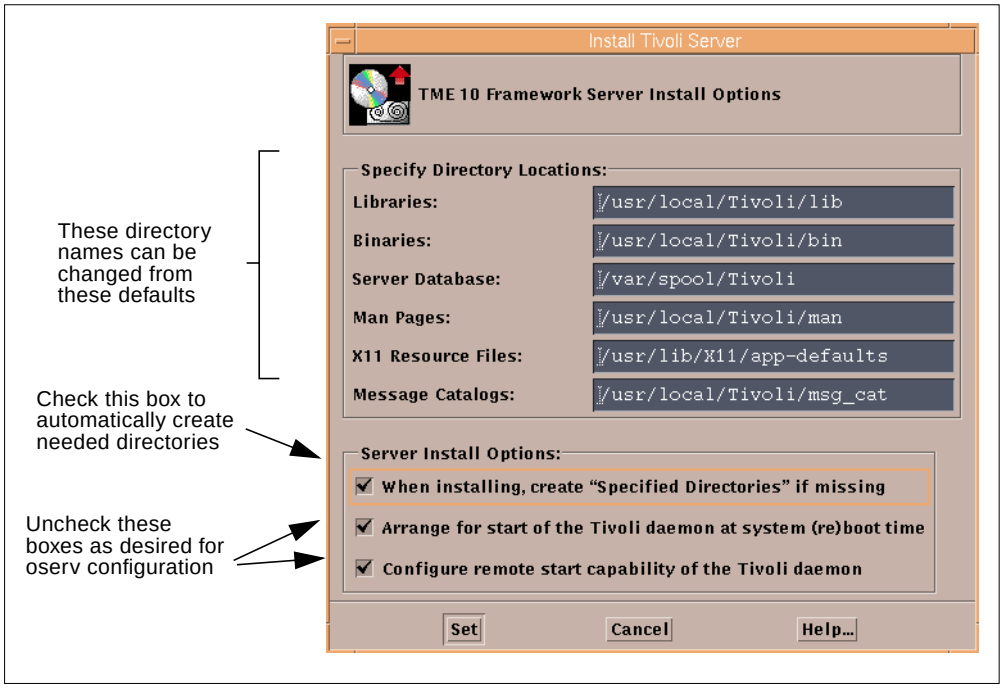


Figure 24. Installation Options Window

7. In the next window that appears, shown in Figure 25, you will be asked to enter the TME 10 license key for your software. This is the only mandatory step for this window. You can set the encryption level for the TMR as well as an optional installation password at this point. The initial policy region's name can be changed as well as the TME server's name to be shown on the desktop. You can also click on the **Install Options...** button to bring up the window shown in Figure 24 again.

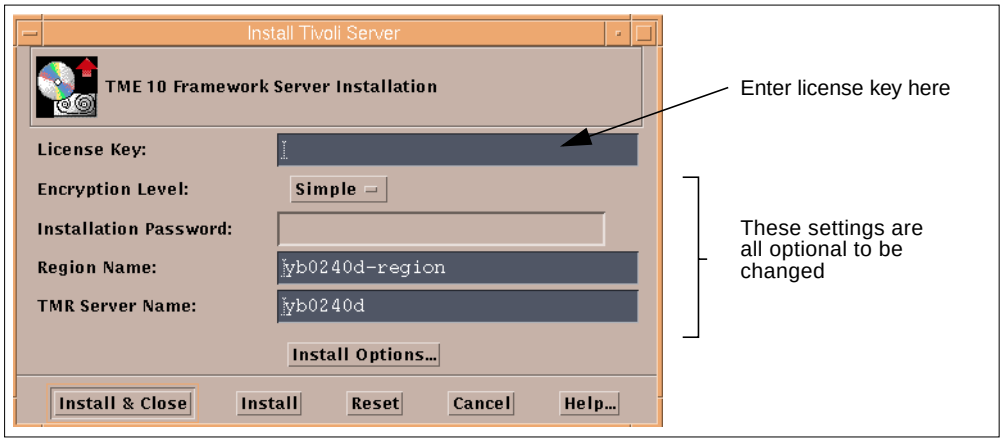


Figure 25. More Server Installation Options

Click the **Install & Close** button to continue.

8. A window will then show the procedures that will be performed on your system (shown in Figure 26). This window provides the last chance to cancel the operation.

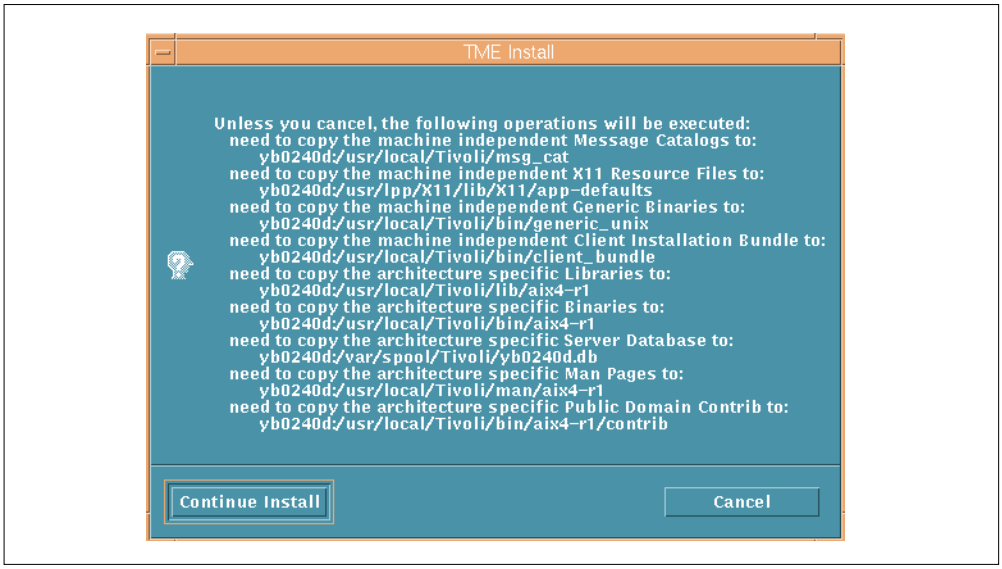


Figure 26. Server Installation Verification Window

Click on the **Continue Install** button to continue.

9. The installation begins and a window will show the status of the installation. Wait for the "`Completed`" message to appear at the bottom of this window and for the **OK** button to appear. Click on the **OK** button to make the window disappear. The Tivoli Management Framework has been installed on the server. The Tivoli desktop will also appear and will be ready to use.

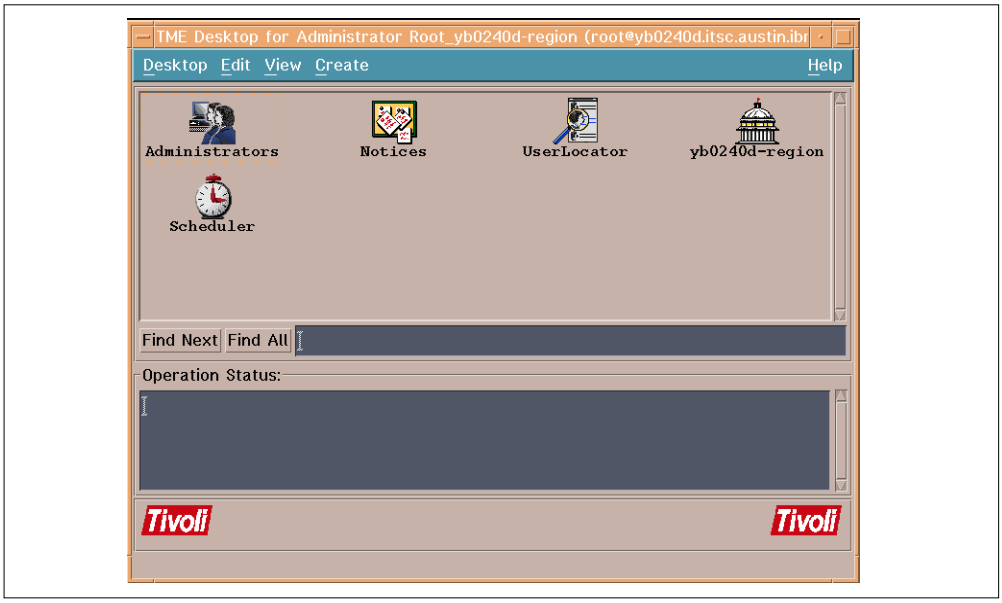


Figure 27. TME 10 Desktop

5.3.3 Installing UNIX Managed Nodes

Installing the client version of the TMF on UNIX systems is done by creating a Managed Node icon within the TME desktop. Our TME server is installed on the

system named yb0240d, and we want to install the TME 10 client code on the UNIX system ev0240h. The steps for doing this follow:

1. Start the TME desktop using the `tivoli` command. You might first need to run the following command in order to set up the Tivoli environment:

   ```
   # . /etc/Tivoli/setup_env.sh
   ```

   We actually recommend that you put this command in your .profile file to avoid entering it each time you need to start the Tivoli desktop.

2. Open the policy region on the TME desktop where you would like to add the managed node icon. This is done by double-clicking on the policy region icon (yb0240d-region in our example).

3. From the policy region window, select **Create**, then **ManagedNode...** The window shown in Figure 28 will appear. You must set the following:

   - TMR Installation Password – Can be left blank if a password was not set during the TME server installation process.
   - Default Access Method – This can either be the remote machine's root password, or you can have previously defined a trusted relationship between the server and the clients using the .rhosts file, for example. If not already done, define a .rhosts file in the root user's home directory on ev0240h, and add root on yb0240d in it. Test the trusted host access by issuing the following command on yb0240d:

     ```
     # rsh ev0240h ls
     ```

     If you get a listing of the home directory of root on ev0240h, you can check the Trusted Host Access radio button.

   - Clients – You must define one or more clients on which to install TME and whether they will use the default access method or something different. Use the **Add Clients...** button and enter ev0240h.
   - Installation Options – Set the remote directories in which to install the software, whether or not these directories will be created automatically, and characteristics of the oserv daemon's behavior. You get the same window as shown in Figure 24 on page 90 for the TME server.
   - Select Media – Lets you define where the TMF software can be found for installation. If the CD-ROM is still mounted on the TME server, you don't have to set anything here.

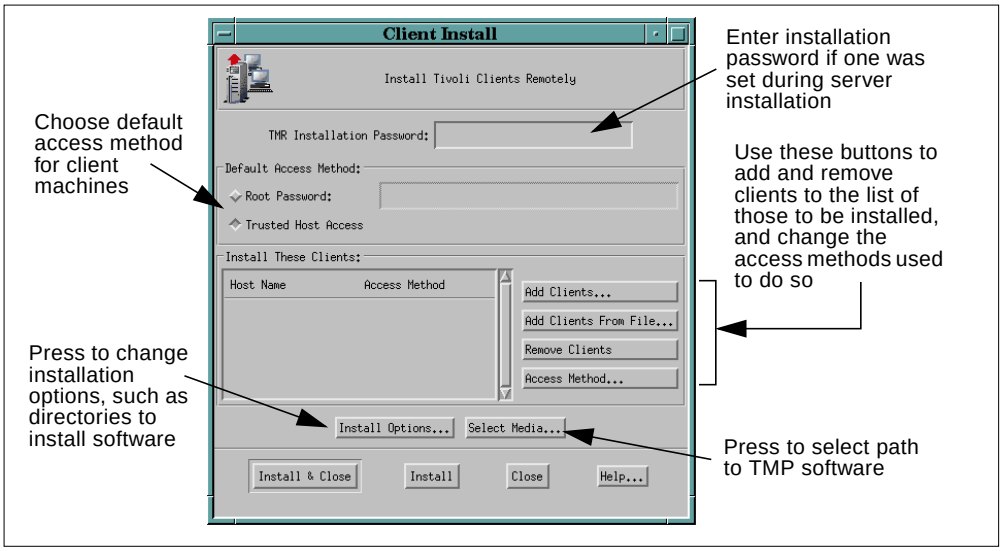


Figure 28. Client Installation Window

When information in this window is properly entered, click on the **Install** or **Install & Close** option.

4. The client install window appears and let you know the actions that will be performed if you continue with the installation. Click on the **Continue Install** button to continue.
5. The same window will remain on the screen and show you the status of the installation. Wait for the "`Finished client install`" message to ensure completion of the client installation. You should then click the **Close** button to close the status window. The managed node icon for this machine should now appear in your policy region.

5.3.4 Installing Windows NT Managed Nodes

Because the scripts used in creating managed nodes rely on the `rsh` and `rexec` commands, it is not possible to perform installations on Windows NT systems without doing some initial preparation. Windows NT systems do not have by default services equivalent to the `rexecd` or `rshd` daemons.

TME 10 provides what is called the *Tivoli Remote Execution Service* that must be installed on the Windows NT system first. Then the system can be installed from the TME 10 server as a Managed Node. The *Tivoli Remote Execution Service* is referred to as TRIP, and instructions for installing it follow:

Make sure you are logged in as Administrator and have the CD-ROM containing the TME software for Windows NT accessible.

Note:

The TRIP code can also be transfered from the TME server (by using FTP) to the Windows NT Managed Node and installed from a local directory.

6. On Windows NT 3.51, go to the Program Manager's *File* menu, select the **Run...** option, and enter the following command:

```
F:\TRIP\SETUP
```

where F: is the drive letter for your CD-ROM drive.

On Windows NT 4.0, click on the **Start** button located on the Taskbar and select **Run**. Then enter the same command.

7. This will bring up an installation *Welcome* window, as shown in Figure 29.

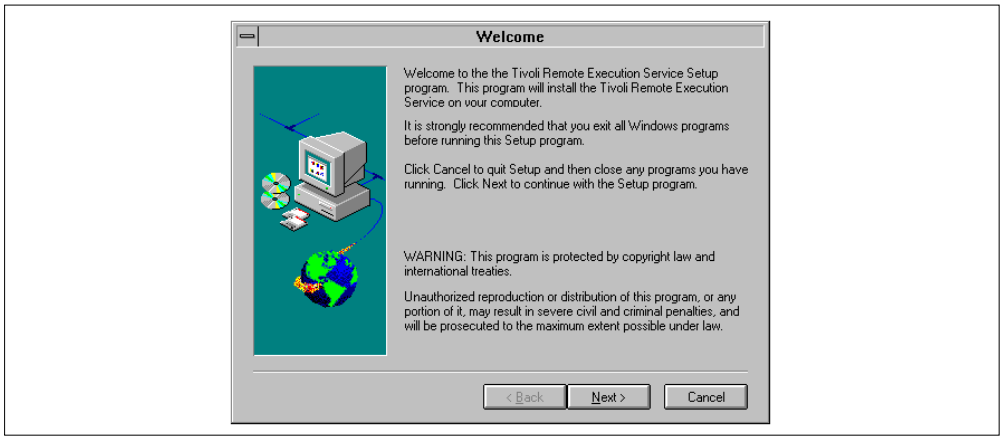


Figure 29. TRIP Welcome Window

Click the **Next >** button to continue the installation.

8. Another window will appear that allows you to choose the destination directory for the TRIP installation. You can choose the default, or click the **Browse...** button to enter your own directory.

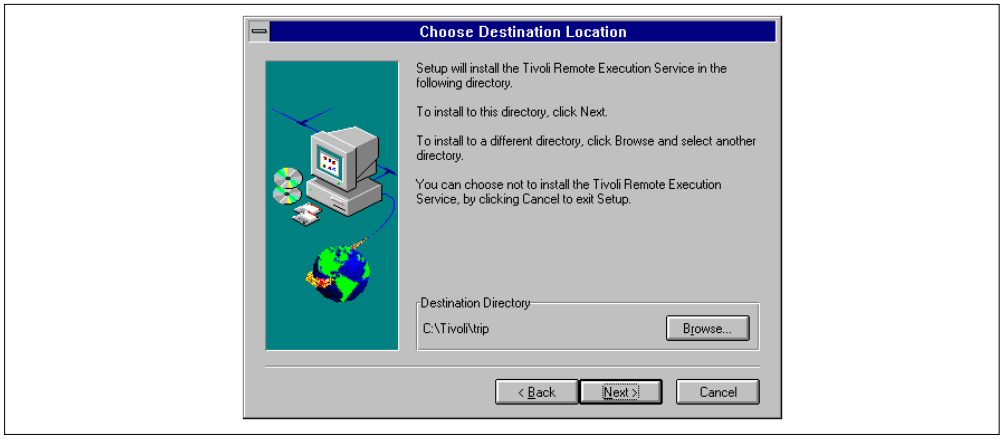


Figure 30. Destination Location Window

After the directory has been chosen, click the **Next >** button to continue.

9. A status window will then appear, showing the status of the TRIP installation. Near the end of the installation, a DOS window will appear instructing you to press any key to continue the installation. It will ask if you'd like to view the README file, and eventually you will see a window saying the installation of TRIP is complete.

10. Now that the TRIP has been installed, you can go to the TME server and create a managed node using this NT system as your target, just as you would for a UNIX system. For details on how to do this, see the previous section.

Note on TRIP

An important thing to note about the installation of the Tivoli Remote Execution Service is that it needs to be installed once per TMR only. After the initial installation, as new Windows NT managed nodes are created, the TRIP software will be installed from this initial Windows NT node.

5.3.5 Installing NetWare PC Managed Nodes

Installing a NetWare PC Managed Node requires TCP/IP on the NetWare server. If TCP/IP is not already set up on your server, you will find below some installation hints and tips that we used for setting up our own environment.

5.3.5.1 Setting Up TCP/IP on the NetWare Server

Before installing the TME 10 PC Agent on NetWare, TCP/IP must be installed on the server(s) that will be defined as PC Managed Nodes.

TCP/IP on NetWare General Considerations

NetWare TCP/IP is a transport subsystem that brings TCP/IP connectivity to NetWare. It is a collection of NetWare Loadable Modules (NLM) designed to support applications requiring TCP/IP connectivity.

There are different ways to implement TCP/IP on a NetWare environment:

- Replacing NetWare's IPX with TCP/IP. Then let's suppose that all the NetWare clients are running TCP/IP as well.
- Using both TCP/IP and IPX/SPX on the NetWare clients (Windows 95, Windows NT and so on)
- Running both IPX/SPX and TCP/IP on the NetWare server. In this case, the server is used as a gateway between the IPX world and the TCP/IP world.
- Tunneling IPX and IP packets. In this case IP must be supported without IPX coexisting, especially for internetwork support within a company or to the Internet. To provide IPX support across an internetwork, the IPX packets must be encapsulated into IP packets, a process called *tunneling*. At the receiving device, the IP packet header is stripped off and the IPX packet rerouted into the destination network.

In our case, we run both TCP/IP and IPX/SPX on the NetWare server. The server acts as a gateway.

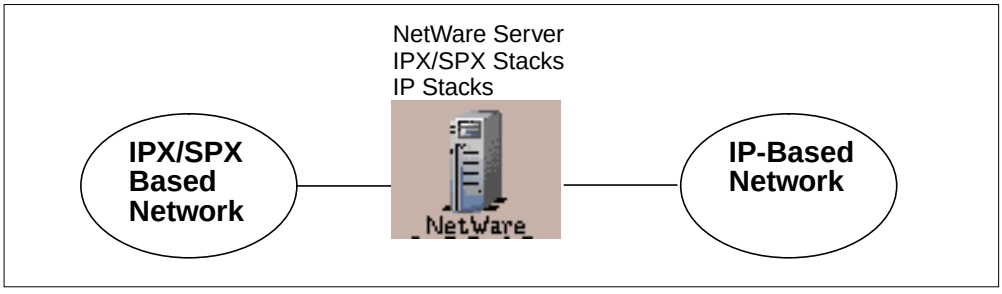


Figure 31. IPX/SPX and TCP/IP Stacks on NetWare Server

The NLMs modules for TCP/IP included in NetWare 4.1 are:

- NetWare TCP/IP NLM (TCPIP.NLM)
- Simple Network Management Protocol NLM (SNMP.NLM)
- SNMP event logger NLM (SNMPLOG.NLM)
- TCP/IP console NLM (TCPCON.NLM)
- IP configuration NLM (IPCONFIG.NLM)

NetWare 4.1 just provides the transport layers of TCP/IP. Most TCP/IP applications and APIs are not supplied by NetWare. SNMP, Line Printer Daemon, Mail Gateway, and the TCP/IP developer's Toolkit are supported.

Installing and Configuring TCP/IP on NetWare 4.1
Following are the steps required to install TCP/IP on NetWare 4.1:

1. The NLMs and drivers (SNMP.NLM, TCPIP.NLM, TCPCON.NLM, IPCONFIG.NLM and IPTUNNEL.LAN) are located in the SYS:SYSTEM directory, and the TCP/IP databases (Services, Protocol, Hosts, Networks, Gateways) are in the SYS:ETC\SAMPLES directory.

   For the databases to be used, they have to be moved to the SYS:ETC directory. These databases are ASCII files and can be viewed or modified with a simple editor.

2. The Maximum Physical Receive Packet Size should be adjusted. In the standard NetWare installation, the value may not be large enough to hold TCP/IP data link packets. The maximum physical receive packet size is changed in the STARTUP.NCF file and given the following value:

   ```
   Set Maximum Physical Receive Packet Size=2048
   ```

3. The Packet Receive Buffers size should also be checked and changed. When NetWare is installed, the default value is 100, and it may be sufficient. MONITOR.NLM can be used to see how many packet receive buffers are currently allocated before changing its value. The maximum packet receive buffers figure is changed in the AUTOEXEC.NCF file to the following value:
   `Set Maximum Packet Receive Buffers=200`

4. As with most NLMs modules, you must issue the `LOAD` command in order to load the TCP/IP protocol stack, and then `BIND` it to the network board driver. These tasks can be performed manually or by using the INETCFG.NLM utility (menu driven) to build your TCP/IP configuration.

   Note: NetWare 4.X LAN drivers are compliant with Open Data Link Interface (ODI). This means that it is possible to run simultaneously multiple network protocols on the same network adapter.

   The command for loading the TCPIP.NLM module is `LOAD TCPIP`. Following is the complete syntax of the `LOAD` command:

   ```
   LOAD TCPIP [FORWARD=YES]
   ```

   where:

   `FORWARD=YES` means that IP routing is enabled

   Note: Uppercase is used in command-line examples. However, case isn't important to NetWare. You can use lowercase or a mix of cases.

   When the TCPIP.NLM is loaded, the SNMP support module is automatically loaded also. If TCP/IP is manually unloaded, however, the SNMP support module isn't automatically unloaded. The module must be unloaded manually.

5. You then need to load the LAN driver. TCP/IP accepts Ethernet or token-ring LAN drivers, but it uses a different frame format from IPX.

   For Ethernet, TCP/IP uses the Ethernet V2 (ETHERNET_II) frame format instead of Ethernet IEEE 802.3 (ETHERNET_802.3). For token-ring, TCP/IP uses the SNAP (TOKEN-RING_SNAP) frame format instead of the token-ring (TOKEN-RING).

   In our case, we inserted the following command in the AUTOEXEC.NCF file:

   ```
   LOAD NTR2000 SLOT=4 FRAME=Token-Ring_Snap NAME=NTR2000_IP
   ```

   where:

   `NTR2000` is the LAN Adapter Driver

   `SLOT=4` is the number of the slot where the LAN adapter is located.

6. You then need to bind IPX and IP to their respective LAN drivers. Binding the TCP/IP NLM to the network board driver is necessary to provide the link to the network. The `BIND` command has several optional parameters, and some mandatory parameters that are shown in Table 11.

Table 11. IP Configuration Options

Parameter		Argument	Default
ADDR	Required	IP address	None
MASK	Optional	Network mask	Standard
ARP	Optional	Yes/No	Yes
GATE	Optional	IP address	None

The parameters given in the table above are described as follows:

ADDR=Local IP address (9.3.1.185 in our example)

MASK=Subnetwork mask (255.255.255.0 in our example). The setting depends on the class of the network.

ARP=Use of Address Resolution Protocol (ARP). When set to YES (the default), the driver uses the Address Resolution Protocol on the network (which maps IP addresses and physical addresses). When set to NO, ARP isn't used for address resolution.

GATE=Default Gateway to be used if there is no specified destination for a packet. In our case it is 9.3.1.74.

The following `BIND` command has been added to our AUTOEXEC.NCF file.

```
BIND IP TO NTR2000_IP ADDR=9.3.1.185 MASK=FF.FF.FF.0 GATE=9.3.1.74
```

The complete AUTOEXEC.NCF file that is used in our example is listed below:

```
Mount All

load tcpip forward=yes
load ntr2000 slot=4 Frame=Token-Ring_Snap Name=ntr2000_ip
bind ip to ntr2000_ip addr=9.3.1.185 mask=ff.ff.ff.0 gate=9.3.1.74
load route name=ntr2000_ip rsp=ar time=10

load ntr2000 slot=4 Frame=Token-Ring Name=ntr2000_ipx
bind ipx to ntr2000_ipx net=00007007
load route name=ntr2000_ipx rsp=ar time=10
```

Hint

We found that when NetWare server is installed for first time, the installation added one line to the AUTOEXEC.NCF: `sys:etc\initsys.ncf`. You might need to comment this line to avoid binding IP or IPX to different network Adapters.

7. You can check your TCP/IP installation by using the PING command provided in NetWare 4.1. On the NetWare server type the following command:

   `: load ping`

   The PING.NLM is then loaded and the screen appears with the fields Host Name and Seconds to Pause Between Pings.

   Enter the name or the IP address of the host you want to contact. Ping tries to contact the machine or the IP address that you entered in the **Host Name** field. It then sends packets of data to the machine and waits for responses, measuring the time taken for the round trip. It shows summary statistics.

   If you desire to terminate the ping command, only press the ESC key and the PING command will terminate.

5.3.5.2 Installing the TME 10 PC Agent on NetWare

It is not possible to install the code directly on the server itself. It is necessary to install it from a NetWare client running Windows (Windows 3.1, Windows for Workgroups, Windows 95 or Windows NT). This client must be able to access the NetWare server through IPX or TCP/IP. It can be a Windows 95 client running IPX, it can also be a Windows NT system running Client Services for NetWare (CSNW) or a Windows NT system accessing the NetWare server through a Windows NT server acting as a Gateway Services for NetWare (GSNW installed).

In our environment, we choose to setup the Windows NT server as a client for NetWare by installing the Client Services for NetWare (CSNW). The following describes how to install CSNW.

1. On Windows NT, Open the Control Panel and double click on the Network icon.

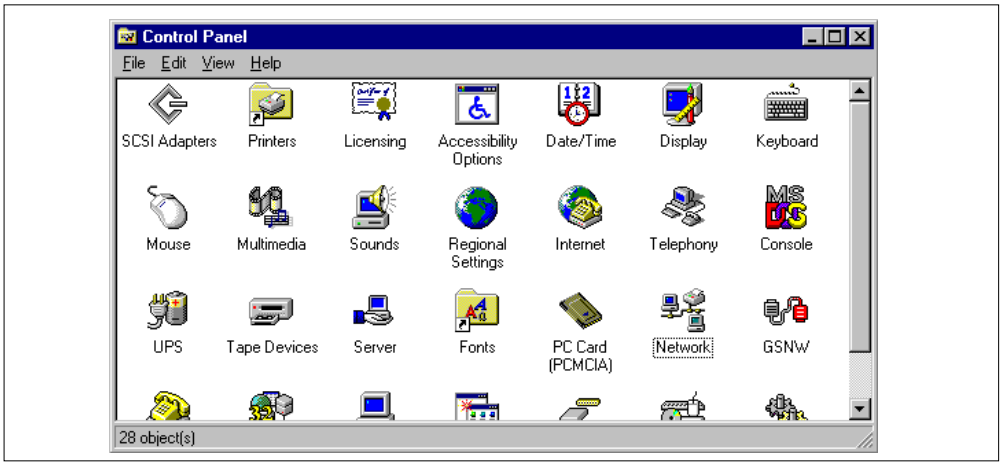


Figure 32. Windows NT Control Panel

2. Select **Services** then **Add...** and select the **Gateway (and Client) Services for NetWare** by double-clicking on it.

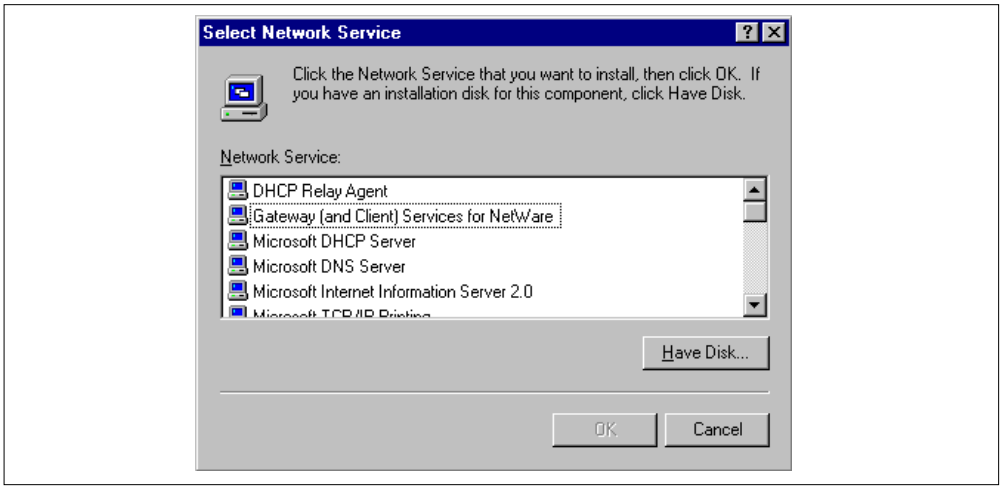


Figure 33. Selecting the Network Service to Install

3. Tell Windows NT Setup the path to copy the files from. It can be from a file server or from the CD-ROM drive.

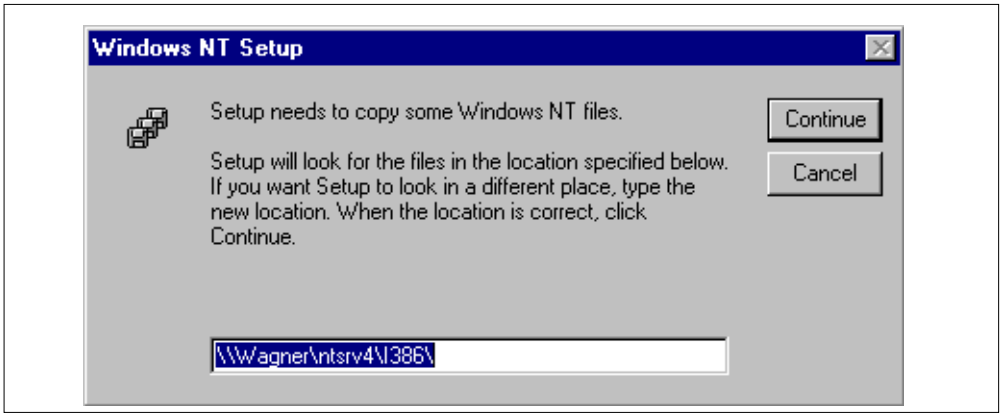


Figure 34. Windows NT Setup

4. Click **OK** to finish the installation. Windows NT will copy the appropriate drivers to your system and make changes to your registry. The Client Service for NetWare will be loaded the next time your start your system. Close the Network Dialog box and your bindings will be reconfigured.
5. Once you reboot the system, Windows NT attempts to log on to the NetWare server for the first time. With the client software provided by Microsoft, you can either logon to a NetWare Server 3.X by clicking on the **Preferred Server** radio button shown in the dialog window, or you can log on to a 4.X NetWare Directory Service Tree by clicking on the **Default Tree** and **Context** radio button. Enter the name of the Tree and its context. In our case the following are the necessary parameters:

   ```
   Preferred Server= yb0240c

   User = Admin

   Default Tree = ITSO

   Default Context = ITSO
   ```

Once you can access the NetWare server from a Windows system, you can install the TME 10 PC Agent code for NetWare.

The TME 10 PC Agent software is shipped on CD-ROM with the TME 10 Framework. The code is located under the directory PC. Below the directory PC are the subdirectories DISK1, DISK2, DISK3, and DISK4. These subdirectories contain the IPX/SPX agent. The content of these directories can be put onto diskettes or transferred with FTP to the Windows NT system used for installing the PC Agent. The procedure to install the PC Agent is as follows:

1. From Windows NT, map a NetWare volume as Administrator.
2. Start the Windows NT Explorer, open the Disk1 directory and run the Setup.exe file.

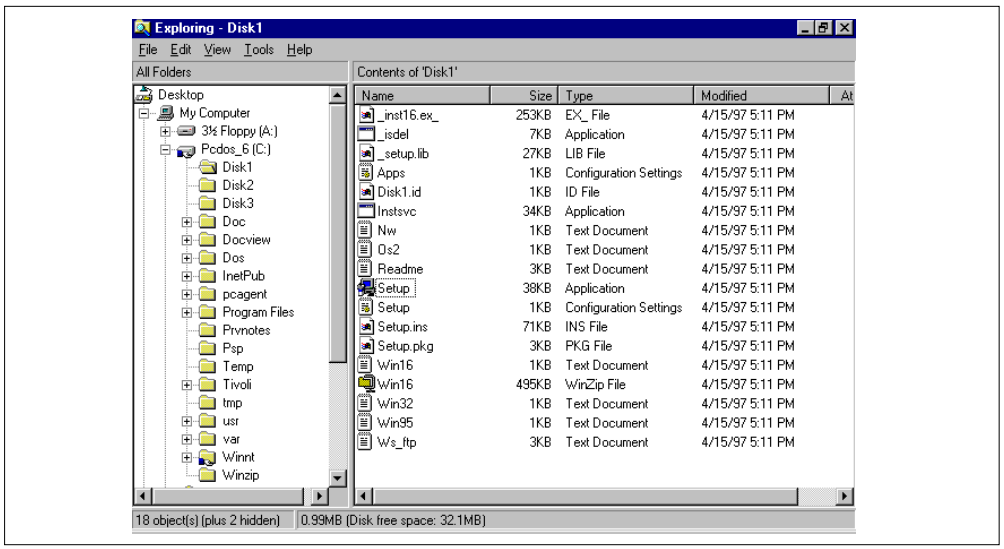


Figure 35. Windows NT Explorer

3. A Welcome installation window will lead you through the PC Agent installation and will display option and information dialogs that provide you with the necessary information. When enabled, use the Back, Next, or Cancel buttons

to navigate through these option dialogs, as illustrated in the Welcome dialog below.

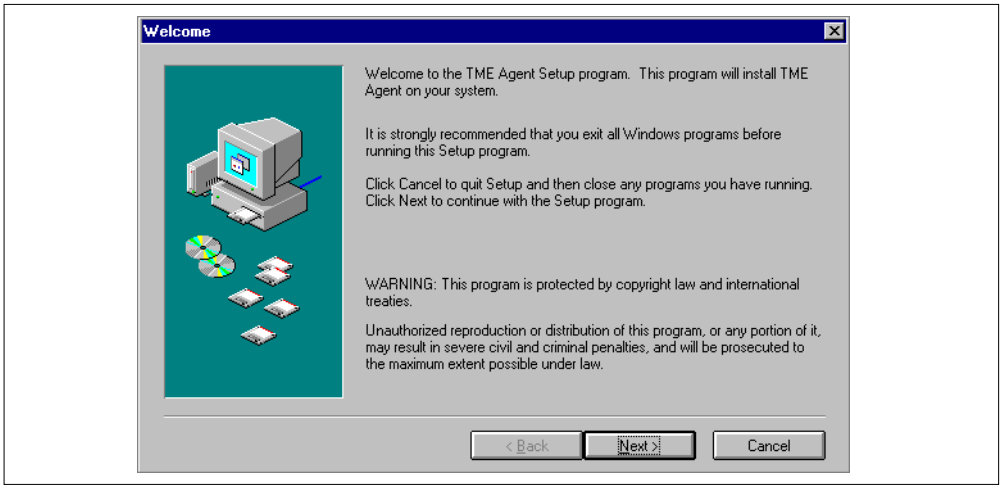


Figure 36. Welcome Installation Window

4. Click on the Next button to display a dialog similar to the following, and select the **NOVELL NetWare** platform to install the PC Agent.

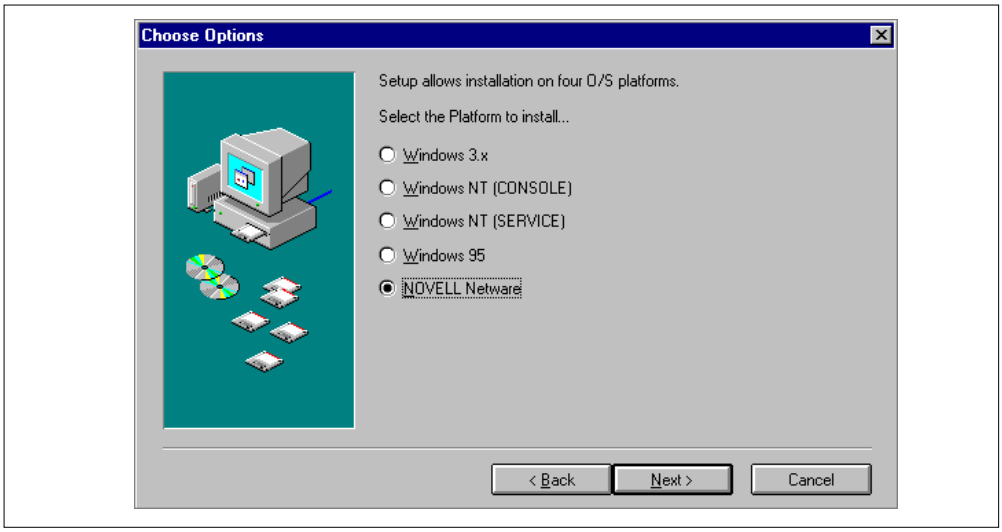


Figure 37. Choose Options Window

5. Specify on which NetWare volume you want to install the PC Agent. Click on the **Next** button to proceed the next dialog.

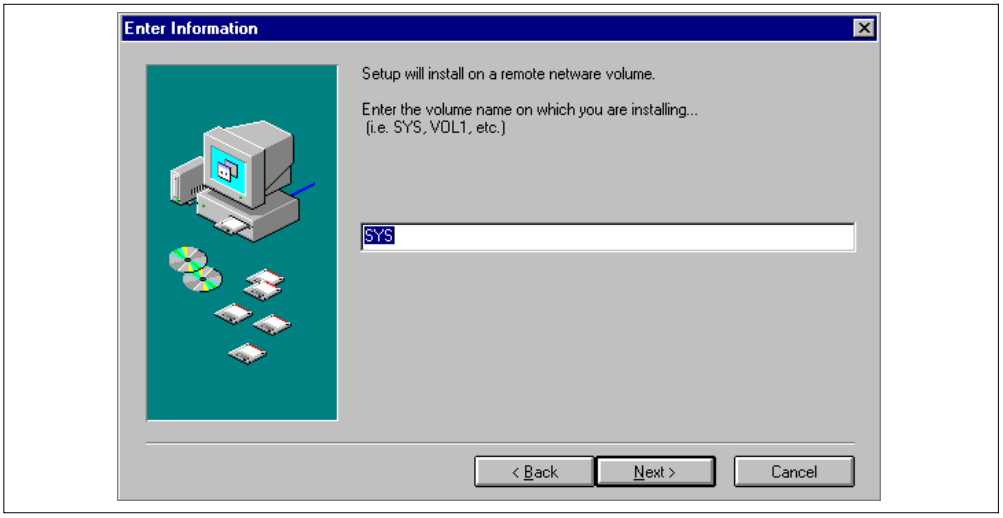


Figure 38. Specifying the NetWare Volume

6. Enter the destination drive on which to install the PC Agent. The drive letter you must enter here is an NT network drive mapped to a NetWare volume. By default, the setup program installs the agent on the C drive; so it is necessary to change the drive to F (in our example).

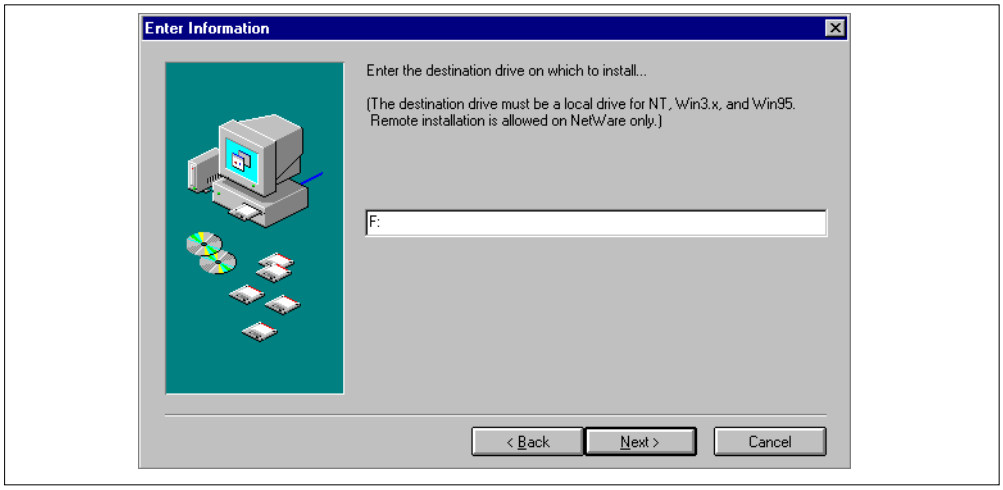


Figure 39. Entering the Destination Drive

7. Click on the **Next** button to proceed to the next dialog.
8. Specify the NetWare volume on the server on which you want to install the product.

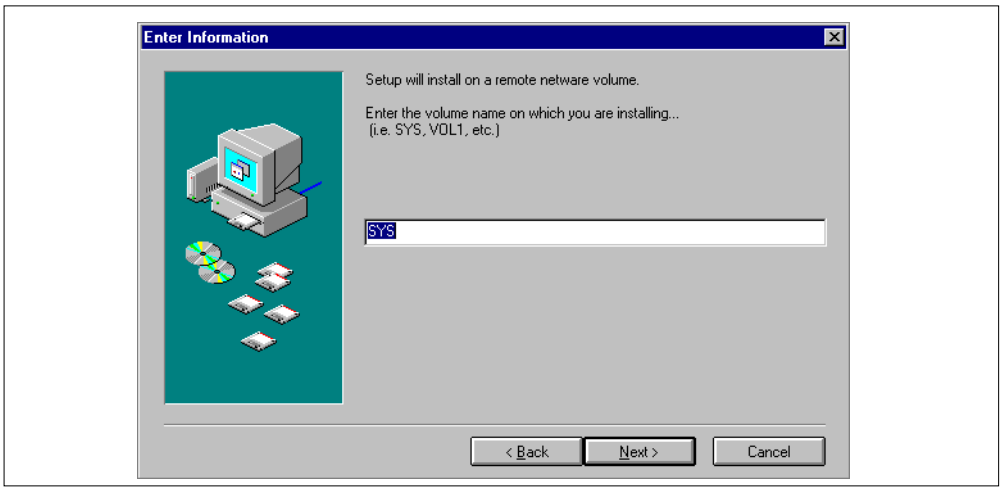


Figure 40. Specifying the NetWare Volume

9. Respond Yes to the following question if you want the product to be installed on the directory \TIVOLI\TMEAGENT.

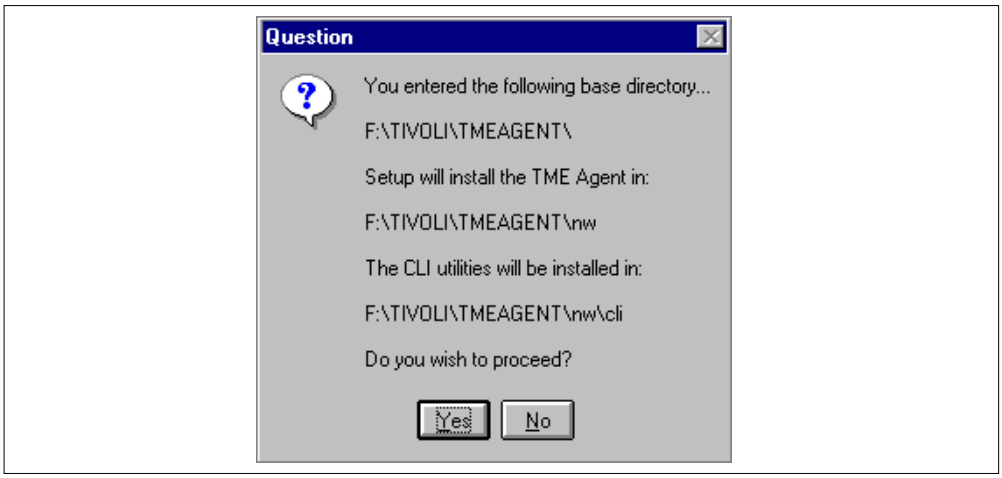


Figure 41. Checking the Directory on Which the Product is Installed

10. Select the **Start Automatically** checkbox to start up the PC Agent every time the system is started.

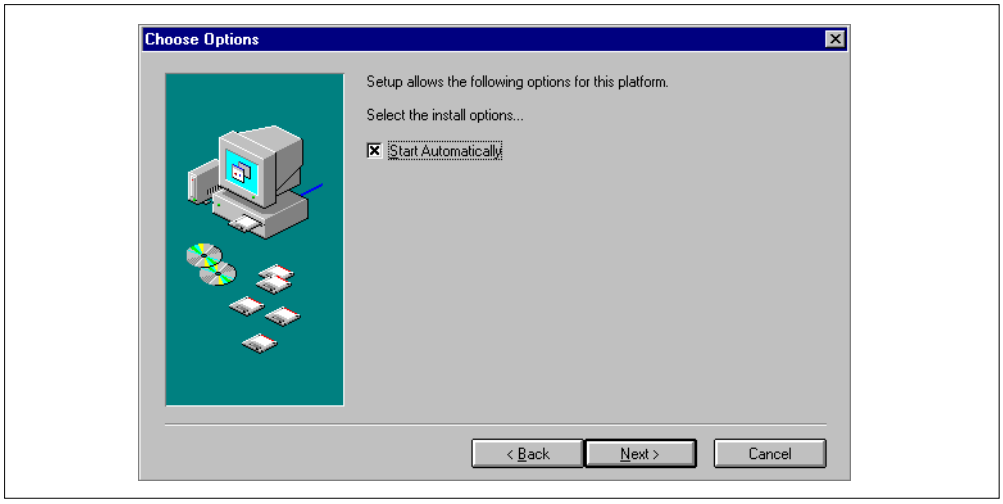


Figure 42. Start the PC Agent Option Automatically

5.3.5.3 Creating the NetWare PC Managed Node

Once the TME 10 PC Agent is installed, you can create within a Policy Region the NetWare PC Managed Node from the TME 10 desktop.

Attention!

Tivoli recommends that you install the PC Agent before creating the PC Managed Node. If the PC agent is installed first, when the PC Managed Node is created, TME 10 will verify that there is a connection to the PC and that the PC Agent is running properly. If the PC Agent is not installed first, the PC Managed Node will be created, but the verification will not be performed.

The following table provides the context and authorization role required for creating a NetWare PC Managed node:

Table 12. Authorization Role for Creating a NetWare PC Managed Node

Activity	Context	Required Role
Create a PC Managed node	Policy region	**install_client**

Following are the steps to create a NetWare PC Managed Node from the TME 10 desktop:

1. Double-click on the policy region in which you want to create the PC Managed Node.

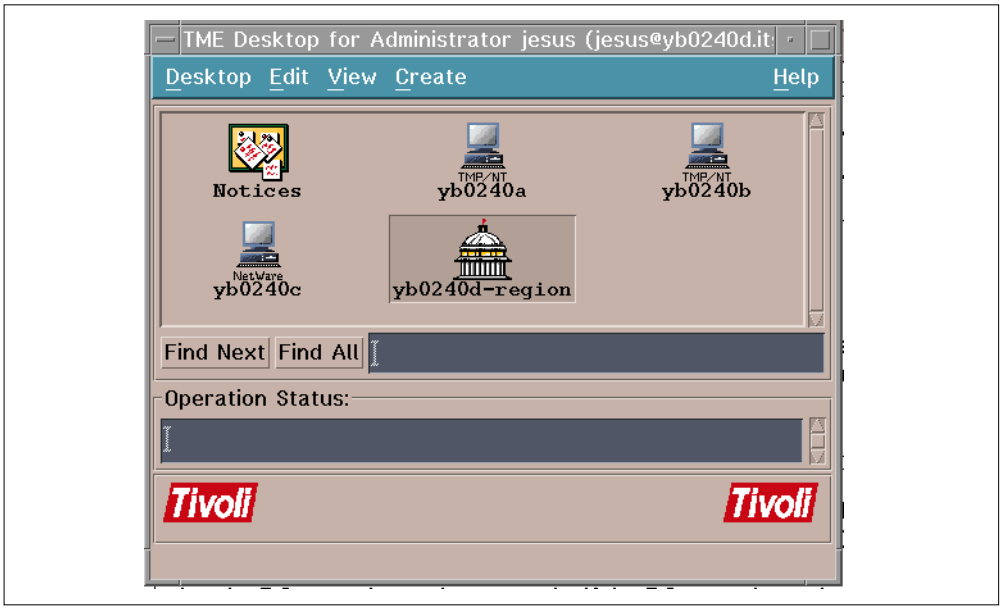


Figure 43. Desktop for Administrator jesus

The Framework displays the Policy Region window:

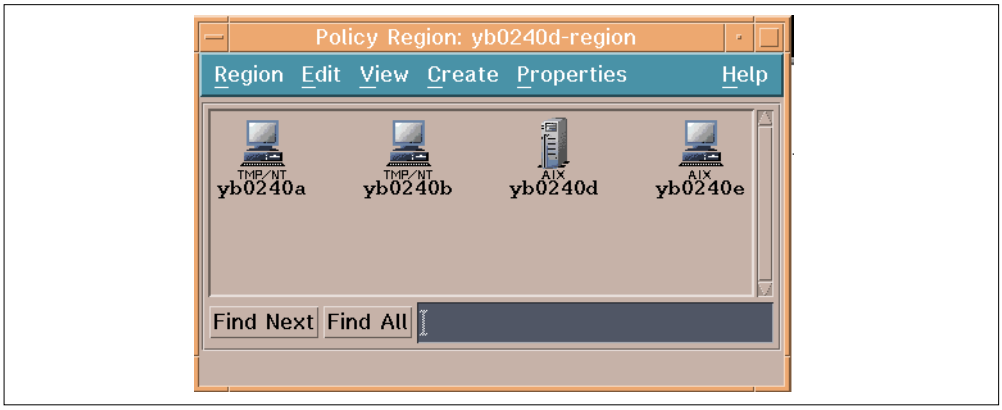


Figure 44. Policy Region

2. Select **Create**, then **PC Managed Node...** The Framework displays the Create PC Managed Nodes dialog.

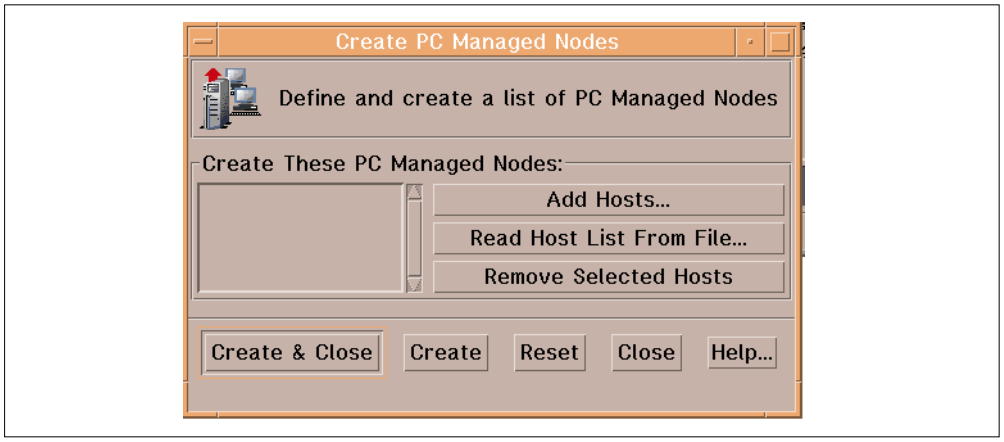


Figure 45. Create PC Managed Nodes Dialog Window

3. Add the names of the PCs you want to install as managed nodes. Click on **Add Hosts...** and the Framework displays the Add Hosts dialog window.

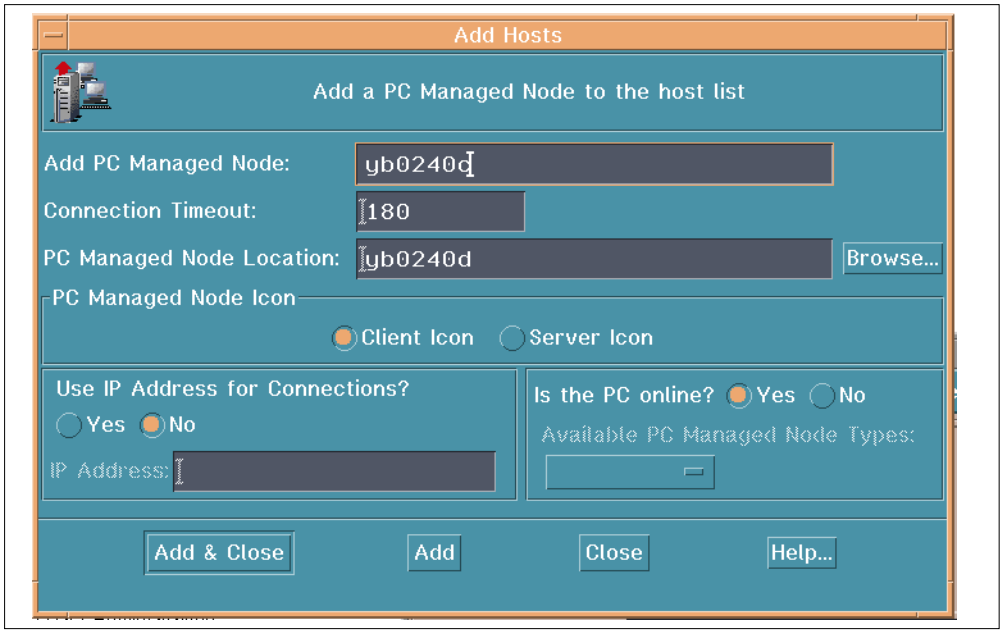


Figure 46. Add Hosts Dialog Window

4. Enter the name of the NetWare server in the Add PC Managed Node field. In our case, the PC name is yb0240c.
5. In the Connection Timeout field, enter the number of seconds that pass without a connection before the operation times out.
6. In the PC Managed Node Location field, specify in which client the PC Managed node object should be created. In our case the PC Managed Node Location is yb0240d.
7. Click on either the **Client Icon** radio button or the **Server Icon** radio button to specify which icon type will be displayed in the policy region window. In our case we selected the **Client Icon**.

8. Indicate whether the IP address should be used to connect to the PC by selecting either the **Yes** radio button or the **No** radio button. If you select the **Yes** radio button, you must enter the IP address of the PC in the IP Address field. If the PC managed node is representing a PC that is running Dynamic Host Configuration Protocol (DHCP), select **No**. In our case the selection is **No**. Because of the nature of DHCP, we will not know the IP address to enter in the IP Address field. In general, selecting **No** is better because IP addresses change more often than machine names.
9. Indicate whether the PC is currently online by selecting either the **Yes** radio button or the **No** radio button. In our case the PC is online. If the PC is not online, the PC Managed Node will still be created. However, TME 10 will not be able to verify that the PC Agent is installed and running or that the connection to the PC is properly established.
10. Choose the PC type from the Available PC Managed Node Types option menu. In our case the type is NetWare**.**
11. Click on **Add & Close** to add the PC managed node and return to the Create PC Managed Node dialog.
12. As we add PCs with the Add Hosts... button, the PC names are displayed in the Create These PC Managed Nodes scrolling list. The following dialog shows the clients that will be installed in the TMR.

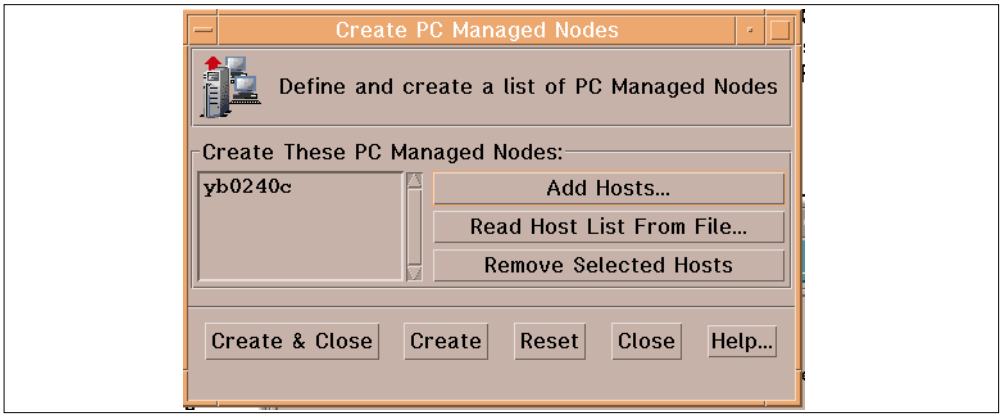


Figure 47. Create PC Managed Nodes Dialog Window

13. Click on **Create & Close** to create the PC managed node and return to the policy region dialog.

Note: Creating a PC Managed Node can also be performed by using the command line interface. The command to use is the `wcrtpcmngnode` command. For information on that specific command, see the *TME 10 Framework Reference Manual*.

5.3.6 Backing Up the Database

Once you have installed the TME 10 server and the UNIX and Windows NT Managed Nodes, we strongly recommend that you back up the TME 10 database. This operation must ALWAYS be performed before installing additional TME 10 clients, products or patches. By doing this operation, you will be able to avoid any inconsistency or wrong state in the TME 10 database. If errors occurred in an

installation, you will be able to restore the database to the previous installation state.

From the TME 10 's Desktop pull-down menu, select **Backup.**

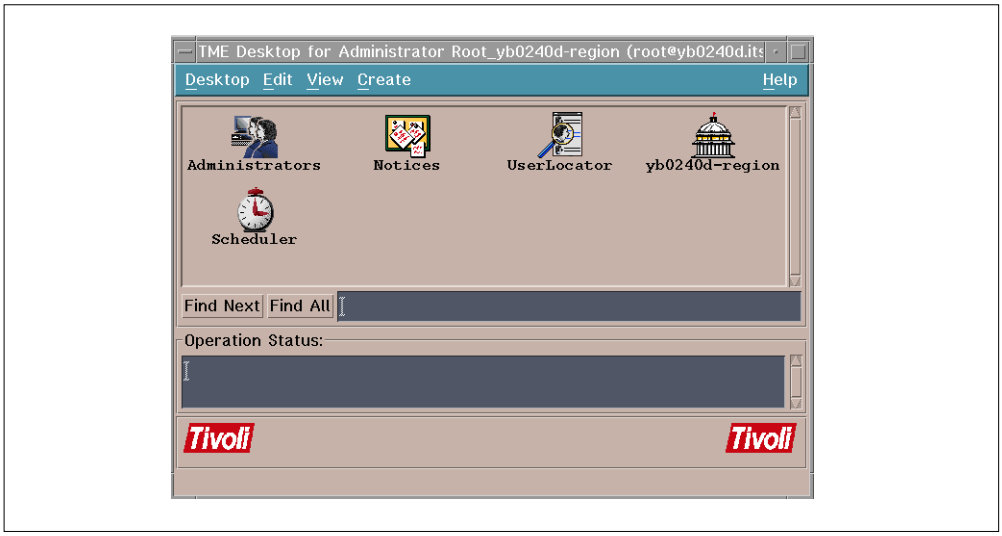


Figure 48. Our TME 10 Desktop

You will then get the following window:

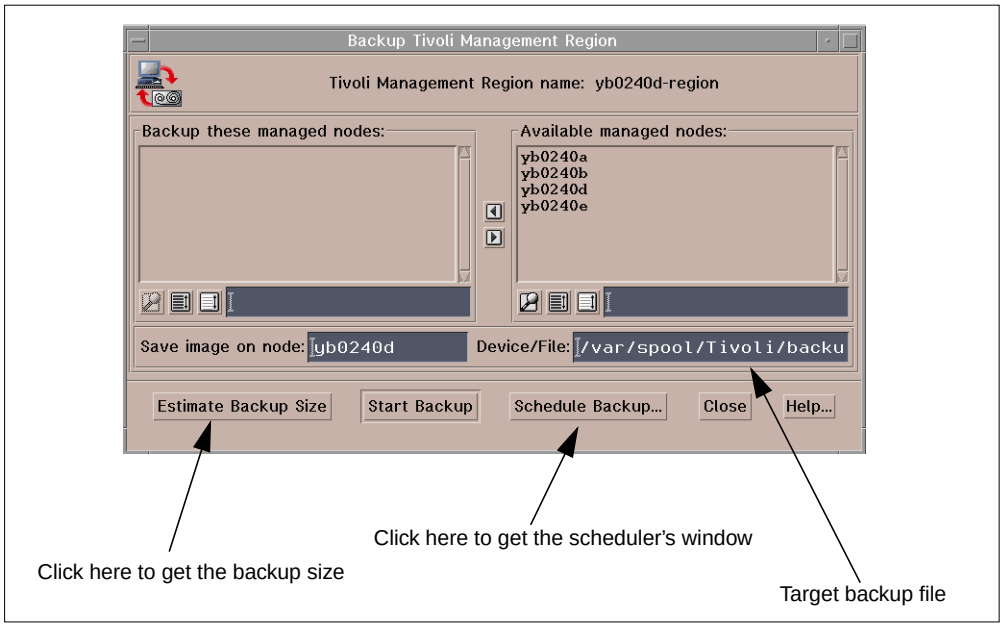


Figure 49. Backup Window

The Estimate Backup Size button determines the amount of disk space needed for the backup of the managed node that you select. Obviously, to back up the entire TME 10 region, you should select all the avalaible managed nodes. If you want to estimate the backup size of (for example) the TME 10 server, select it from the list and click the button. You will get the following window:

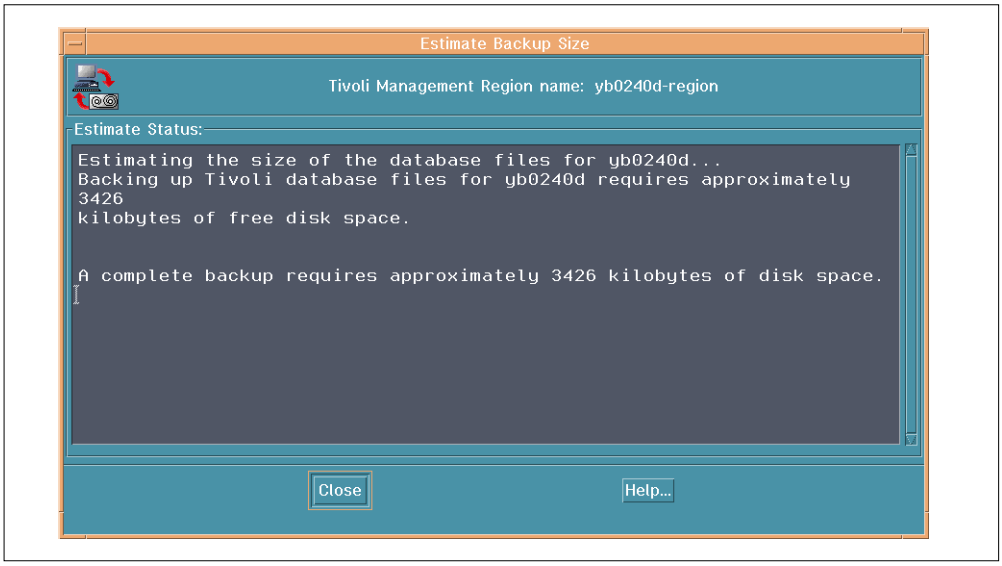


Figure 50. Disk Space Needed to Back Up the TME 10 Server

You might want to schedule the backup to occur during the night to avoid a supplementary workload of the machine. In this case click the **Schedule Backup** button and fill in the following window:

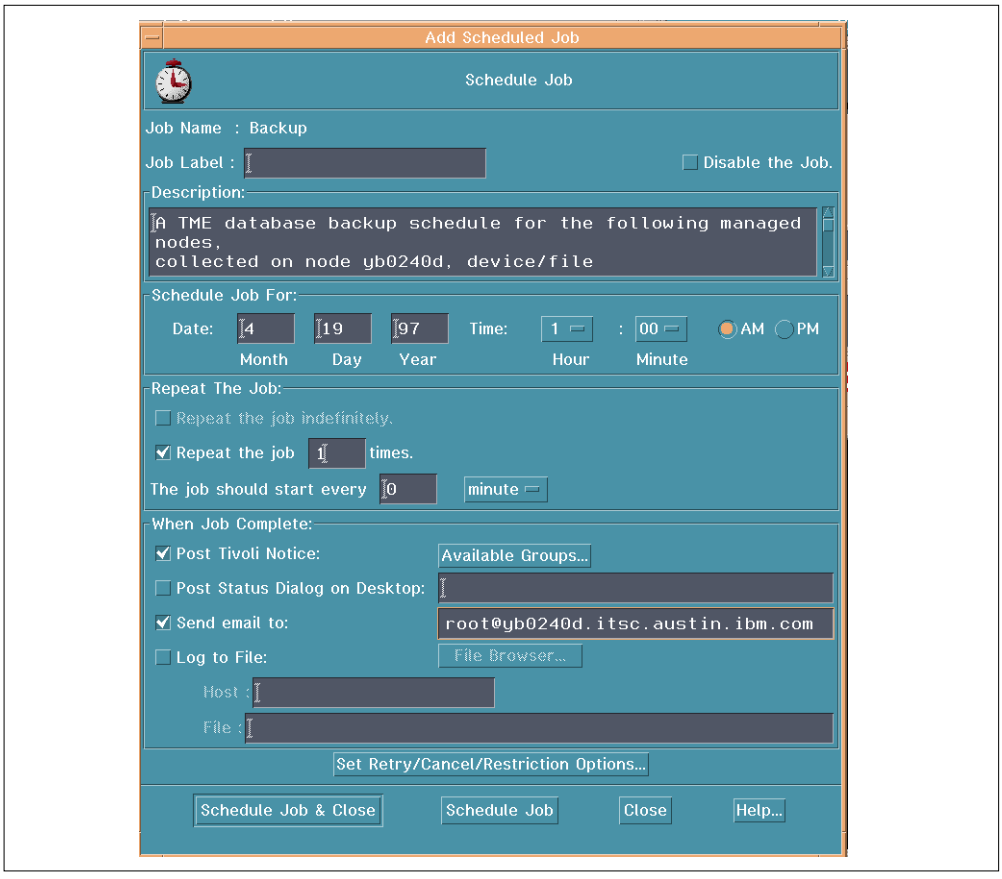


Figure 51. Scheduling a Backup

We scheduled the backup to occur on 1 a.m. on April 19 1997, to repeat the job one time if the first backup attempt was unsuccesfull, to post a notice for an administrative group, and to notify the operation to the root administrator of the TME 10 server.

By clicking **Start Backup**, you perform the backup operation of the selected managed node.

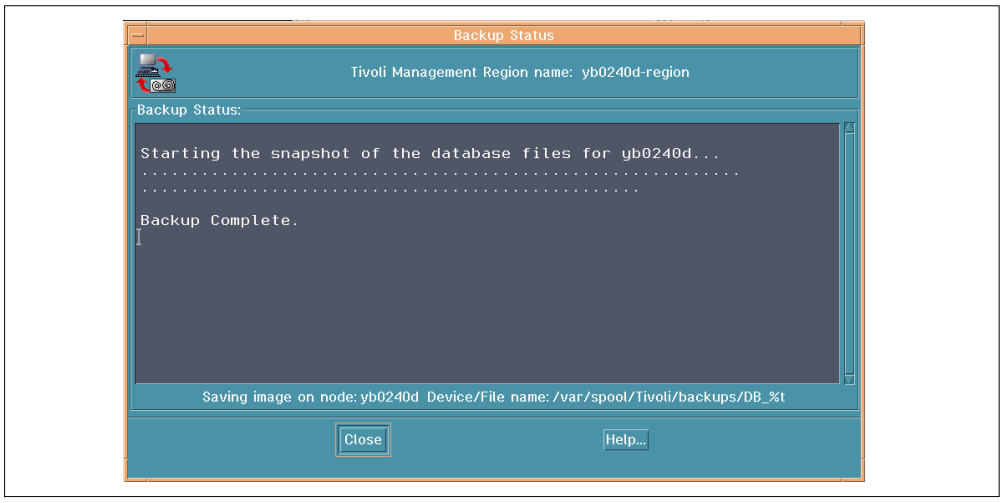


Figure 52. TME 10 Server Backup Window

5.3.7 Restoring Your Database

Once you have a backup of the TME 10 database, you will be able to restore it in a very simple way. For example, to restore the TME 10 database on the server, you have to type the following command:

```
$wbkupdb -r -d /var/spool/Tivoli/backups/DB_Apr18-1645 yb0240d
```

Where `/var/spool/Tivoli/backups/DB_Apr18-1645` is the backup file. The TME 10 Framework stores the backup file in the default directory, /var/spool/Tivoli/backups and names the specific file DB_<backup_date_and_hour>. The name of the managed node on which you want to restore the database is yb0240d.

5.4 Installing TME 10 User Administration

This chapter provides step-by-step installation instructions for installing TME 10 User Administration on the technical environment described ealier in this chapter. The first section discusses the TME 10 User Administration installation on the TMR server, on Managed Nodes and PC Managed Nodes. Once the installation is complete, we will guide you in creating some administrators and using some basic functions provided by TME 10 User Administration.

5.4.1 Installing TME 10 User Administration on UNIX and NT Managed Nodes

To be able to use the user administration functions provided by TME 10 User Administration, the product must be installed on each managed node.

Therefore, you must repeat these installation instructions for each Managed Node, including the TME server, that you plan to manage with TME 10 User Administration, or you can choose them all at once.

TME 10 User Administration has the following prerequisite on the TME 10 Framework:

- TME 10 Framework Version 3.1 Patch 3.1-TMP-0003

This patch is available on the TME 10 User Administration CD-ROM.

Use the following steps to install the TME 10 User Administration application from the TME desktop onto the Managed Nodes.

1. From the Tivoli desktop's *Desktop* pull-down menu, select **Install**; then **Install Patch...**
2. You may see an error about the media not being properly set; this is normal and will start the window that allows you to select the correct path to the TME 10 Framework Version 3.1 Patch 3.1-TMP-0003.
3. The Install Patch dialog should then appear as shown in Figure 53. Select the **TME 10 Framework Version 3.1 Patch 3.1-TMP-0003** from the Select Patch to Install scrolling list and the clients on which you wish to install the patch. You can click on the **Select Install Options...** button or the **Select Media...** button on this screen for more options.

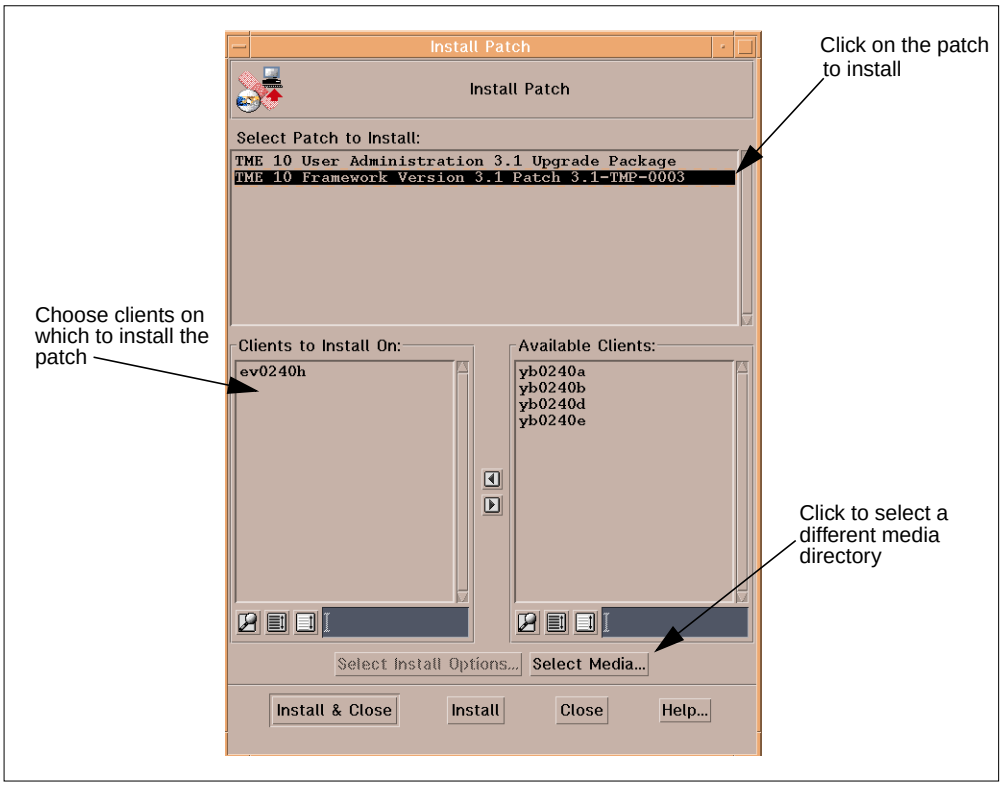


Figure 53. Patch Installation Window

Click on the **Install & Close** button to install the patch and close the installation window, or the **Install** button to install and keep the installation window open after completion.

4. The Patch Install dialog should then appear as shown in Figure 54. This window lists all of the software that will be installed. Click the **Continue Install** button to continue or the **Cancel** button to cancel. This is your last chance to cancel the installation of the patch.

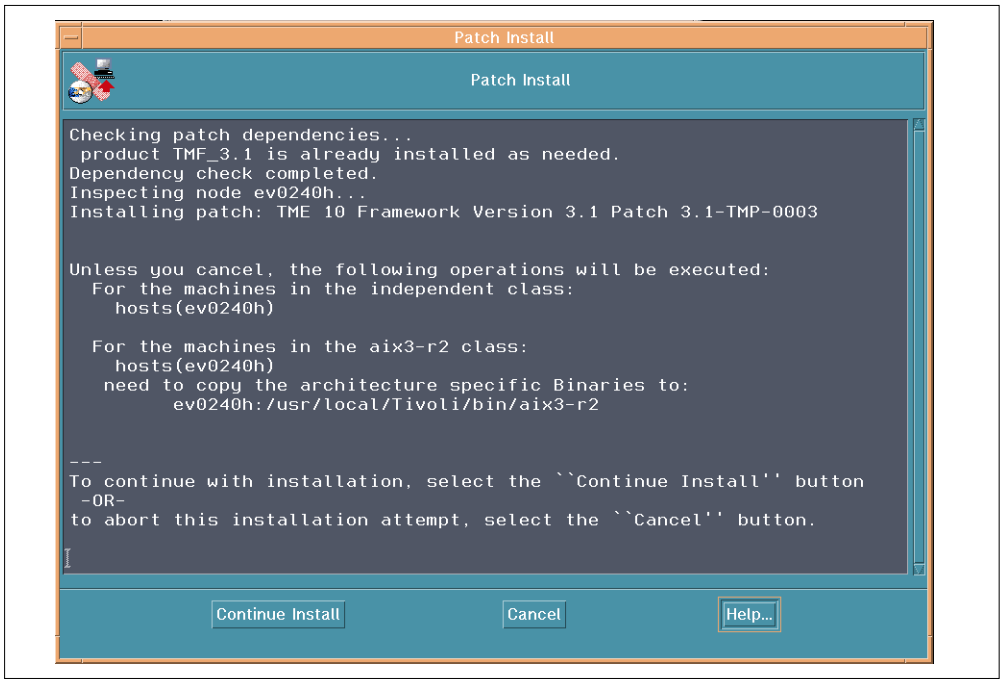


Figure 54. Patch Installation Confirmation Window

5. The window will then display the status of the product installation. Wait for the `Finished Patch Installation` message to appear.

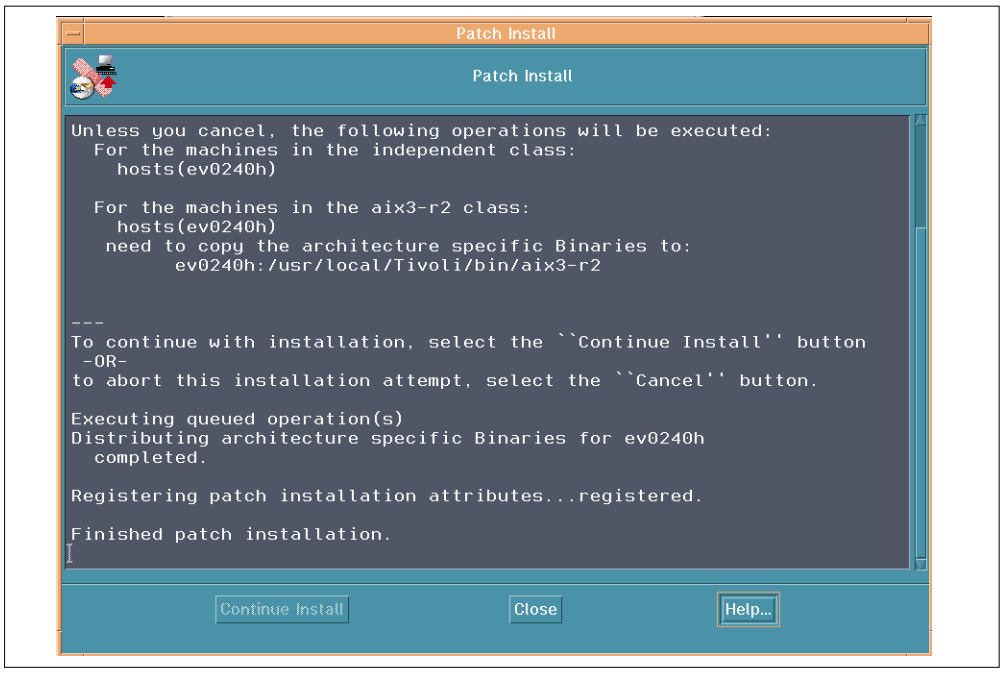


Figure 55. End of Patch Installation

It is then safe to click the **Close** button; the installation is complete.

6. From the Tivoli desktop's *Desktop* pull-down menu, select **Install**, then **Install Product...**
7. You may see an error about the media not being properly set; this is normal and will start the window that allows you to select the correct path to the TME 10 User Administration 3.1.
8. The Install Product dialog should then appear as shown in Figure 56. Select **TME 10 User Administration 3.1** from the Select Product to Install scrolling list, and select the clients on which you wish to install the patch. You can press the **Select Install Options...** button or the **Select Media...** button on this screen for more options.

Note about Installation

Besides the TME 10 User Administration 3.1 choice, you will see also the choice TME 10 User Administration 3.1 PC Filepack Utilities. This is used to install the User Administration product on a PC Managed Node. This version of TME 10 User Administration provides full support for Windows NT machines defined as Managed Nodes. You will have to select the TME 10 User Administration 3.1 PC Filepack Utilities only if you defined your Windows NT machines as a PC Managed Node or if you have to manage a NetWare server. Actually, you only need to install the PC Filepack Utilities on the TMR server. That is where you could then do the distribution from.

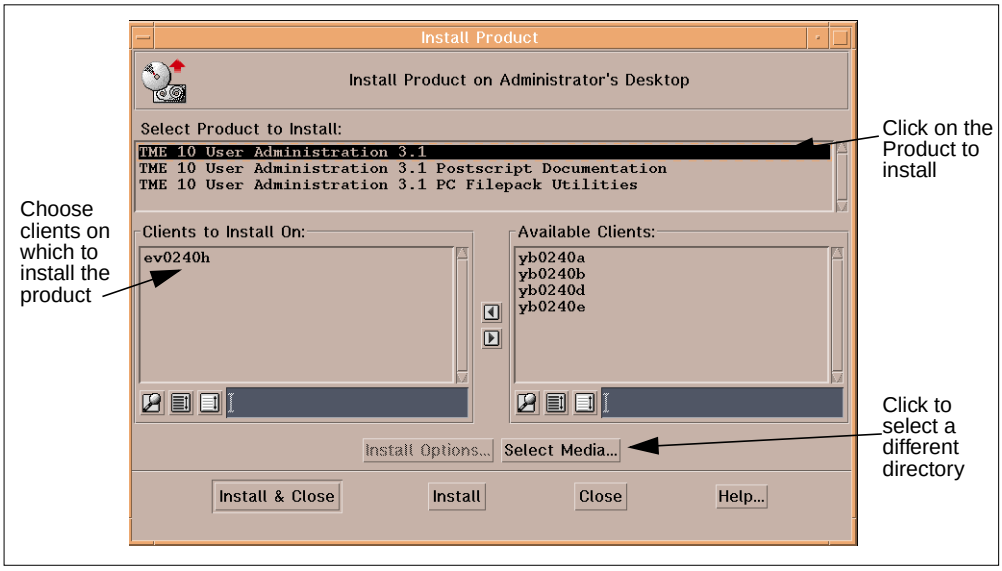


Figure 56. Product Installation Window

9. The Product Install dialog should then appear as shown in Figure 57. This window lists all of the software that will be installed. Click on the **Continue Install** button to continue or on the **Cancel** button to cancel. This is your last chance to cancel the installation of the product.

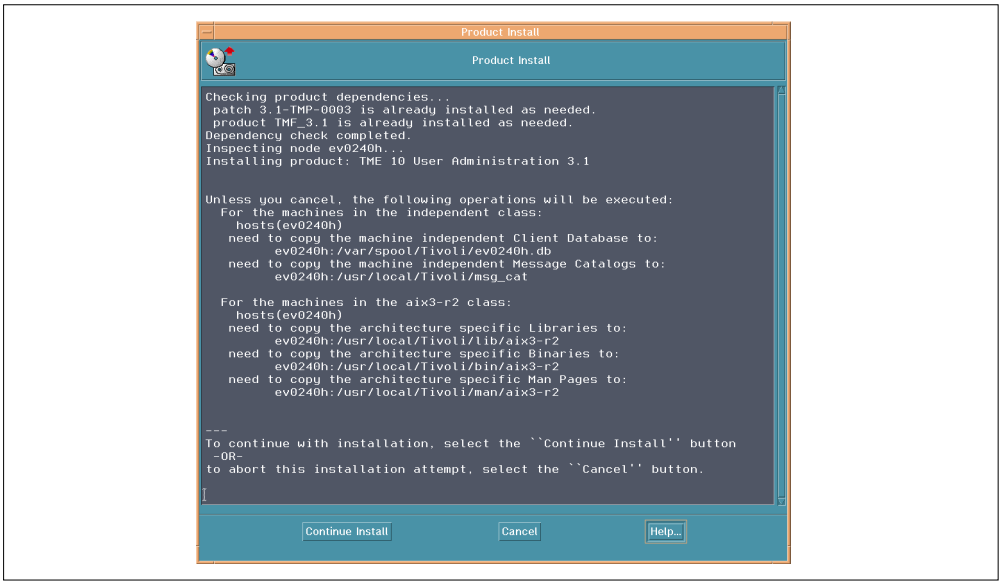


Figure 57. Product Install Dialog

The window will then display the status of the product installation. Wait for the `Finished Product Installation` message to appear. It is then safe to click the **Close** button; the installation is complete.

5.4.2 Installing TME 10 User Administration on a NetWare Managed Node

We can now install the TME 10 User Administration application on the PC Managed Node. The corresponding product comes on diskette with TME 10 User Administration. The installation can be performed by distributing the code to the PC Managed Node with TME 10 Software Distribution or by installing the code on a server-by-server basis using the installation diskette. In our case we install directly from the diskette.

Attention

When you are installing TME 10 User Administration on a NetWare server PC Managed Node from the installation diskette, you must run the installation on a Windows workstation able to access the NetWare server resources.

The following table provides the context and authorization role required for this task.

Table 13. Authorization Role for Installing User Administration

Activity	Context	Required Role
Installing TME 10 User Administration	TMR	**super** or **install_product**

Following are the steps to install TME 10 User administration on the NetWare PC Managed Node:

1. Run the setup.exe file located on the diskette and press **OK** to start the installation.
2. Press the **Next** button to display the **Select Target Machine Type** dialog.

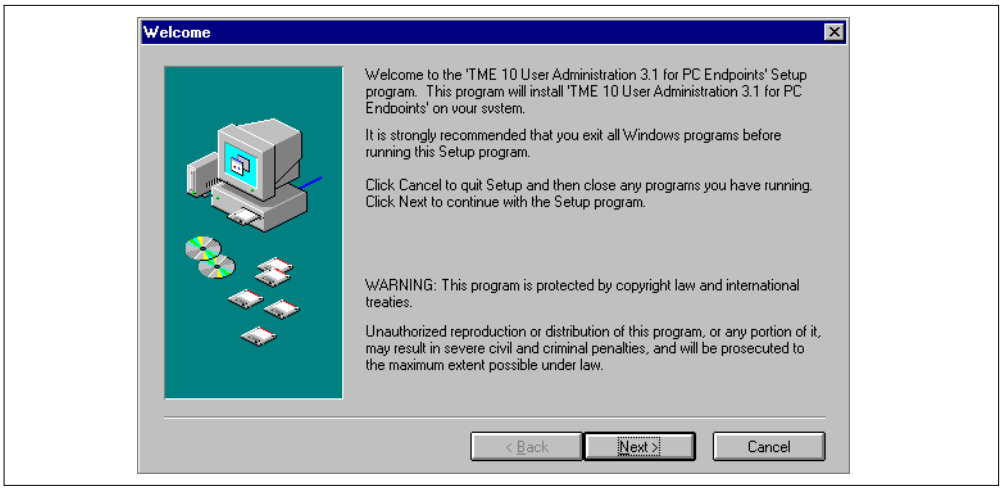


Figure 58. Welcome Installation Window

3. Select the system on which you want to install the product, **NetWare 4.X** in our example, and click on **Next**.

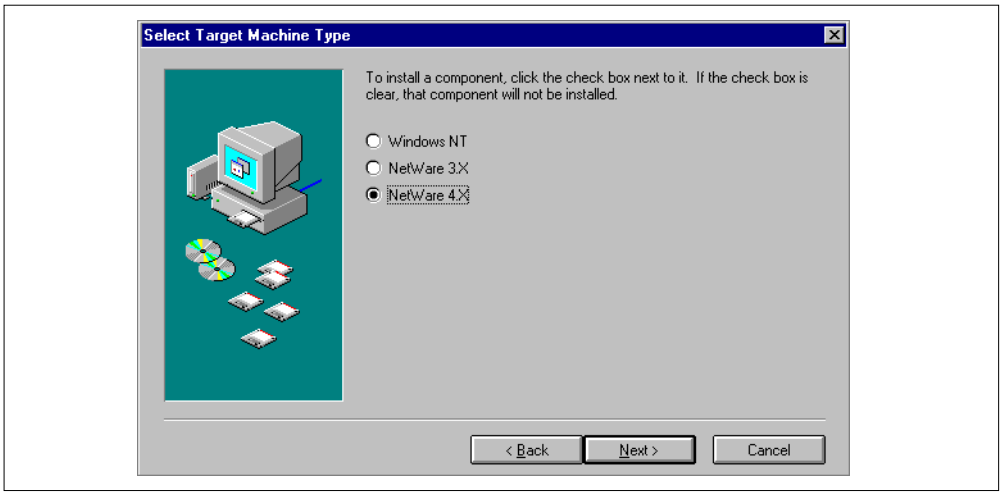


Figure 59. Selecting the Target Operating System

4. Select the destination directory in which to install the product and click on **Next**.

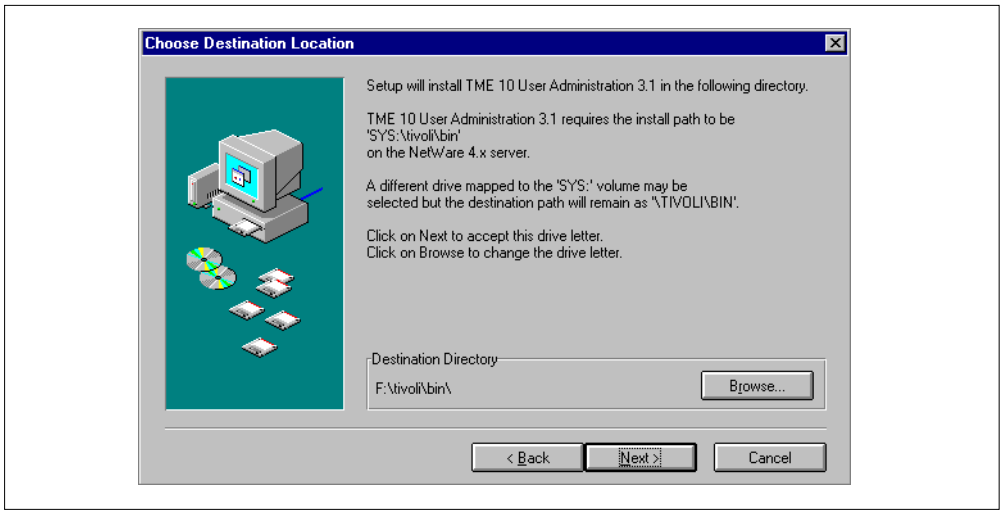


Figure 60. Specifying the Destination Directory

5. The following dialog is displayed when TME 10 User Administration is successfully installed. Then click on **OK**.

   Note: The User Administration code for a PC Managed Node must be in \tivoli\bin.

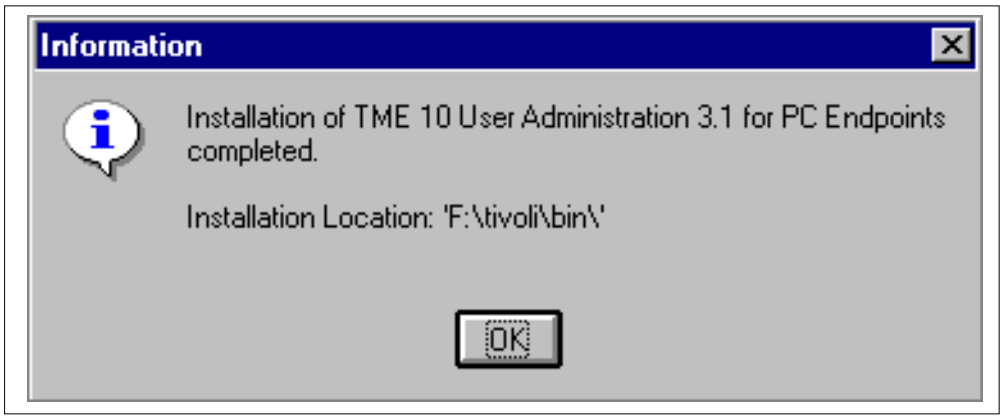


Figure 61. Installation Completed

5.4.2.1 Connecting to the NetWare PC Managed Node

If you are using NDS on NetWare 4.X, you need to run the `wsetnds` command to establish a connection between the TMR server and the NetWare PC Managed Node. This command allows the application to login to the NetWare NDS tree. This command must be run once. It does not need to be run every time you want to manage the PC Managed Node. You will need to run it again if you change the login or the password of the account used for connecting to the NetWare server (for example, user Admin). The account must have "Admin" privileges.

The command must be run for each NetWare NDS tree you manage. The `wsetnds` command is not applicable to NetWare 3.X because NetWare 3.X does not support NDS trees.

Following is the syntax of the `wsetnds` command:

```
wsetnds -l Admin -p password -c ITSO@PcManagedNode:yb0240c
```

where:

`-l Admin`	Specifies the login name of the account to use to login to NDS.
`-p password`	Specifies the login name of the account.
`@PcManagedNode:yb0240c`	Specifies the name of the NetWare PC Managed Node.

For more information on the `wsetnds` command, refer to *TME 10 User Administration User and Group Management Guide*.

You are now ready to manage users on the PC Managed Node.

5.4.3 Installing TME 10 GEM User Administration for OS/390

This section describes the installation of the User Administration product on the OS/390 system.

5.4.3.1 What is the Global Enterprise Manager?

The Global Enterprise Manager (GEM) product is intended to be a bridge between the OS/390 host environment and the distributed environment. It is built to facilitate systems and network management. The distributed environment could consist of UNIX, Windows NT, NetWare, OS/2, and other platforms.

There are several separately installable entities within the OS/390 side of GEM, the OS/390 Connection Service being one of them.

The OS/390 Connection Service administers security tasks across multiple platforms with a single action. It manages System Authorization Facility (SAF) compliant products such as RACF. SAF is the component in OS/390 which responds to standard SAF service calls. SAF will route these calls to any security manager that is coded to understand these SAF-compliant calls. By using the OS/390 Connection Service you can increase security through faster updates and consistent administration of policy while eliminating the need for administrators to log on to different systems.

The OS/390 Connection Service is the OS/390 component that responds to requests originating from the TME 10 oserv daemon running on the TME server or on a TME Management Station. It is implemented as an OS/390 address space and contains the TCP/IP protocol support to manage the communications link between the Transaction Program server (TPs) and TME 10.

In order to ensure that requests coming from the TME 10 server are from authorized users, the OS/390 Connection Service uses link encryption and authentication of incoming requests. Standard SAF services are used to process the requests.

Since the OS/390 Connection Service is supposed to be a bridge between the host environment and the distributed environment, there are products corresponding to it on the TME 10 side. These products are in addition to the TME 10 Framework:

- TME 10 GEM OS/390 Connection Service

- TME 10 GEM User Administration Service for OS/390

The TME 10 GEM OS/390 Connection Service enables you to send commands using TCP/IP communication to the OS/390 Connection Service (also called the Transaction Processing Server(TPS) on the host side. The TME 10 GEM User Administration Service is used to manage users in a distributed environment including the host environment with RACF or equivalent products.

TME 10 User Administration in a larger picture provides single-action management of user accounts on multiple platforms. Single-action in this context means being able to process management operations that span multiple platforms in a single step.

5.4.3.2 Prerequisites

The User Administration Service and the OS/390 Connection Service require the following:

- For the OS/390 Server:
  - OS/390 Release 3 with Authorized Program Analysis Report (APAR) OW23446 applied
  - OS/390 Release 3 Security Server with APAR OW23445 applied
  - Transmission Control Protocol/Internet Protocol (TCP/IP) for Multiple Virtual Storage (MVS), Version 3 Release 1 or later
- For the system running the TME Framework:
  - TME 10 Framework Version 3.1 with Service Pack 1 and Patch 3.1-TMP-0003
  - TME 10 User Administration 3.1 with Service Patch 01
  - A Perl Interpreter

5.4.3.3 Installing the TP Server on an OS/390 Server

This chapter describes how to install the TP server on an OS/390 server.

1. Make sure that your system fulfills all the installation requirements and considerations for the OS/390 Connection Service as described in the *Program Directory for TME 10 Global Enterprise Manager*, Chapter 5.
2. Install the OS/390 Connection Service using the SMP/E `RECEIVE`, `APPLY`, and `ACCEPT` commands. Sample jobs are provided on the distribution tape to help you install the code. Details about the job names and other information can be found in the *Program Directory for TME 10 Global Enterprise Manager*, Chapter 7.
3. Give the TP Server load libraries necessary authorization using either the SYS1.PARMLIB member IEAAPFxx or PROGxx.
   - If you are using an IEAAPFxx member, add the following:

     ```
     yourqual.SIHSMOD1    volser
     ```

   - If you are using a PROGxx member, add the following:

     ```
     APF  ADD,DSNAME(yourqual.SIHSMOD1),VOLUME(volser)
     ```

5.4.3.4 Customizing the TP Server

The OS/390 Connection Service executes as a started task and uses TCP/IP services. You can customize this TP server using the sample initialization statements as follows:

1. Copy the sample Job Control Language (JCL) from member IHSTTPS in yourqual.SIHSSMP1 to member TPS in SYS1.PROCLIB. Edit the JCL to conform with your data set names for the SIHSMOD1 library, the LE run-time library and the TCP/IP profile data set. Sample JCL for the TPS member in SYS1.PROCLIB follows:

```
//TPS     PROC M=00,               /* IHSTPMxx in SYS1.PARMLIB */
//             P='NOFOLDMSG'       /* Additional server parms */
//TPS     EXEC PGM=IHSTTPS,REGION=32M,TIME=NOLIMIT,
//            PARM='M(&M),&P'
//STEPLIB DD DSN=TME10GEM.V1R1M0.SIHSMOD1,DISP=SHR
//        DD DSN=CEE.SCEERUN,DISP=SHR
//SYSTCPD DD DSN=TCPIP.DATA.TME10,DISP=SHR
```

2. Copy the OS/390 Connection Service initialization statements from member IHSTPM00 in yourqual.SIHSSMP1 to member IHSTPM00 in SYS1.PARMLIB . If necessary, change the statements as described in the comments included with the member. For a full description of the various options, refer to *Global Enterprise Manager: User's Guide.* Sample initialization statements in SYS1.PARMLIB(IHSTPM00) follow:

```
OPTIONS TRSIZE(128)      /* Set internal trace buffer to 128K       */
TCPIP ENCRYPT(DES)       /* Encrypt data using DES                  */
TCPIP PORT(5001)         /* The connection port number can be       */
                         /* specified here.                         */
LOG START(NO)            /* Do not start logging at initialization  */
SERVICE                  /* Use system defined routines             */
```

3. Optionally, update your TCP/IP profile data set to reserve a port for the OS/390 Connection Service using the PORT initialization statement. The server name specified on the PORT statement should be the same as the procedure name used to start the TP server; TPS in our example. See the *TCP/IP for MVS Customization and Administration Guide* for syntax and usage of the PORT statement. For our sample the statement should read:

```
PORT 5001 TCP TPS  ;OS/390 Connection Service;
```

5.4.3.5 Configuring the OS/390 Environment for TME 10 GEM

Following are the steps required to configure the OS/390 environment for TME 10 GEM.

1. Defining the RACF User ID for the TMR Server (TME 10 side)

   You need to define a RACF user ID that will be assigned to, and associated with the TMR server. For example, if the TMR server user ID is TMRSRVR, you would issue the following RACF command:

```
ADDUSER TMRSRVR
```

   Please note that the above statement only serves to show a way of adding a user. In real life you will have to add information about profile ownership, default group and so on.

2. Enabling the Use of RACF PassTickets

The RACF Secured Signon function, which provides an alternative to the RACF password called a PassTicket, allows workstations and client machines to communicate with a server without using a RACF password. Administrators can use the PassTicket to authenticate their user IDs and log on to computer systems that contain RACF. You need to perform the following tasks to set up Secured Signon communications between OS/390 and TME 10.

3. Activate the PassTicket Data (PTKTDATA) Class

   Before you can use the Secure Signon function, you must activate the PTKTDATA class. The PTKTDATA class is the class to which all profiles that contain PassTicket information are defined. To activate the class and the function, enter the following RACF command:

   ```
   SETROPTS CLASSACT(PTKTDATA)
   ```

4. Defining a Profile in the PTKTDATA Class

   You use a PassTicket to gain access to an application. The PassTicket is generated using a secret PassTicket application key. The TMR server secret PassTicket application key is stored in the RACF PTKTDATA class in a profile named TMEADMNA. This secret PassTicket application key (keymasked) must be the same as the 16-hex-digit PassTicket key that was specified in TME 10. To define the secret PassTicket application key in the TMEADMNA profile, enter the following command:

   ```
   RDEFINE PTKTDATA TMEADMNA SSIGN(keymasked) UACC(READ)
   ```

   Activate SETROPTS RACLIST processing by:

   ```
   SETROPTS RACLIST(PTKTDATA) REFRESH
   ```

5. Mapping TME 10 Administrator User IDs to RACF User IDs

   The RACF TMEADMIN class is used to map TME administrators' user IDs and the Tivoli Management Region (TMR) name to RACF user IDs. The RACF user ID will be associated with the TME administrator's user ID that was defined at the TME workstation. Associating a TME administrator user ID with a unique RACF user ID allows accountability so that an administrative action may be tracked to the administrator issuing the request. We recommend that each TME administrator user ID maps to a unique RACF user ID.

   After the administrator's user ID is defined to RACF, you must define a profile in the IBM-supplied resource class TMEADMIN for each TME 10 administrator that is able to perform RACF user administration.

   Activate the TMEADMIN class before you define profiles by RACF command:

   ```
   SETROPTS CLASSACT(TMEADMIN)
   ```

6. Defining profiles to the TMEADMIN Class

   Define a profile in the TMEADMIN class for each TME administrator who will be performing RACF user administration functions. The profile name in the RACF TMEADMIN class is the TME administrator's string name. The string name is a combination of the TME administrator's user ID (a UNIX login name) and the TMR name. The format of the string name is:

   ```
   unix-login-name@TMR-name
   ```

   For example, a TME administrator with a UNIX login name of *hilding* at the TMR of *yb0240e* has the string name of *hilding@yb0240e*.

The APPLDATA field of this profile contains the RACF user ID. To define a general resource profile in the TMEADMIN class to associate the TME administrator *hilding* in the TMR of *yb0240e* with a RACF user ID of *HILDING*, enter:

```
RDEFINE TMEADMIN hilding@yb0240e APPLDATA('HILDING')
```

As you will see later on, you may have to expand the TMR name to a fully qualified name in some instances. The command would the look like this:

```
RDEFINE TMEADMIN hilding@yb0240e.xxxx.yyyy.zzzzz.com APPLDATA('HILDING')
```

5.4.3.6 Start Using the TP Server

You will find below how to start or stop the TP Server on the OS/390.

1. Starting the TP Server

   The OS/390 `START (S)` command is used to start the TP server. The `START` command initializes the server and establishes the communication environment. To start the TP server named TPS, enter:

   ```
   /S TPS
   ```

   As a result, you would see messages like the ones below:

   ```
   $HASP100  TPS  on STCINRDR
   IEF695I   START TPS with Jobname TPS is assigned to user TPS, Group STCGRP
   $HASP373  TPS-STARTED-TIME=xx.xx.xx
   IHST0501I TP server 1.1.0 TPS started.
   IHST0539I Member IHSTPM00 found in dataset SYS1.PARMLIB.
   IHST0508I TP server TPS ready for connections using port 5001.
   ```

   The TP Server for the OS/390 environment is now ready to communicate with the TMR server in the TME 10 environment.

2. Stopping the TP Server

   The OS/390 `STOP (P)` command is used to stop the TP Server. The TP Server will attempt to halt all connections prior to shutting down. The following command is an example of how to stop the TP Server:

   ```
   /P TPS
   ```

3. Other Commands for the TP Server

   There are OS/390 `MODIFY (F)` commands available for `DISPLAY`, `KILL`, `LOG`, `LOGOUT`, `MAXUSER` and `DEBUG` of the TP Server.

5.4.3.7 Hints and Tips for the OS/390 Connection Service (OS/390 Side)

The GEM User's Guide lists all the necessary steps to take to get the TP Server installed and operating on the OS/390 server and we have gone trough them in the previous sections.

There are a few things to look out for, however. First of all, it must be stressed once again that the RACF commands shown in the book are just examples. This means that there are no provisions made in these commands to cater for things like profile owner, default group or installation data. You should, of course, adhere to your normal policy in these matters and define resource names to your own standards where this is possible. Some resource names are fixed and will, therefore, have to be named accordingly.

Since the TP server runs in its own address space, you can use, for example, Spool Display and Search Facility (SDSF) to peek at what is going on in there.

Among other things you will see messages like these being produced by the TP Server:

```
ICH70001I TMRSRVR  LAST ACCESS AT 13:01:36 ON FRIDAY, APRIL 11, 1997
ICH70001I HILDING  LAST ACCESS AT 13:01:36 ON FRIDAY, APRIL 11, 1997
ICH70001I TMRSRVR  LAST ACCESS AT 13:04:08 ON FRIDAY, APRIL 11, 1997
ICH70001I HILDING  LAST ACCESS AT 13:04:08 ON FRIDAY, APRIL 11, 1997
ICH70001I TMRSRVR  LAST ACCESS AT 13:04:27 ON FRIDAY, APRIL 11, 1997
ICH70001I HILDING  LAST ACCESS AT 13:04:28 ON FRIDAY, APRIL 11, 1997
ICH70001I TMRSRVR  LAST ACCESS AT 13:05:10 ON FRIDAY, APRIL 11, 1997
ICH70001I HILDING  LAST ACCESS AT 13:05:20 ON FRIDAY, APRIL 11, 1997
```

These messages tell you that commands from the TME 10 side have successfully been received from the TMR (TMRSRVR) and that the administrator named HILDING has originated the commands.

The TME administrators who will be performing RACF user administration have all to be defined in the TMEADMIN class. The profile names have a general format of:

```
unix-login-name@TMR-name
```

The UNIX login name is that of the TME administrator, and the TMR name is the name of the TME Management Region from where he is working. We had defined profiles of the format HILDING@YB0240E, but found that this did not work. The following message in the security log gave us the explanation:

```
ICH70001I TMRSRVR  LAST ACCESS AT 12:57:58 ON FRIDAY, APRIL 11, 1997
IHST0128I (TMRSRVR) Unable to map administrator userid "HILDING@YB0240
E.XXXX.YYYYYY.ZZZ.COM" to host userid.
```

What the message told us was that the TMR host name could not be properly resolved and that we had to enter the fully qualified name in the profile, that is to say:

```
HILDING@YB0240E.ITSC.AUSTIN.IBM.COM (in our example)
```

This being done, things started working just fine. We did detect another slight problem with using UNIX login names. We tried using a name of the format adm-RACF and found it could not be resolved properly by the TP Server. The message looks exactly right, but it seems that the hyphen does not compare properly as represented in UNIX and in OS/390, respectively. The obvious suggestion is to stay away from such login names.

There is another lesson to be learned: UNIX login names are case sensitive such that "HILDING" and "hilding" are two separate users in UNIX. In OS/390 these users would be treated as one and the same.Take note of this and avoid defining login names like these, at least for users who have to work in mixed environments.

5.4.3.8 TP Server Not Responding

We happened to try out sending commands from the TMR when the RACF address space was not started. The result showed up in the reponse window as:

```
Returned output for  Run Command
SAF Return Code: 8 RACF Return Code: c RACF Reason Code: 4
```

5.4.4 Installing the TME 10 GEM User Administration for OS/390 Users

This section gives some hints and tips useful for installing TME 10 GEM User Administration for OS/390 users on the workstation side.

5.4.4.1 Hints and Tips

If you do not have a Perl interpreter installed on your system, you can find one at the UCLA FTPsite with the following URL:

`ftp://aixpdslib.seas.ucla.edu/pub/perl/RISC/`

The above site is for the AIX code. If you have another platform, you will have to find a corresponding site.

It is recommended that you install the TME Framework and the User Administration products along with their service and patches plus the Perl Interpreter and then take a full backup of the Tivoli directories before installing the TME 10 GEM OS/390 Connection Service and the TME 10 GEM User Administration for OS/390 Users.

You should do this in order to be able to restore the Tivoli products if you encounter installation errors when installing the GEM products onto your platform. You will also need this backup if you need to reinstall the GEM products because of a new version, a patch or similar reason. Failure to make a backup before installing the GEM products can result in your having to reinstall all the products again on the server as well as all the clients.

Figure 62 below shows you a sample UNIX script to use to back up your Tivoli installation. If you are accustomed to using TME, you probably have built your own scripts adapted to your installation standards.

```
tar -cvf - /usr/local/Tivoli | compress > /Tivoli_backup/usr.Z
tar -cvf - /var/spool/Tivoli | compress > /Tivoli_backup/var.Z
```

Figure 62. Sample Script to Back Up Tivoli Directories

Figure 63 below is an example of a script you can use to restore your previous Tivoli installation.

```
rm -rf /usr/local/Tivoli
rm -rf /var/spool/Tivoli
uncompress < /Tivoli_backup/usr.Z | tar -xvf -
uncompress < /Tivoli_backup/var.Z | tar -xvf -
```

Figure 63. Sample Script to Restore the Tivoli Directories

Once your installation is backed up, you can start installing from the Tivoli desktop, TME 10 GEM Connection Service and TME 10 GEM User Administration for OS/390 Users.

5.4.5 Setting Up the OS/390 Connection

We followed the steps in the *TME 10 Global Enterprise Manager User Administration for OS/390 User's Guide* to set up and test our OS/390 Connection from the TME 10 server. The OS/390 side and the TME 10 side should be

customized in concert so that you are in agreement over the IP address, the IP port and the user IDs to be defined in OS/390 as well as in the TMR server. The manual to use for the OS/390 side of things is the *Global Enterprise Manager User's Guide* (GC31-8474).

Table 14. Information Necessary for Setting Up the OS/390 Connection

What Resource	Where Used	Source of Information
Policy region name	Add OS/390 Connection	Naming policy
Server name	Add OS/390 Connection	TMR Admin
IP address of host	OS/390 Connection properties	TCPIP profile
TP Server port	OS/390 Connection properties	SYS1.PARMLIB (IHSTPMxx)
Connection User ID	OS/390 Connection properties	RACF Admin
PassTicket Seed	OS/390 Connection properties	RACF Admin

We did not have any major problems with the definition of the OS/390 Connection on the TME side of things. We found, however, that when you fill in the "OS/390 Hostname" field, you should maybe use the IP address instead of the name if you are not sure that your name server will be able to resolve the name. Failing to resolve the name into an IP address will produce messages that are not easily understood by a beginner.

Having created and defined the properties of the OS/390 connection, you have to subscribe it to the profile manager from which you plan to manage RACF user accounts. Having done this, you can now start distributing RACF user accounts to an OS/390 server.

Since you can run most RACF commands from an OS/390 Connection, we used this facility to test that we had actually defined everything properly. The first few tests gave negative results, but soon enough, we remembered that the use of PassTickets requires the time in participating hosts to be set with an accuracy of about five minutes.

If the hosts are in different time zones they have to have the proper time zone set that they agree on the Universal Coordinated Time (UCT, used to be GMT and still is displayed that way). On a UNIX machine you can display the time with the `date -u` command; in OS/390 you use the `d t` command. These things being straightened out, we soon had our commands send us back just the output we asked for.

5.5 Creating Administrators

A TME administrator is someone who has been given authorization to perform management tasks in the TME. The TME Administrator facility provides a senior administrator the ability to create other administrator accounts and assign them the authority to perform tasks. Then, each administrator has his or her own TME desktop that reflects the access and control he or she has been given.

5.5.1 Authorization Roles

A major concept in TME security is that of *authorization roles*. Authorization roles are predefined names for sets of management task abilities. These roles are

discrete, not hierarchical, meaning that each role has specific functions it can perform, and these functions cannot be performed by any of the other roles. The role or roles given to an administrator will define what that administrator can do to a particular set of resources.

Following is a list of the TME authorization roles and their meanings:

- ***super*** – Allows the administrator to configure the TME environment. Example: Connecting and disconnecting TMRs
- ***senior*** – Allows the administrator to create and define all of the TME resources. Example: Creating a new policy region
- ***admin*** – Allows the administrator to perform day-to-day operation, configuration, and policy tasks. Example: Distributing a set of files to TME clients
- ***user*** – Allows read-only access to the TME. This role is required to run the graphical desktop. Example: Displaying configuration of a client machine
- ***backup*** – Allows the administrator to backup the TME databases
- ***restore*** – Allows the administrator to restore TME databases
- ***install_product*** – Allows the administrator to install applications into the local TMR
- ***install_client*** – Allows the administrator to install managed nodes within policy regions that support the managed node resource type
- ***Query_edit*** – Allows the administrator to edit existing queries within a query library
- ***Query_execute*** – Allows the administrator to perform queries using the query facility
- ***Query_view*** – Allows the administrator to view query libraries and queries defined in the query facility

These authorization roles can be delegated for the entire TMR and also for individual resources. Most often, roles are delegated specifically for policy regions. For example, an administrator could be given a senior authorization role in one specific policy region so that he/she could make various changes to that specific group of resources. The same administrator could be given user authorization for the rest of the TMR so that he/she would only be able to view TME configuration, but not make any changes.

To be able to perform user or group management with the TME 10 User Administration product you have to have one or more of the following roles:

- ***senior***
- ***admin***
- ***user***

Before defining administrators, you have to know which roles are required to perform a given operation on users and groups. The following table shows the

role and the context in which you need it in order to perform these operations. Then we show how to apply these rules to our scenario.

Table 15. Roles Required for User and Group Management Operations

Required Role	Context	Activity
senior in policy region	Profile manager	Cloning user or group profiles Creating user or group profiles Deleting user or group profiles
senior in policy region	User or group profile	Editing user or group default policies Editing user or group validation policies
admin in policy region	User or group profile	Copying user or group records between profiles Creating user or group account records Deleting user or group account records Synchronizing the user or group profile database with system files
admin in profile manager policy region -----AND----- **admin** in profile subscriber region	User or group profile or profile manager	Distributing user or group profiles to subscribers
admin in policy region	User or group profile	Editing multiple user or group account records Editing user or group account records Populating a user or group profile
admin in policy region	User or group profile or profile manager	Retrieving subscriptions copies of user or group profiles
admin in policy region	User or group profile	Validating user or group records against profile policy
user in policy region	User or group profile	Finding a record in a user or group profile Sorting and displaying the attributes of user or group records Sorting user or group records Viewing user or group account records

5.5.2 Setting Up an Administrator

The *Administrator* resource icon on the desktop has two options on its pop-up menu:

- Open...: this option shows you the administrators already created. See Figure 64.

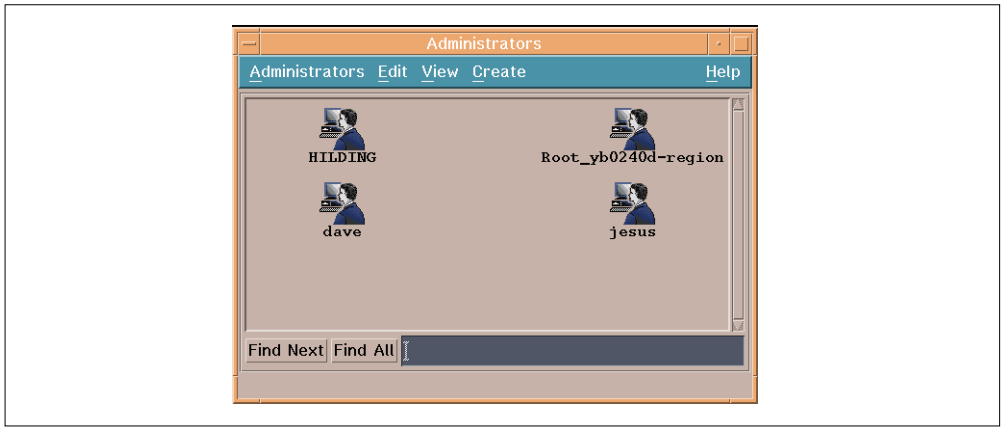


Figure 64. Administrators Previously Created

- Create Administrator...: If you want to create a new administrator, from this window, select **Create Administrator...**. The following window comes up:

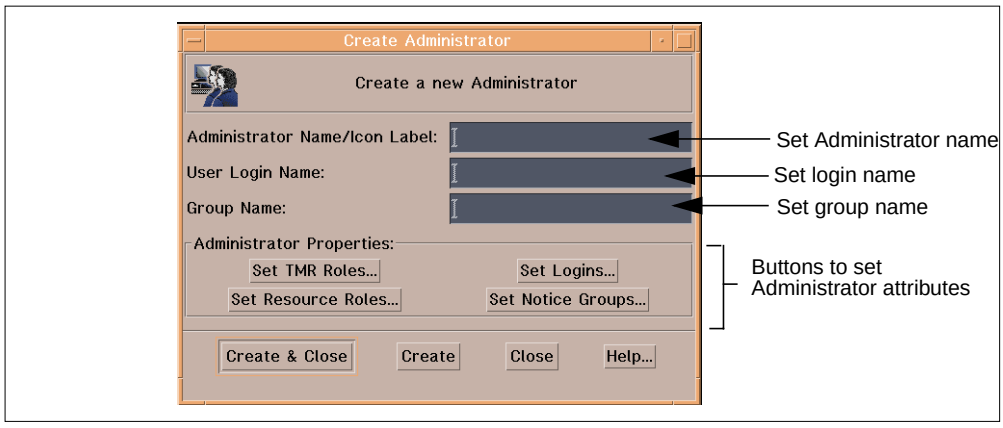


Figure 65. Create Administrator Window

- *Administrator Name*: The administrator's name inside the TME. The newly created administrator will be labeled with this name in the administrator collection.
- *Login and group name*: Each administrator must have a valid UNIX or Windows NT user and group name on every system they are going to work on (start the TME desktop).
- *TMR Roles* – A TMR role provides the assigned authorization level to *all* resources in the TMR. For example, if an administrator has a senior role in the TMR, this administrator has the senior role over every resource in that TMR. TMR roles should be assigned with great care.
- *Resource Roles* – Authorization roles are given out here on a per resource basis. For example, if an administrator has been given the *admin* role for the TMR as a whole, you could give him or her the *senior* role for a specific policy region by using the **Set Resource Roles...** option.
- *Logins* – You must define where the administrator will be logged in when starting the TME desktop or running commands. You can define numerous logins for the same administrator.

Hint

When creating an administrator, TME 10 does not create the corresponding user on the managed node that will be used by that administrator. You need to create the user ID separately. We also recommend that you edit the .profile of this user to automatically set the TME environment.

- *Notice Groups* – You must also define which notice groups administrators will be able to access.

In the following example, we create a new administrator who can create and delete user and group profiles and distribute them to all the AIX machines of our lab. This new administrator will be able to work from yb0240e (AIX V4.1.5 Managed Node) and will be assigned to the user name *marco,* already defined on this machine, belonging to the AIX primary group *staff.*

1. In the Create Administrator dialog, fill in the **Administrator Name**, **User Login Name** and **Group Name** fields, as shown in Figure 66.

Figure 66. Creating a New Administrator

2. Click on the **Set TMR Roles...** button and select the roles **admin** and **senior** from the list of the available roles (roles required to perform the operations, see Table 15 on page 126)**.**

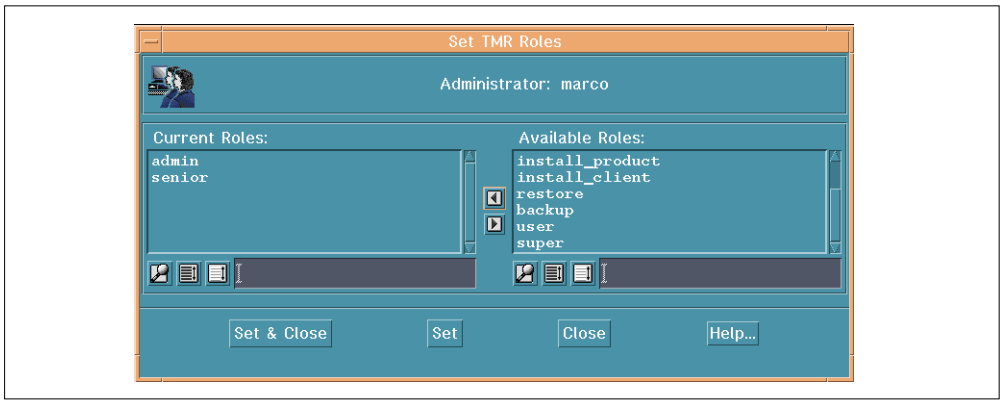


Figure 67. Setting the TMR Roles

3. Click on the **Set & Close** button**.** Figure 66 on page 128 will appear again.

4. Click on the **Set Logins** button and enter the login name in the *Add Login Name* field as:

   `<login name>@<host name>`

   In our example: `marco@yb0240e.itsc.austin.ibm.com`

   After entering the login name, click on **Enter**. The login name will be added to the *Current Login Names* list, as shown in the following figure. Check carefully that the login you specify is really corresponding to a defined user on a given machine. TME 10 will not let you define an administrator without specifying a valid Login Name.

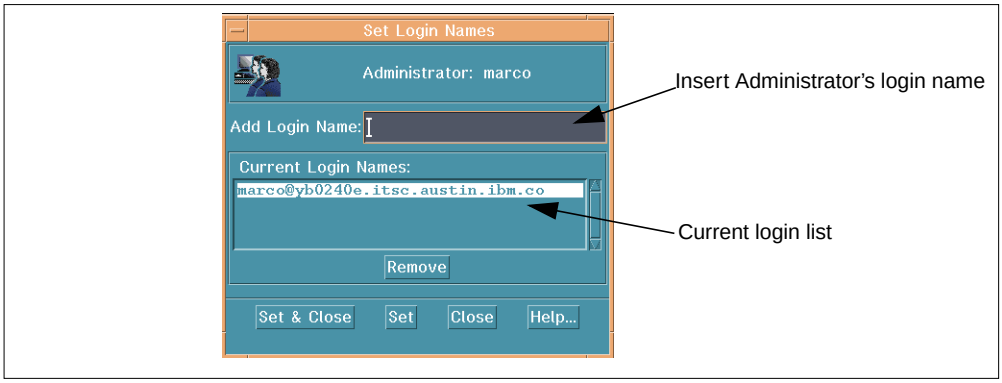


Figure 68. Setting a Login Name

   Click on the **Set & Close** button**.** The window in Figure 66 on page 128 will appear again.

5. Click on the **Set Notice Groups** button and select the notice groups the new administrator will have access to. In our example we selected *Group Management* and *User Management.*

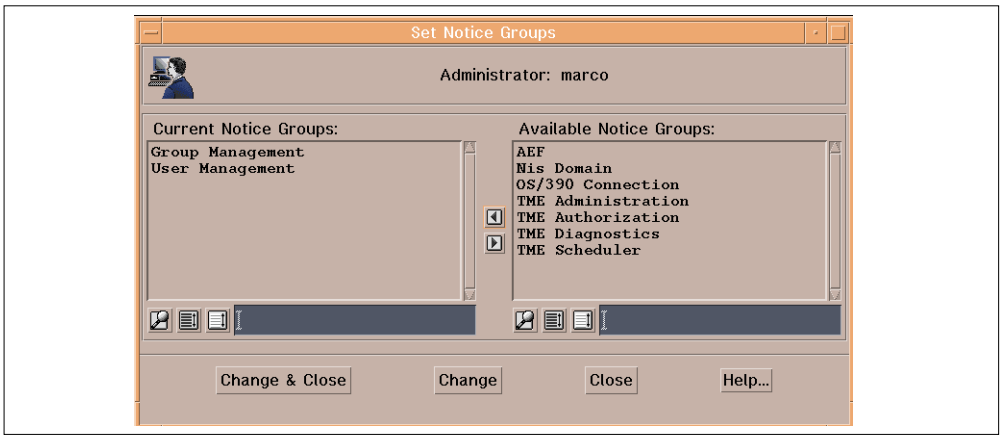


Figure 69. Setting Notice Groups

   Click on the **Change & Close** button to confirm your choices. The window in Figure 66 on page 128 will appear again.

6. Click on the **Create & Close** button to have your new administrator added to the existing administrator's list, as shown in Figure 70.

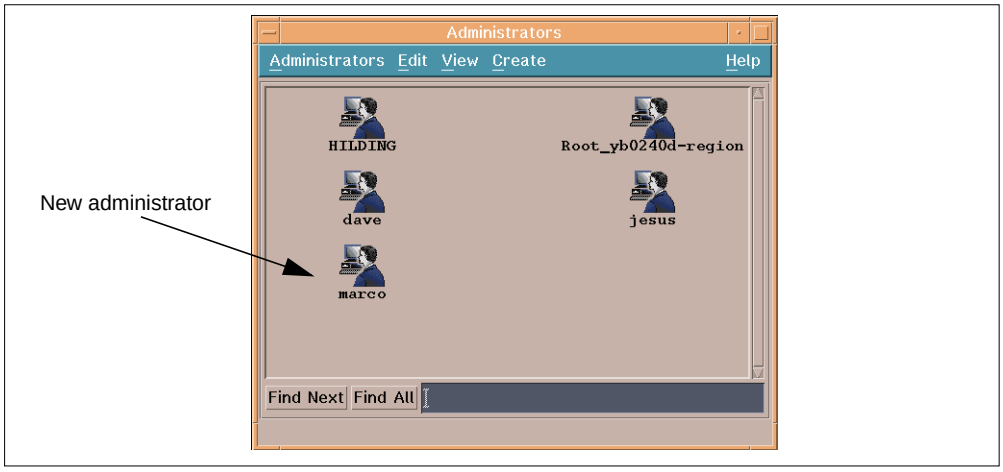


Figure 70. List of Administrators

The administrator's icon has its own pop-up menu that allows you to modify any of the information previously configured for that administrator.

7. The next required step is to populate marco's desktop. Double-click on the icon *marco.* The following window comes up.

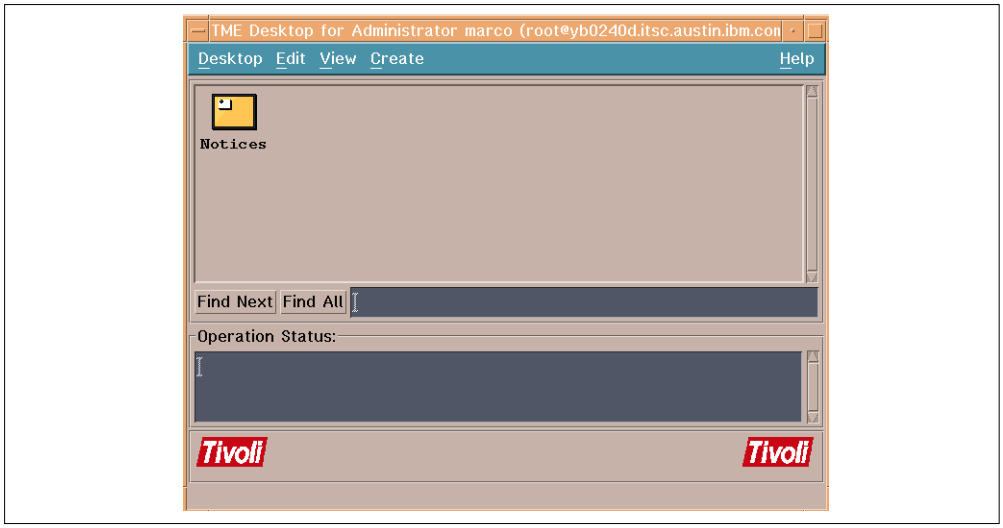


Figure 71. New Administrator's Desktop

8. The last operation is to customize marco's desktop. We said that this administrator should manage users and groups for all the AIX machines in our TMR. This means that we have to populate the desktop with these AIX hosts. Simply by opening the root administrator's desktop, we are able to drag and drop the AIX managed nodes.

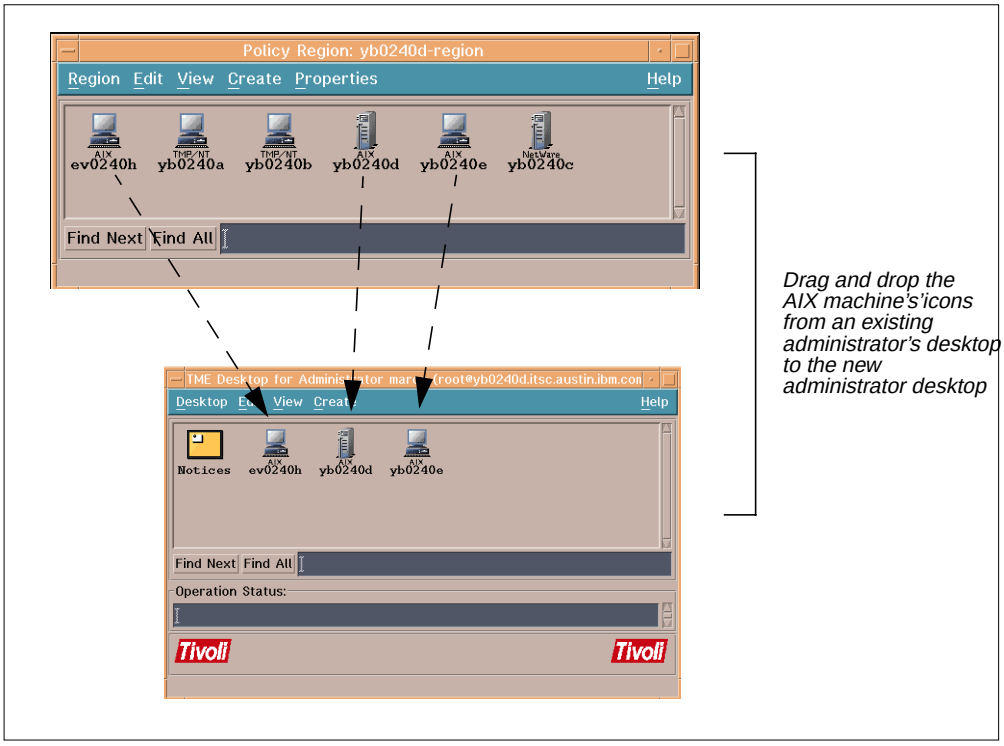


Figure 72. Populating the Administrator's Desktop

9. Now you are able to work with the new administrator. Log on to the machine *yb0240e* as *marco* and execute the command:

   `. /etc/Tivoli/setup_env.sh`

   Note: This command should be added to the .profile file in the administrator's home directory.

   Then launch the TME 10 desktop with the command `tivoli`; marco's desktop will come up.

5.6 Creating Profiles

TME 10 makes use of the TME 10 functions such as management by subscription. In pratical terms this means you should do two things:

- Create a policy region structure that maps the administrative organization of your managed environment.
- Create a profile manager structure that maps to the application organization of the managed nodes.

5.6.1 Setting Profile Managers and User/Group Profiles

In order to create TME 10 User Administration profiles, you must create at least one Profile Manager to contain these profiles and properly set the managed resources.

1. From the marco's desktop, select **Create**, then **Region**. The following window will come up.

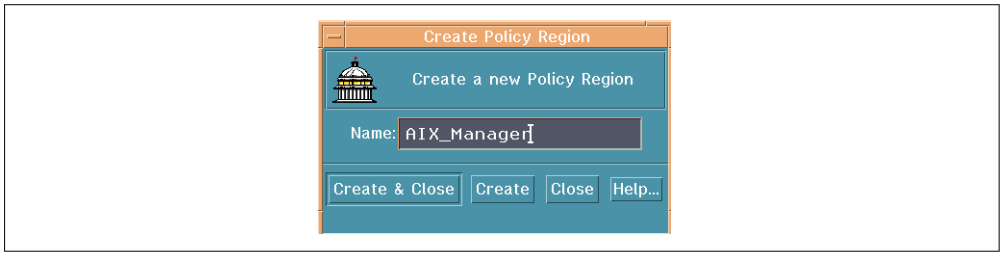


Figure 73. Create Policy Region window

Fill up the *Name* field with the name you want to assign to the new policy region. In our case we named the region *AIX_Manager*. Then click on the **Create & Close** button to have the region's icon added to the desktop as shown in the following figure:

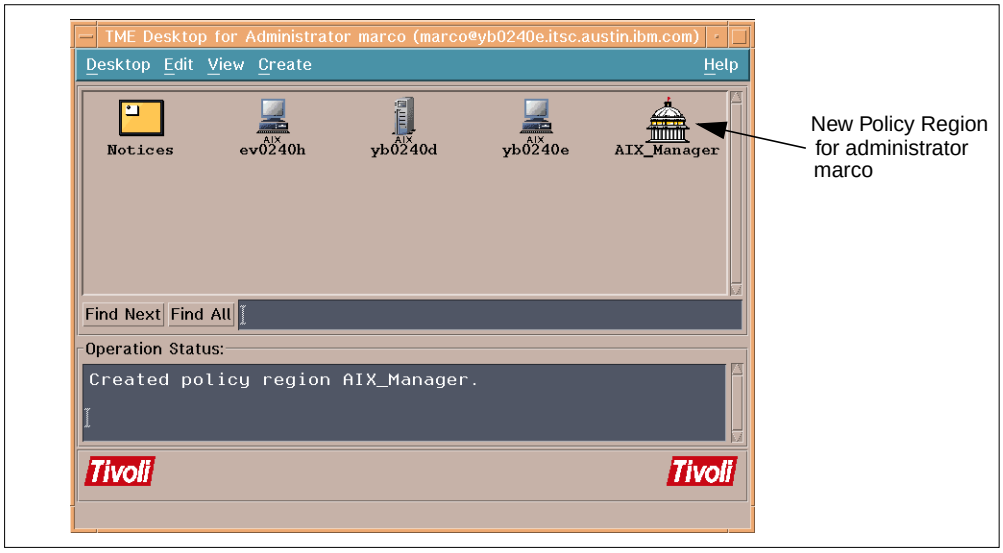


Figure 74. Administrator's Desktop Window

From the Policy Region's icon pop-up menu, select **Managed Resources**. The following window will appear:

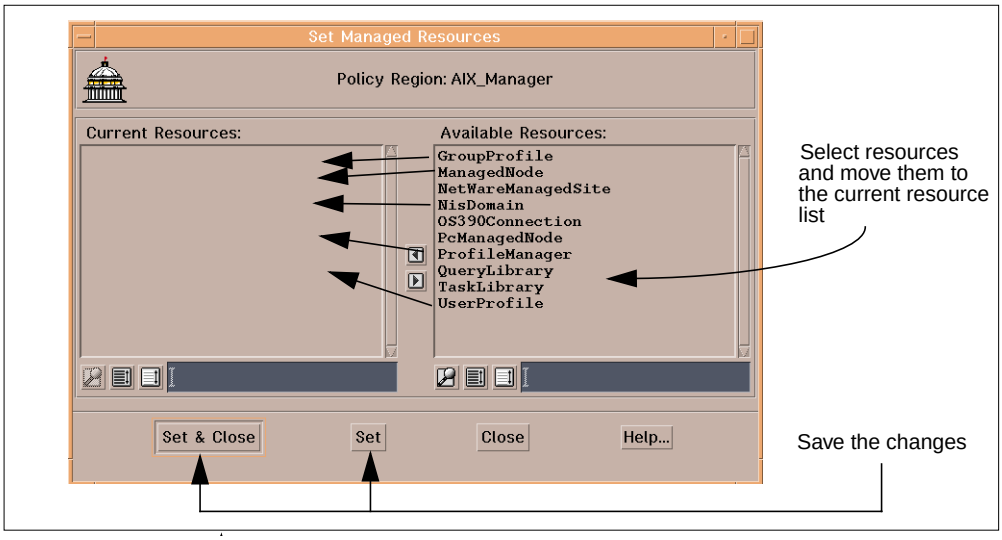


Figure 75. Set Managed Resources Dialog

After its creation, the Policy Region does not have current resources set. You need to add the resources you're going to use: *Group Profile*, *Managed Node*, *NIS Domain*, *Profile Manager* and *User Profile.* This allows you to include these managed resources in the *AIX_Manager* policy region. After adding the resources to the Current Resources list, click the **Set & Close** button.

2. From the desktop of Figure 74 on page 132, double-click on **AIX_Manager** Policy Region icon; an empty window will appear. This is the Policy Region's window. From its pull-down menu select **Create.**

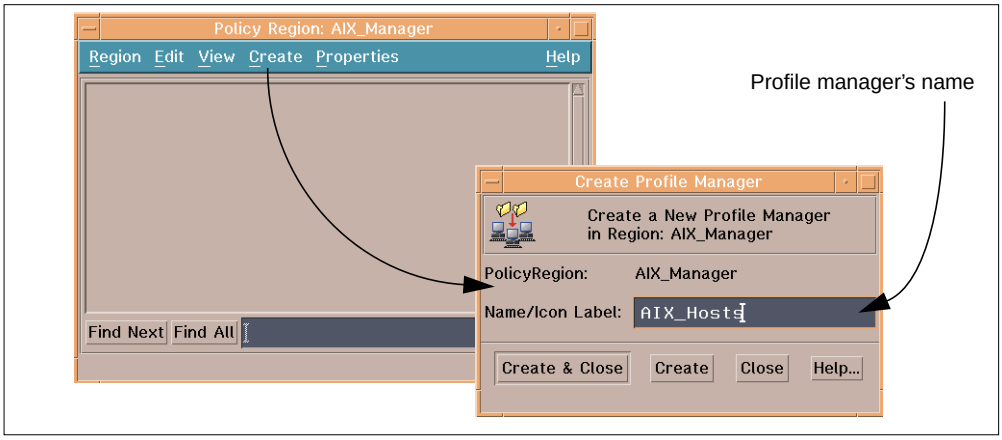


Figure 76. Profile Manager Creation

Fill in the name of the Profile Manager in the *Name/Icon Label* field, then click the **Create & Close** button to have the Profile Manager created in your Policy Region.

3. Double-click on the Profile Manager's icon. You'll get the Profile Manager window. In this window the profiles and the subscribers to these profiles must be specified. From the Profile Manager's pull-down menu, click on **Create**, then on **Profile**. You need to create two profiles:

   - *Group Profile*: to manage groups

- *User Profile* : to manage users

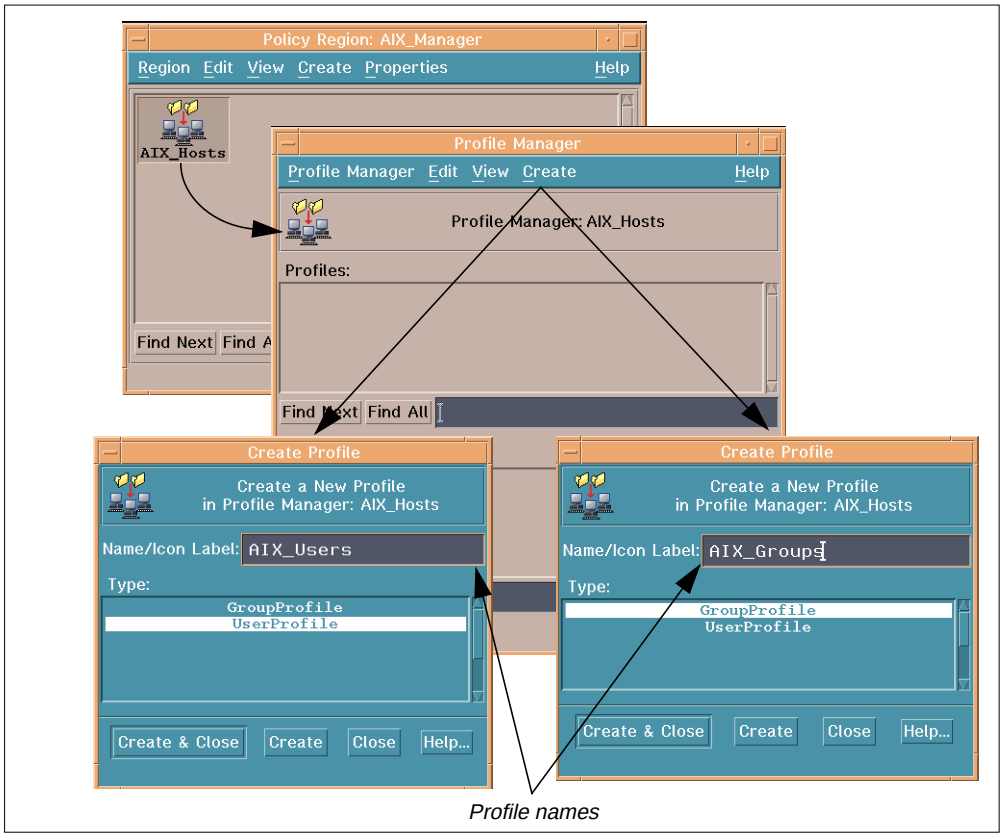


Figure 77. Profiles Creation Window

Fill in the *Name/Icon Label* fields in the *Create Profile* windows, then click **Create & Close** to finish the profiles creation.

4. The next step is to set the subscribers in the Profile Manager *AIX_Hosts.* You can perform this operaton in two ways:

   - By clicking on **Profile Manager** on the Profile Manager's pull-down menu and selecting the subscribers from the *Available to become Subscribers* list, as shown below:

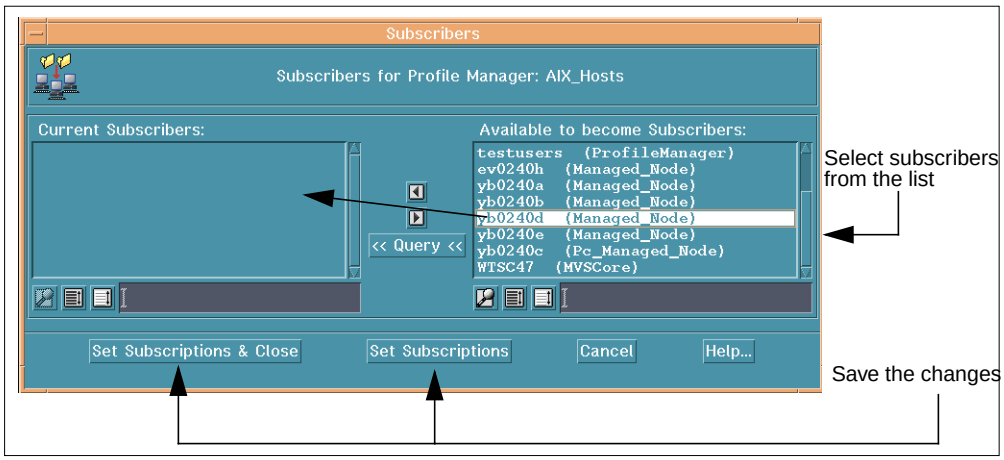


Figure 78. Subscribers Selection by List Selection

- By dragging and dropping subscribers from an existing desktop (in our case marco's desktop), as shown in the following figure:

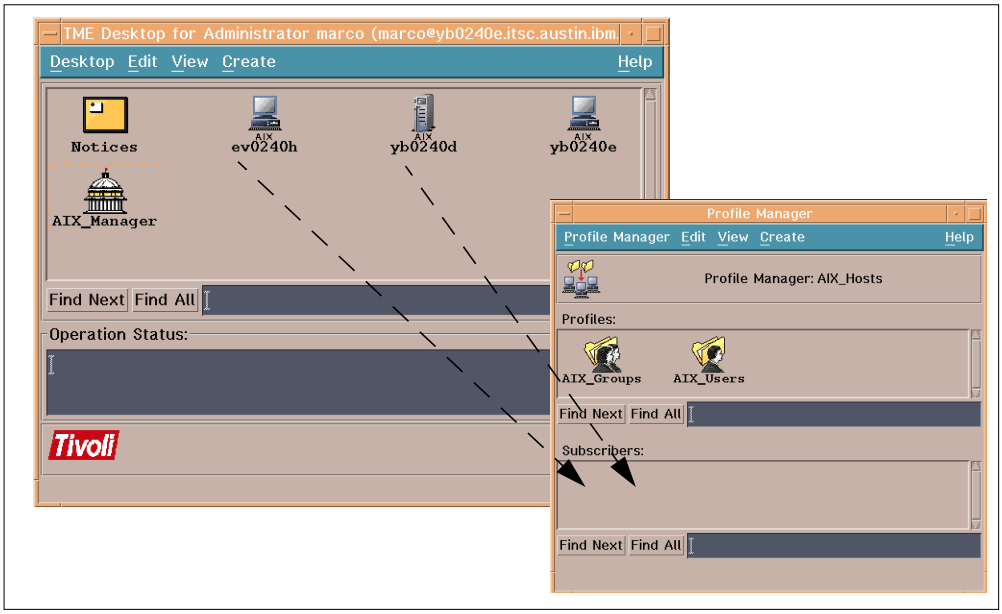


Figure 79. Subscribers Setting by Dragging and Dropping

5.6.2 Setting User and Group Profile Policies

Before attempting to perform any administrative management operation on profiles or subscribers (populate profiles, add users, remove users, and so on), it is necessary to understand the default and validation policies effects on these operations. These policies will be extensively put in practice in Chapter 6, "Working with TME 10 User Administration" on page 139.

The *default policy* is a kind of template that is used to set default attributes to users and groups when they are added in the profile.

The *validation policy* is a way to check that values entered in the profile for a user or a group comply with the policy rules.

Note about Validation Policies

Validation policies prevent you from adding non-compliant users or group definitions in the profile AND from populating the profile with users or groups previously created on the subscriber's machines that are not compliant with these policy rules. Every profile's record must be consistent with the validation policy profile.

5.6.2.1 Default policies

To see, and possibly edit, some user or group default policies, double click on the profile's icon, then from the window's pull-down menu, select **Edit** and then **Default Policies.** You will get the following window:

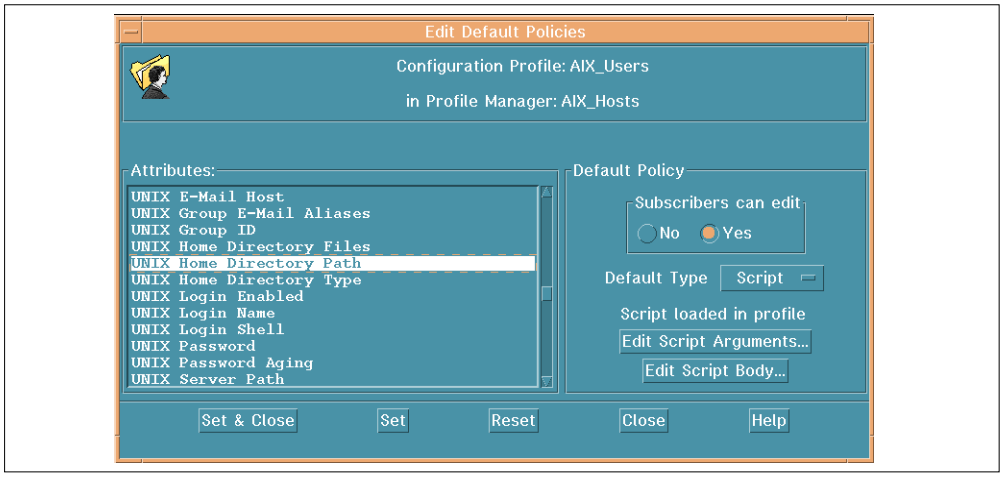


Figure 80. Edit Default Policies Window

This window shows the default policy for the user attribute *UNIX Home Directory Path*. This means that when you add a user, you may use this default policy to provide the value for the home directory attribute for that user record. We know that typically a new user is put in the /home/<login_name> directory as home directory. This is exactly what this default policy does. Let's have a look at the script body by clicking on **Edit Script Body**. You can see the script that generates this default:

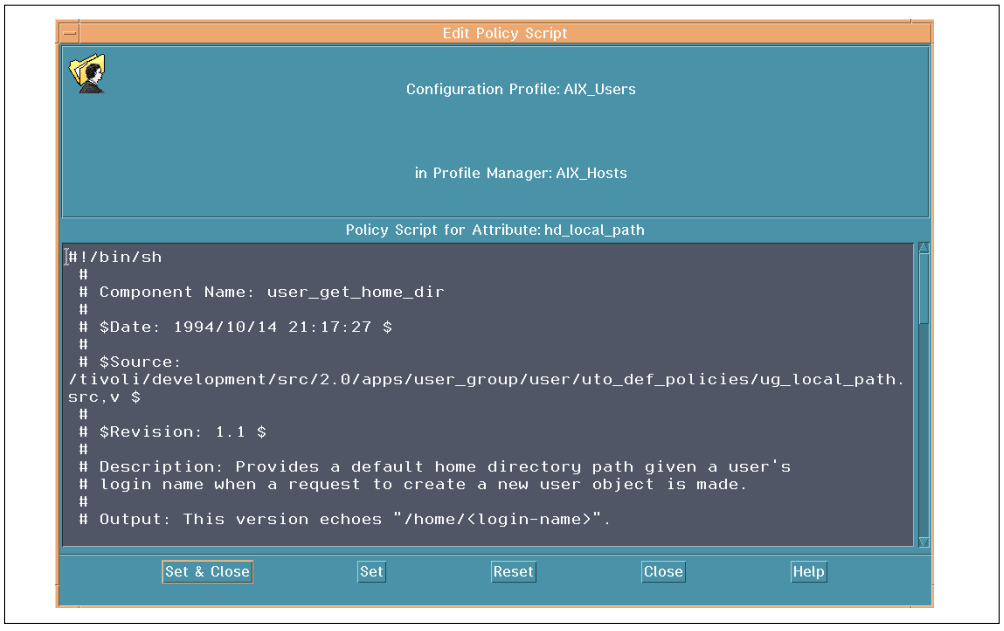


Figure 81. Default Policy Script

The script simply echoes the home directory of the newly created user:

```
echo /home/$LOGIN_NAME
```

If you want to change this default policy (for example, put all the new created users in /users/<login_name>), you need to edit the script body and change the `echo` command to :

```
echo /users/$LOGIN_NAME
```

then click **Set & Close** to make the change effective.

Another good example is the UID default policy. Every time you create a new user, it is assigned a unique identification number. The TME 10 default is to use the next available UID greater than 100. If you want to change this policy, you only have to modify the script's body in the following way:

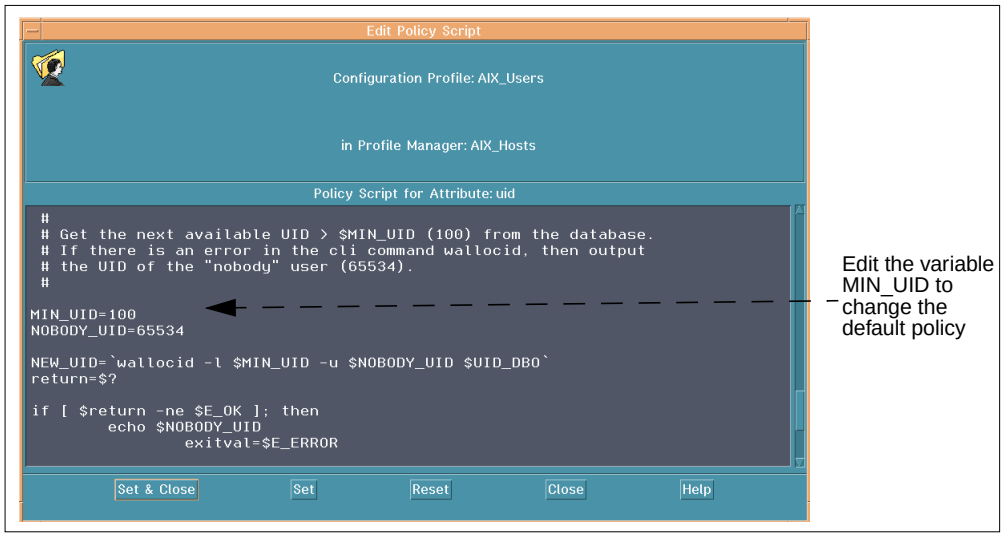


Figure 82. UID Assignment Default Policy

If you want your policy to use the next available UID greater than 150, you have to set MIN_UID=150.

The same way to operate is enabled for Group Profiles. You use the default policies as a template to add new groups complying with these specifications. For example, the UID default policy is to assign the new group the next available GID greater than 100.

Looking at Figure 80 on page 136, you can also note the option *Subscribers can edit*. This defines whether a policy can be changed by a subscriber. This means you can apply different policies to fields in the user records at the subscriber level. This capability is provided to enable a local administrator to customize the user information that a central administrator has provided.

Having a different default policy at a subscriber level will not change the attribute value at distribution time. It affects a default attribute value if you add a user at that level and do not provide a value for that attribute.

The default type can be:

- **Script**: This means that a shell script will be executed when you create a new user. This script will provide you the default value for the attribute.
- **Constant**: This will insert a fixed value into the field when you add a new user.
- **None**: No default value will be supplied for this attribute when a new user is added.

5.6.2.2 Validation Policies

A validation policy checks that values entered in the profile. For a user or a group, comply with the policy rules. To see these policy rules (for User or Group Profiles), double-click on the profile's icon. Then, from the window's pull-down menu, select **Edit** and then **Validation Policies.** You will get the following window:

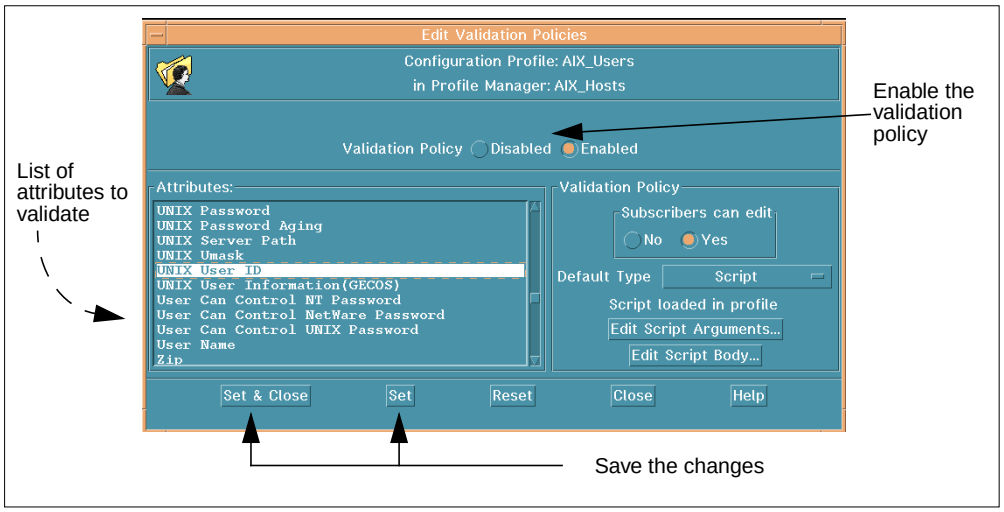


Figure 83. Validation Policies Window

We will consider again, as an example, the *UNIX User ID* Attribute validation policy. Looking at the script body, we read that the validation policy validates only UIDs within a range 1-65534, explicitly excluding the UID 0. You'll not be able to populate your profile with users having UIDs outside this range, or define users with UIDs outside this range. A good proof of this validation policy is the fact that (unless you disable the Validation Policy with the radio button) the user **root** (UID 0) and the user **nobody** (UID -2) fail the test and are not added to the profile when you populate it. (We'll test this feature in the following chapter).

Now we are able to:

- Define a profile manager
- Define User and Group Profiles
- Set subscribers
- Edit default and validation rules

This makes us ready to test the features of TME 10 User Administration 3.1.

Chapter 6. Working with TME 10 User Administration

This chapter provides general information on how to use TME 10 User Administration. Also, it gives more specific details for each environment on how to administrate users and groups. Because each environment (UNIX, Windows NT, NetWare, OS/390) is specific in terms of user administration, this chapter describes what you should expect from the product in terms of functions and limitations. It also gives some useful hints and tips that should help you in taking advantage of the product.

6.1 General Operations

This section covers user and group administration tasks and issues common to all the platforms. All platform-specific tasks are covered in the corresponding platform section. The operations listed in this section are common for every type of profile. In order not to repeat the same information for each type of profile, the following explanations will be general. From this point on to the end of the section, we will use the term *profile* to refer to any type of TME 10 User Administration profile.

6.1.1 Creating User and Group Profiles

Before you can add any user or group to the TME 10 User Administration database, you must create the appropriate TME 10 profile in a profile manager. Initially, when you create a profile, it does not have any records. This means that you need to manually add records to the profile, one at a time, copy records from another profile, or populate your profile by retrieving user and group information from one or more endpoints. When you create a profile, you are basically creating an empty template.

Just like any other Tivoli profile, a profile is created within a profile manager by using the *Create* pull-down menu and specifying the appropriate profile type (UserProfile, GroupProfile).

However, before the profile options are presented to you in the upcoming *Create Profile* dialog, you must add the profiles to the managed resources in your policy region. You can do this from the *Properties* pull-down menu in the policy region window when you select the **Managed Resources...** option. You can also call the *Set Managed Resources* dialog to check whether the profiles are listed under the currently managed resource types.

Important

Remember that in order to create or maintain a profile you must have the particular profile type as a managed resource and an appropriate administrator role within your policy region.

6.1.2 Populating a Profile

Populating a profile means importing information defined in a system configuration file from one or more managed nodes or NIS domains. When populating a profile, you can specify which endpoints to retrieve the information from and whether this information should overwrite the original profile information

or append that information to the profile. For example, you can populate a user profile with the users from one or more endpoints.

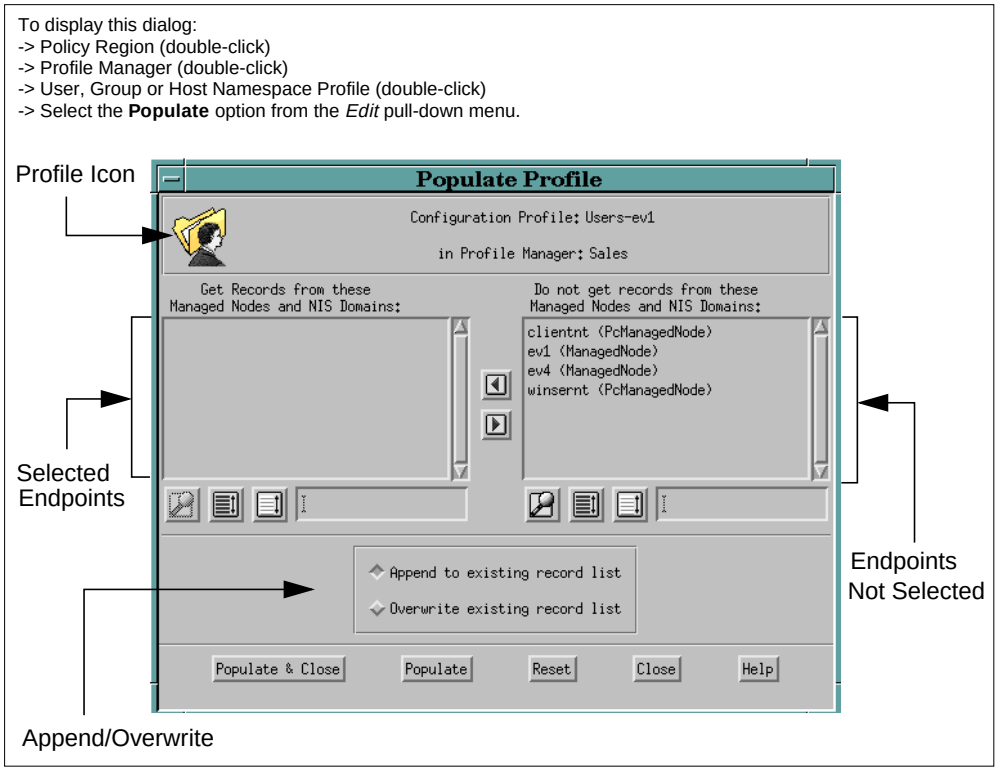


Figure 84. Populate Profile Dialog

The Selected Endpoints area in the Populate Profile dialog (Figure 84) lists the TME resources from which to populate the profile. You can move one or more entries from the other area, Endpoints Not Selected, to the left in order to designate the source(s) for the populate operation. The Append/Overwrite radio buttons determine whether to add the new records to the existing records in the profile or replace the contents of the profile with the new records.

Note: Populating from the OS/390 server cannot be done with the Populate Profile dialog; the `wpopusrs` command must be used. As a result of the large numbers of user accounts generally defined on OS/390 systems, there are special considerations for populating from OS/390 servers. Refer to Section 6.6“Managing RACF Users” on page 259 for full details.

For more information about populating a profile, see the *TME 10 Framework User's Guide*.

Note: Populate does not run default policy. So any attribute that is not directly derived from the system configuration files will be left blank.

User Merge when Populating a User Profile

When you populate a user profile, TME 10 User Administration attempts to merge duplicate user information coming from different managed nodes into the user records of the profile. The login name is used as the key to determine whether there is a match between two users. If there is a match between login names, then TME 10 User Administration verifies the operating system type (UNIX,

Windows NT, NetWare, RACF). If the information comes from the same operating system type, TME 10 User Administration returns an error. Otherwise, if the operating systems are different, TME 10 User Administration merges the new record information into the existing profile record.

There are two types of information regarding a user: general information that is platform independent, such as the user name, and platform-specific information. When two users have the same login name on two different systems, the first user information found is populated into user record into the profile, and the second user information is merged with the user record already created.

When the user information is merged, the general information is merged on a attribute-by-attribute basis with the information that exists in the user record taking precedence. This means that attributes already having a value are not overwritten with the value of the second user's attribute. Attributes that were not filled out are gathered with the new value.

If the first user is a UNIX user and the second user is a Windows NT user, Windows NT information will be added to the user record. If the two users are UNIX users, UNIX information for the second user will not be merged to the first one.

6.1.3 Adding Subscribers

Profiles reside in profile managers. In order to distribute the profiles to endpoints, it is necessary to subscribe endpoints to a profile manager. A list of subscribers can be defined at two levels:

- Profile manager level
- User record level

Actually, you can define for each user a list of subscribers. TME 10 User Administration provides a user attribute called *Subscribers*. Defining a list of subscribers to a particular user allows the system administrator to distribute that user only to specific endpoints.

User-record-level subscribers are only available for user profiles; they do not exist for group profiles.

6.1.4 Distributing a Profile

After you have populated a profile or modified records of a profile, you must distribute the profile to the subscribers to make use of the new information contained in the profile.

It is extremely important to understand the way distribution works to avoid mistakes.

First of all, valid endpoints for profile distribution are:

- Profile Manager
- Managed Node (UNIX or Windows NT)
- PC Managed Node (Windows NT or NetWare)
- NIS Domain
- OS/390 Connection

There are two types of profile distribution:

- **Next level of subscribers**

  When you distribute the profile using this option, you create copies of the profile on the next level of subscribers. This next level of subscriber can be a profile manager, a Managed Node, a PC Manage Node, an OS/390 Connection or an NIS domain.

  System files will not be updated even if the next level of subscriber is just a managed node. The TME 10 database on that managed node is updated with the changes to the profile. This actually allows an administrator to make local changes in the profile and then distribute that local profile to the endpoint and therefore update the system files. For more information on how to distribute a profile from an individual endpoint, refer to“Distributing from an Endpoint” on page 144.

- **All levels of subscribers**

  When you distribute the profile using this option, you actually distribute a copy of the profile to all the objects in the distribution chain, and you modify the system files or NIS maps on the endpoints.

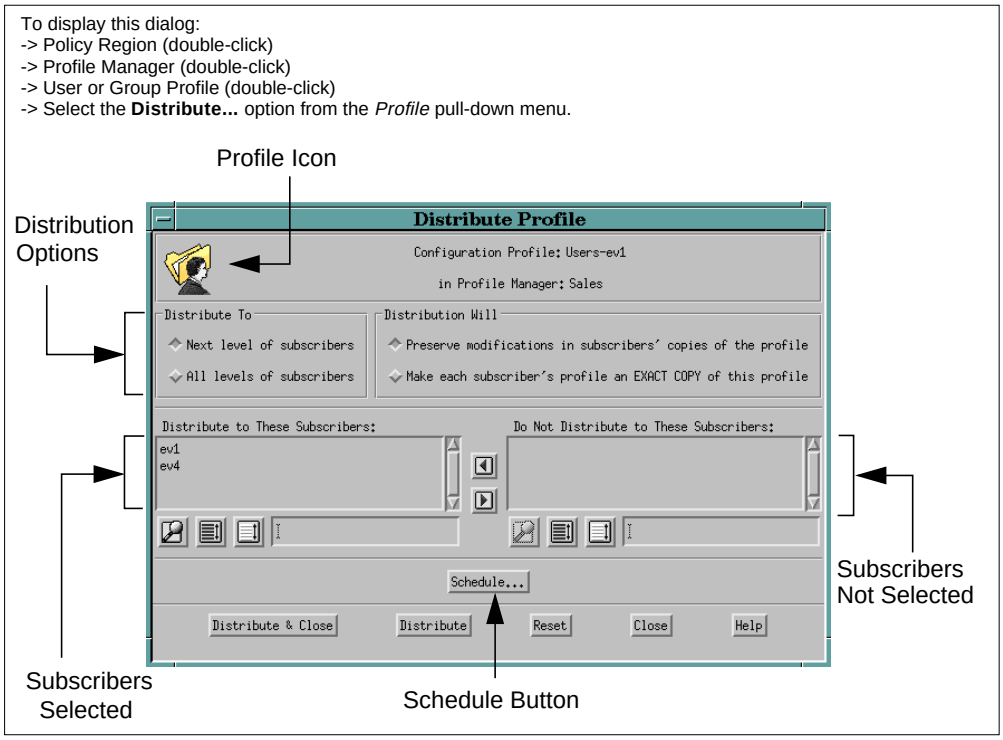


Figure 85. Distribute Profile Dialog

Figure 85 shows the Distribute Profile dialog that allows you to distribute the profiles. The subscribers that are selected will receive all records defined in the profile. The subscribers not selected are subscribers to the profile manager that you want to exclude from receiving this particular profile.

There are two modification options:

- **Preserve modifications in subscribers' copies of the profile**

  This option allows you to keep any changes made on the subscriber's copy of the profile. These local changes are not overwritten when you distribute the profile. For example, if a user profile is edited directly at a managed node to add new users and the top-level profile (original) is distributed, then the users created locally will be preserved. Also, if a user attribute has been modified in the local user profile, then that modification will be preserved.

  This is also true for system files. If you update the system files by distributing a local copy of a profile, any records that have been added to the system files will be preserved (kept). Also, any changes made directly on the system files will be preserved.

  However, if a record attribute has been changed in the profile, that attribute will be changed to the new value in the local copy of the profile or in the system files even if that particular attribute was modified locally.

  When profiles are distributed with the above option, only records that have changed are actually pushed. For example, if a user profile has 200 users, these 200 users will be pushed the first time you distribute the profile, but only records that have changed will be pushed at the next distribution, not all 200 users.

  This option has the great advantage to give some flexibility in terms of system administration. You might want to locally maintain a specific set of users on a specific system, or you might want to maintain specific security attributes for users working on a system having sensitive information.

- **Make each subscriber's profile an EXACT COPY of this profile**

  This option will make all downstream copies of the profile identical.

  If you use this option in conjunction with the All levels of subscribers option, the system files will be overwritten; any accounts except root that are not in the merged profiles will be deleted. Home directories are not deleted.

Attention!

If the profile you are distributing contains a subset of users or groups, all additional users or groups defined on the local profile or on the system files will be deleted!

This option must be used with lot of care.

Note that changes to local copies of profiles can be limited on a record level by locking records (see 6.1.7.2“Locking and Unlocking Profile Records” on page 149). The distribution of the profile can be scheduled for a later time by using the Add Scheduled Job dialog. Clicking on the **Distribute** or **Distribute & Close** buttons will execute the distribution and either leave the Distribute Profile window open or close it.

For more information about distributing a profile, see the *Tivoli Management Platform User's Guide*.

Distributing from an Endpoint

After a profile is distributed, it appears in the dialogs of its subscribers (endpoints or profile managers) as a local profile icon. You can access local profile copies by double-clicking on a managed node's icon. The window presented displays the node's local profile icons.

To display this dialog:
-> Policy Region (double-click)
->ev7 Managed Node icon (double-click)

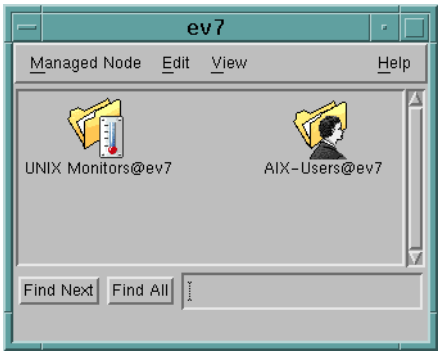


Figure 86. Local Profile Copies an on Endpoint

Distributing such a local profile updates the system files for only that node. This is also called *distributing from an endpoint* versus distributing from a profile manager.

To display this dialog:
-> Policy Region (double-click)
->ev7 Managed Node icon (double-click)
-> User, Group Profile (double-click)
-> Select the **Distribute...** option from the *Profile* pull-down menu.

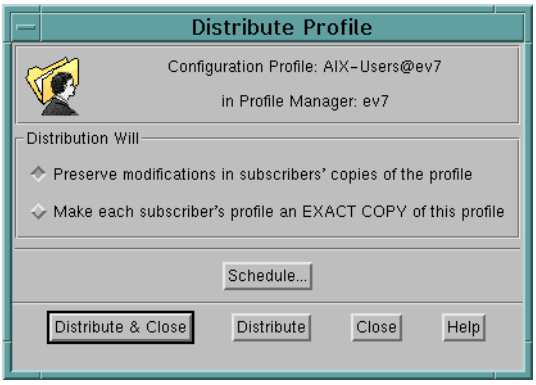


Figure 87. Distribute Profile Dialog on an Endpoint

When distributing from a local profile on an endpoint, you have the option to replace the whole system configuration file, making it an exact copy of the profile, or you can choose the preserve modifications option which will not delete any non-profile accounts (there is no profile downstream from this one that needs local modifications).

Determining to Which Subscribers the Profile is Distributed

We have seen previously that subscribers to a profile can be defined at two levels:

- Profile manager level
- User record level

When distributing a user profile, TME 10 User Administration first uses the profile manager subscribers to determine which endpoints and profile managers are possible targets for the distribution. Then TME 10 User Administration makes use of the list of subscribers defined at the user record level to verify to which subscribers each record of the profile will actually be delivered. For details on how to set the record level subscribers for a user profile record, see Section 6.1.7.1“Adding Users” on page 147.

For example, let’s suppose that you have a profile manager containing the user profile called *ITSO-Users*. The managed nodes itso1, itso2, itso3, itsorus, itsobig, ev1, and ev4 are subscribers to this profile manager.

The user profile ITSO-Users has three user account records with the following record level subscribers:

- The first user record lists the managed nodes, *itso1*, *itso2,* and *itso3*
- The second user record lists the managed nodes, *itsorus* and *itsobig*
- The third user record lists only the managed node *ev1.*

If you distribute the *ITSO-Users* profile using the **All levels of subscribers** option the following distributions occur:

- The first user record is added to the managed nodes *itso1*, *itso2,* and *itso3.*
- The second user record is added to the managed nodes *itsorus* and *itsobig.*
- The third user record is added to the managed node *ev1.*
- No user records are added to the managed node *ev4*.

Hidden Distribution Methods

If, for example, a system administrator accidentally removes some entries from /etc/group on a UNIX system, he/she might want to retrieve these entries. Distributing the profile with Exact Copy will put back the missing entries, but will remove all entries added locally. Distribution with Preserve modifications will not restore the missing entries since no records have been changed in the user profile.

It is possible to distribute all the records in the profile without making an exact copy. This is possible by using the `wdistrib` command along with the `over_opts` option as shown below:

```
wdistrib -m -l over_opts @UserProfile:<profile_name>
@ManagedNode:<managed_node_name>
```

Note:

If you do not specify `-m`, the system files will not be updated but the local copy of the profile at the managed node level will be updated. If you want to update a group profile, substitute @UserProfile with @GroupProfile. Also, if you do not specify any managed node with the @ManagedNode option, the profile will be distributed to all subscribers.

Getting a New Copy of a Profile

From a subscriber, TME 10 User Administration allows you to get a copy of a profile from the profile manager one level higher in the subscription hierarchy. Instead of pushing a profile from a profile manager to its subscriber, one subscriber can pull a copy of that profile stored in the profile manager. This can be done by opening the subscriber's profile and selecting **Profile**, **Get New Copy**.

6.1.5 Cloning a Profile

Cloning a profile consists in creating an exact copy of the profile you are cloning, including the default and validation policies associated with it. However, the profile records and the list of subscribers are not copied. The new profile has no records.

6.1.6 Deleting a Profile

Deleting a profile deletes the original profile, the entries contained in the profile, and the copies residing in the profile manager's subscribers.

Deleting a profile does not delete the information contained in the system files at the endpoints.

To delete the contents of the system's configuration files, you must delete all the entries in your profile and then distribute the empty profile to the endpoints. The previous operation deletes everything corresponding to deleted profile entries, except the root entry, any NIS directives in the configuration files, the Administrator entry for Windows NT or the Admin entry for NetWare.

6.1.7 Adding Users or Groups

This section explains how to add a user record or a group record to a profile. These tasks can be performed from the corresponding Profile Properties window (User Profile Properties window, Group Profile Properties window) that can be open by double-clicking on the profile icon.

Remember to Save Profiles

Every time you modify the contents of a group profile, you must save the profile before closing the corresponding profile properties window in order to preserve the changes. If you modify the contents of a user profile, it is not necessary to save the profile.

Group profiles utilize profile-level locking. This means only one Tivoli administrator can edit a particular group profile. User profiles utilize record-level locking. Multiple administrators can concurrently edit the same user profile. When you save an edited user record, the profile is updated; so there is no need to save the profile itself.

Adding records to a profile can be performed one at a time, manually, by populating the profile or by copying records from another profile. Populating a profile is explained in "Populating a Profile" on page 139. Therefore, this section describes how to add records manually.

When you create a new record, TME 10 User Administration stores the information in the corresponding profile database. The new information is not

applied to any system files until the profile is distributed to its ultimate destination, which is a set of subscribing systems or NIS domains.

6.1.7.1 Adding Users

In order to add a new user, you push the **Add User...** button in the profile window. See Figure 17 on page 69 for a profile window. Figure 88 shows the User Properties dialog that allows you to enter the user account information.

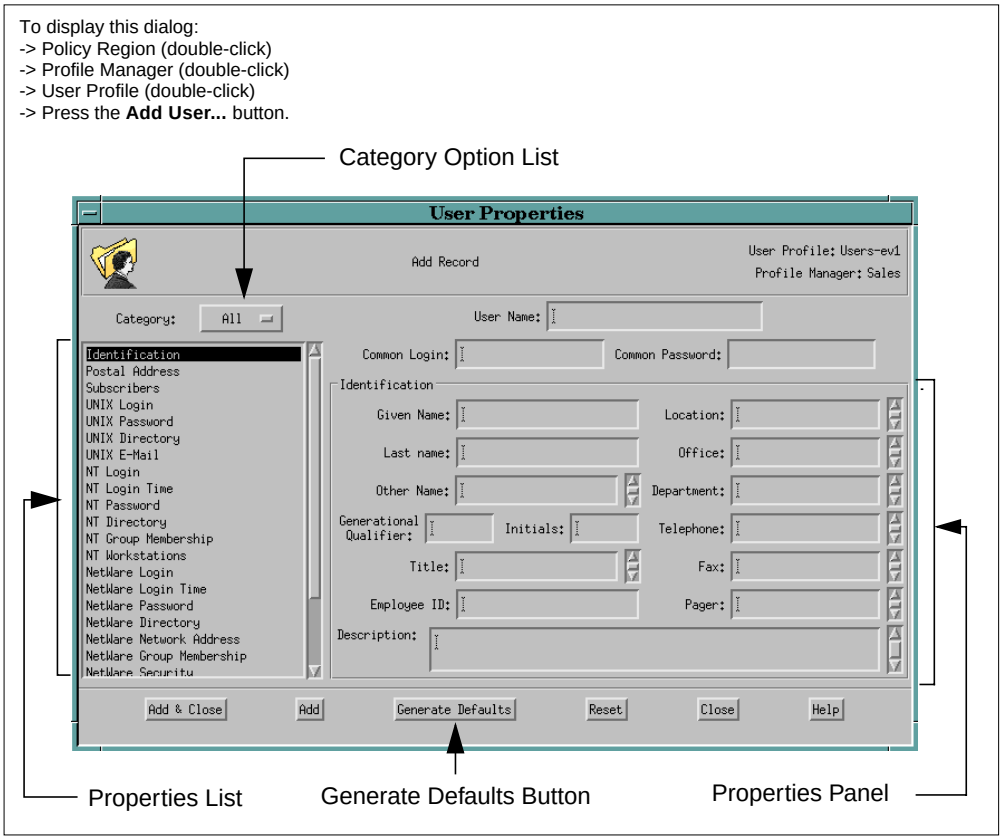


Figure 88. User Properties Dialog

The Properties Panel area is where you add the profile record information. Its content changes with what is selected in the Properties List. Figure 88 shows the panel for User Identification. With the Category Option list, you can filter what is displayed in the Properties List. The available categories are: All, General, NT, NetWare, UNIX, and RACF (if the TME 10 GEM User Administration Service for OS/390 is installed).

Common Login and Password

When creating a user in a user profile, you can specify a login name and a password that are common to all platforms. This means that, once the profile is distributed to all the subscribers and the system files modified, the user can use the same login name and password to log in to the systems. This is a way to keep user IDs and passwords consistent across all platforms.

However, you can still specify a different login name on a specific platform. For examples you might want to use a different login name for that user on UNIX platforms.

Defaults Attributes

The Generate Defaults button allows you to apply (fill in) the default policy values to the fields in the properties panel. The Add function implicitly runs a Generate Defaults for all values left empty.

As explained in “Determining to Which Subscribers the Profile is Distributed” on page 145, subscribers can be defined at the profile level or at the user level.

If you want to specify record-level subscription for the user record you are currently modifying, you must select the **Subscribers** option from the Properties List (third item from the top in Figure 88) and then select the corresponding subscribers. Remember that the record-level subscribers override the profile manager subscribers.

Adding Groups (UNIX Only)

Figure 89 shows the Add Record To Profile dialog that allows you to enter the group account information.

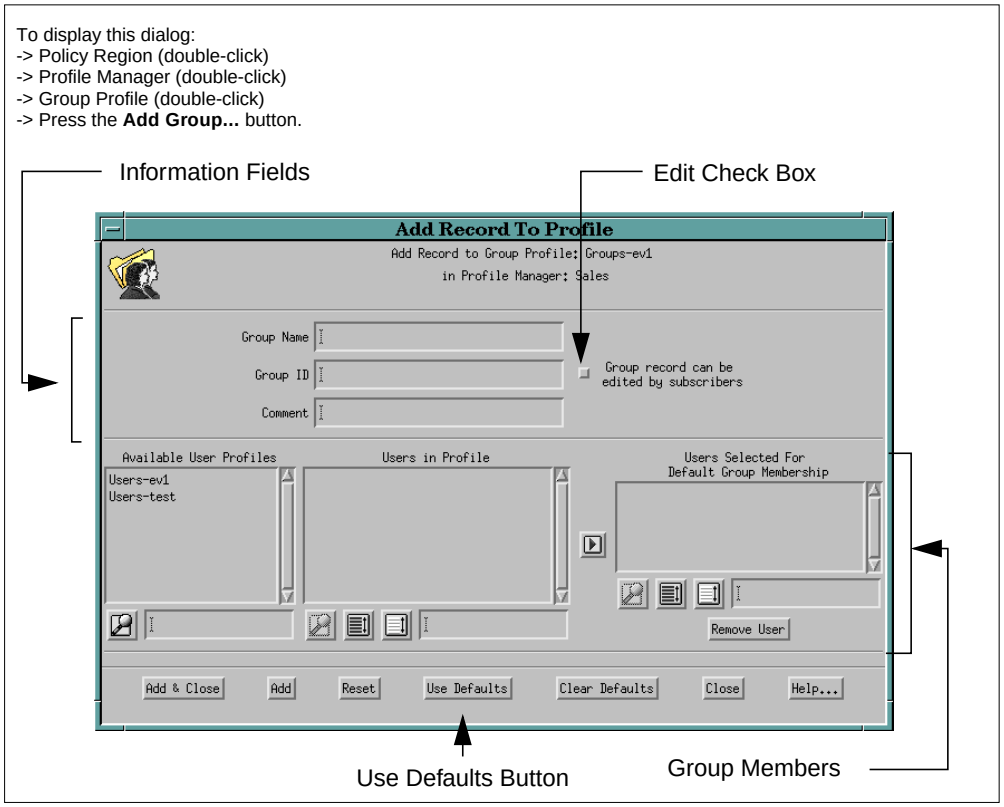


Figure 89. Add Record To Profile Dialog

The information fields allow you to enter the Group Name, Group ID (GID), and comments about the group. The Edit Check Box specifies whether or not subscribers can change the record in their own copies of the profile.

Group members can be added by opening a profile from the Available User Profiles list and selecting users from the Users in Profile list. The **Use Defaults** button allows you to fill in the default policy values set for these fields. If you press this button after you have entered information into a field for which a default policy

is defined, TME 10 User Administration replaces your information with the default information.

6.1.7.2 Locking and Unlocking Profile Records

It is possible to lock any record of the profile to prevent the local administrators of the lower levels from changing the contents of a specific record. You must distribute the profile after locking or unlocking records in order for this operation to take effect, which means you actually lock/unlock records on the target machines.

You can lock all records contained in a profile, but it is not possible to lock an entire profile. In other words, administrators cannot modify the locked records, but they can add new records to a lower-level profile copy.

Unlocking the information in profile records is the opposite operation of locking the information. Unlocking records that were previously locked allows the local administrators of the lower-levels to change the contents of those records.

6.1.7.3 Handling and Manipulating Records

This section briefly explains the available functions for manipulating profile records. It includes descriptions of the following topics:

- Viewing records
- Editing records
- Deleting records
- Copying records
- Moving records
- Validating records
- Retrieving records
- Finding records
- Sorting records
- Sorting record attributes

These tasks can be performed from the appropriate profile properties window, for example from a User Profile Properties window, which is shown in Figure 17 on page 69.

Viewing Records

You can view the information contained in a profile (whatever type of profile) in a table format. Each column contains specific information about the record. You can scroll through the window to view the records stored in the profile and the information stored in each record. The View pull-down menu provides you some options, such as redefining the sort order of the records and which of the many attributes are displayed for each record. See “Sorting Records” on page 153, and “Sorting Record Attributes” on page 154, for details.

Editing Records

Double-clicking on a profile record brings back the edit record window, such as the User Properties window shown in Figure 88 on page 147, which also allows you to modify a record. Every time a record is changed, the new information is stored in the profile database, and a notice reporting the changes is sent to the notice database.

It's important to keep in mind that any change made in a profile record will not take effect until you distribute the profile to its ultimate destination, the endpoints subscribed to the profile.

When you edit an entry of a user profile, the entry is locked to prevent someone else from editing the same entry. Only the entry you are working on is locked, meaning that several administrators can have the same user profile open at the same time.

Note on UIDs

If you edit a user profile entry and you change the user ID (UID) of a user account, TME 10 User Administration will change the ownership of the user's home directory and the files in the home directory owned by the user, if you selected the option Change Owner ID of Files when the UID is changed.

Deleting Records

If you no longer need the information stored in a record, you can delete the record from the profile. Remember that if you delete a specific record from a profile and if you want to update the copies on the target machines of that profile, you must distribute the profile.

To delete a user profile record, you either click on the **Delete Users** button or select the **Delete Users** option from the Edit pull-down menu of the profile window. TME 10 User Administration displays the following warning dialog.

Figure 90. Delete Warning Dialog

In this dialog you can click on the **Delete Home Directory** button to delete the user's home directory or click on the **Leave Home Directory** button to leave the user's home directory and still delete the user record from the profile.

This dialog is presented for all user deletions, regardless if the platforms affected support the concept of a user home directory. For instance, consider a user that only has an OS/390 account. On deletion of this user, the delete home directory dialog will still be displayed, regardless of the fact that a user does not have a home directory on OS/390 RACF. This is a further example of TME 10 having to provide an architecture that supports all platforms, resulting in some dialogs that do not have meaning for some platforms.

Copying Records

It is possible to copy one or more records from one profile to another. When you copy records from one profile to another, you are creating an exact copy of the source records in the target profile. The target profile must be the same profile type as the source profile. The target profile cannot be in the same profile manager as the source profile. In other words, a single profile manager cannot have two profiles of the same type with the same information.

Figure 91 shows the Copy Profile Records dialog that allows you to copy records from one profile to another.

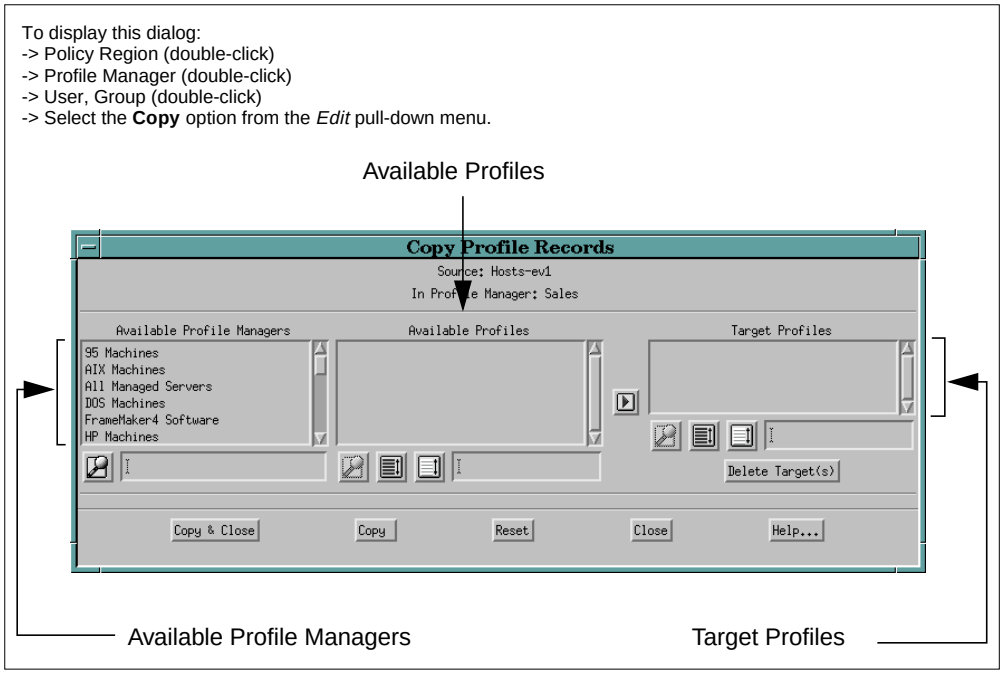


Figure 91. Copy Profile Records Dialog

In order to copy records, you highlight them in the profile window, and select the **Copy Users...** option from the Edit pull-down menu. In the upcoming Copy Profile Records dialog (Figure 91), you select a target profile manager, which brings up a list of profiles. Select one or more profiles from the Available Profiles list. The selected profiles are displayed in the Target Profiles panel. Then click on the **Copy** or **Copy & Close** button to perform the copy.

Moving Records

Figure 92 shows the Move Profile Records dialog that allows you to move records from one profile to another. To display this dialog, select the **Move Users...** option from the Edit pull-down menu within the corresponding profile properties window.

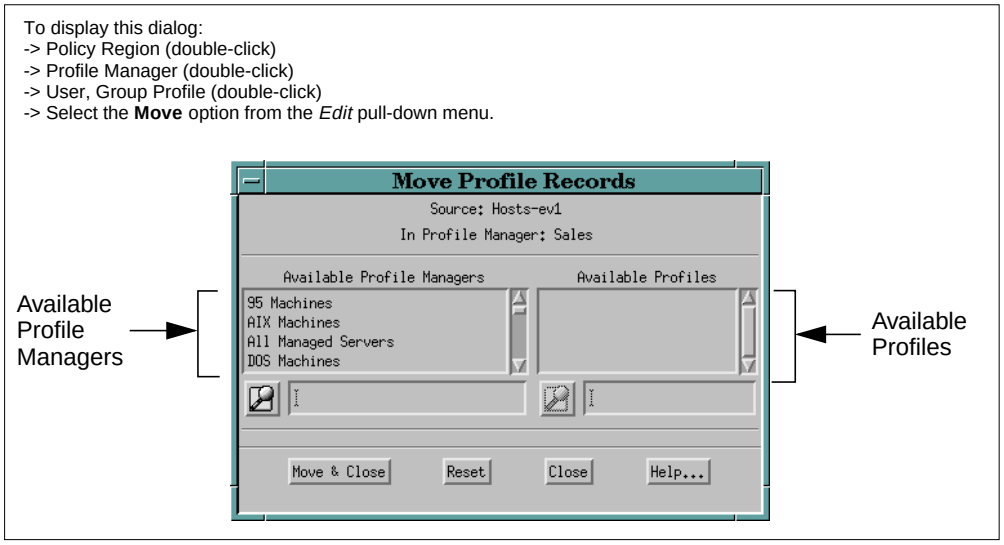


Figure 92. Moving Profile Records Dialog

When you select a profile manager, its profiles are displayed in the *Available Profiles* list. Choose one to which the selected records are moved.

Validating Records

Every time a record is changed or added, TME 10 User Administration automatically validates each attribute that has been assigned a validation policy. If you have changed the validation policy after adding or changing records, you may want to verify if the records that you had before the changes comply with the new validation policy. TME 10 User Administration provides a mechanism to validate all profile records at any time. It is important to remember that TME 10 User Administration will only validate the attributes with a validation policy assigned.

Finding Records

Sometimes it is necessary to find a specific record that is stored in a profile. TME 10 User Administration provides a mechanism to perform this task. Figure 93 shows the Find Records dialog that allows you to find records stored in a profile.

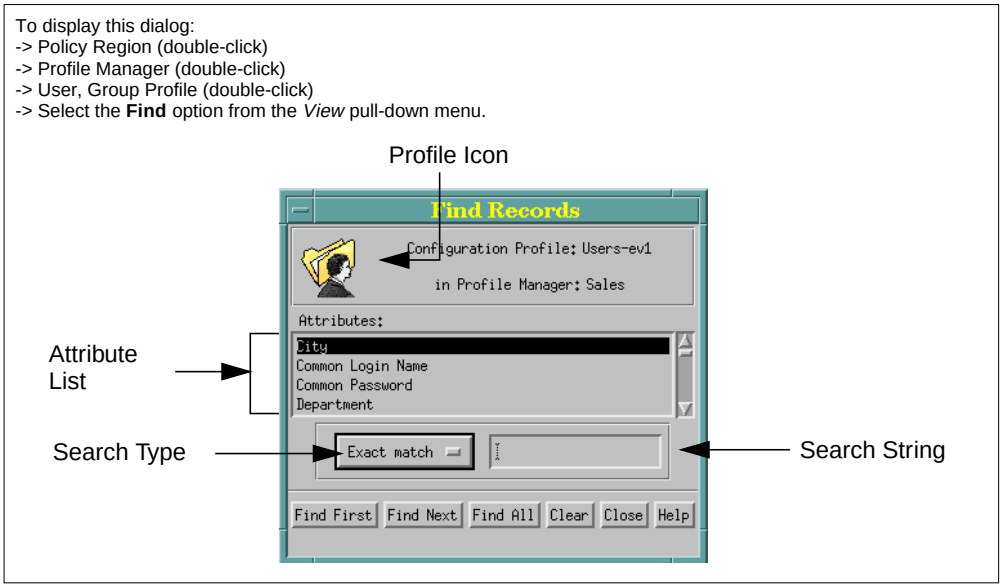


Figure 93. Find Records Dialog

In order to search for records, you select an attribute from the Attribute List, enter a search string to be matched against the attribute value, and specify the search type, which can be *Contains*, *Exact match*, *Greater than,* or *Less than*. The records that match the criteria are highlighted in the profile properties window.

Sorting Records

TME 10 User Administration provides a mechanism to set the order in which the information is displayed in the table-formatted Profile Properties window.

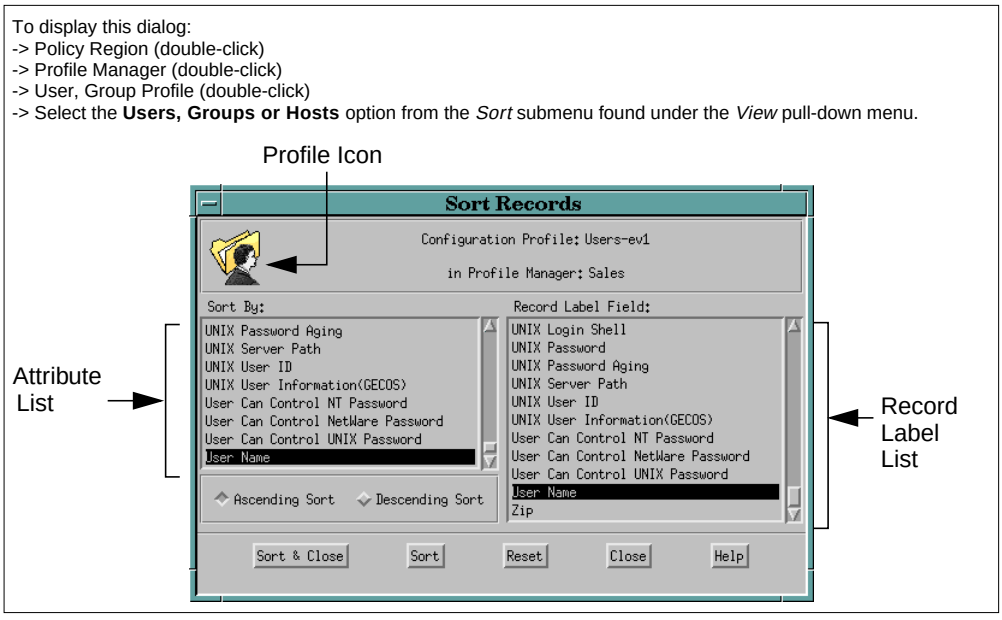


Figure 94. Sort Records Dialog

Figure 94 shows the Sort Records dialog that allows you to set the order in which the records are displayed (Attribute List) and to set the attribute that is used as the record label (Record Label List).

Note: When you close a profile that has been sorted and you reopen, your sort is lost.

Sorting Record Attributes

The table-formatted Profile Properties window provides a list of all profile records contained in the profile. However, since profiles have a lot of attributes, only a few can be displayed. TME 10 User Administration provides a mechanism to select which attributes are displayed in the entries table of a profile and also the order in which they are displayed.

Figure 95 shows the Display Attributes dialog that allows you to set the attributes that are to be displayed and their display order.

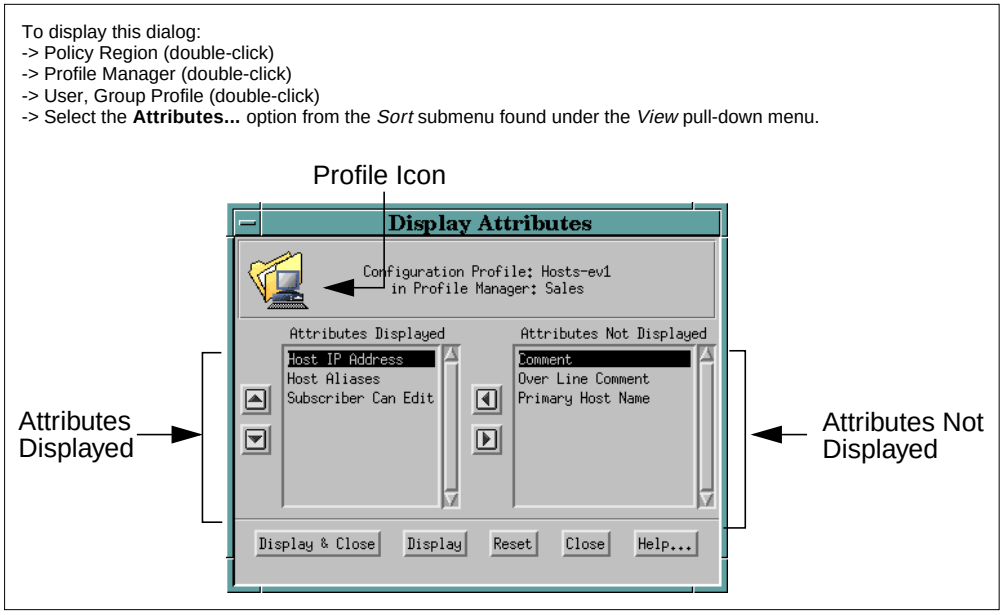


Figure 95. Display Attributes Dialog

6.1.8 User Profile Passwords

Passwords are one of the most sensitive pieces of information in a distributed environment. It is very important to understand how passwords are managed by TME 10 User Administration. Note that password management might be slightly different from one platform to another. This section provides the general mechanisms used to manage passwords. You should refer to the platform-specific sections for details on password management on each platform.

When distributing a profile, only records that have been changed/updated are distributed. If a record has been changed (for example, one attribute has been modified), the entire record will be distributed EXCEPT the password.

When user profiles are distributed, user passwords are overwritten in the system files ONLY IF the password itself has been changed in the user profile by the

administrator or the user changed the password in the profile with the wpasswd command.

In fact, there are two ways of managing passwords with TME 10 User Administration:

- User Control
- Administrator Control

6.1.8.1 User Control

User Control means that the user can change his/her own password by using the appropriate command on the system (for example passwd in UNIX) or by using the TME 10 User Administration command wpasswd.

In UNIX, the passwd command will only update the system files. Since the administrator allows users to change their own password, the distribution will not overwrite the user password in the profile at the subscriber level or in the system files.

The user can also change his/her password with the wpasswd command. This will change the user's password in all the profiles where this user is defined. This means that the local profile as well as the top-level profile will be updated. When used in conjunction with the -l option, the wpasswd command will update the password in the system file also. If the -l option is not used, the system file will be updated only when the profile is distributed.

A pre-expire option when set to TRUE (check-box selected), will prompt the user to change his/her password.

6.1.8.2 Administrator Control

When the Administrator Control option is used, the user cannot update his/her password with wpasswd or passwd (on UNIX). Only the administrator can change a user's password. The password will be changed in the system files once the profile is distributed to all levels.

The administrator can update the user's password by editing the profile or by using the wpasswd command. The administrator must have the admin authorization role.

A pre-expire option, when set to TRUE (check-box selected), will tell the user that his/her password needs to be changed. However, only the system administrator will be able to change the user's password.

6.1.8.3 Populating Passwords

Password information will be retrieved and stored in the user profile when populating from UNIX. However, the password will not be retrieved from Windows NT, NetWare and RACF.

6.1.8.4 Password Encryption

There are several methods used by TME 10 User Administration for password encryption.

- At the framework level:

When populating from UNIX, TME 10 User Administration stores the standard, one-way encrypted password into the user profile. Resetting the password via the GUI or via the `wpasswd` command stores the password encrypted with tas_encript(). This encryption method is used by TME 10; it is similar to Data Encryption Standard (DES) encryption.

For Windows NT, NetWare and RACF, the password is always encrypted using tas_encrypt().

- At the endpoint level:

  UNIX password are encrypted using the UNIX encryption. Windows NT and NetWare passwords are stored in NT and NetWare using their native encryption methods.

Therefore, "on the wire", all passwords are transmitted as UNIX encrypted or Tivoli's tas_encrypted.

6.1.9 User Profile Home Directories

A home directory is a place where users's files are stored by default. This home directory can be on a local system or on a remote system. The creation of a home directory is supported on UNIX and NetWare. It is not supported on Windows NT (even though the concept of home directory exists), and it is not supported on RACF.

However, it is possible to automatically create home directories in Windows NT. Refer to 6.4.4"Creating NT Home Directories" on page 223 to see how to automatically create Windows NT home directories when the profile is distributed.

6.1.10 Databases Used by TME 10 User Administration

TME 10 User Administration creates several databases to keep up with user and group records. These databases are:

- UserNameDB
- UID
- GroupNameDB
- GID
- LocatorDatabase

These databases are populated from user and group profiles and are used with the UserLocator application and with commands such as `wlsids` and `wlsnams`, which are commonly used in default and validation policies.

6.2 Managing UNIX Users and Groups

This section describes how to manage users and groups on UNIX with TME 10 User Administration. In this section, each UNIX system is maintaining its own user and group database that is Network Information Service (NIS) is not set up to centrally manage users and groups. This will be covered later in this document in Section 6.3, “Managing Network Information System Domains” on page 193.

For illustrating our examples, we used AIX systems. The functions described below should work in a very similar fashion on other UNIX platforms. However, we will highlight, as much as possible, differences between all the UNIX flavors.

All the operations are performed from the user marco’s desktop, launched from yb0240e (AIX V4.1.5 machine). Remember that marco is an administrator that has admin and senior roles on the TME 10 yb0240d-region.

6.2.1 Populating a User Profile

After creating a user profile within a profile manager, the profile needs to be populated with the users defined on the machines subscribing to that profile. This allows us to centrally control the users on these machines.

Remember that during a populate operation, it is possible to find accounts having the same login name on different machines. In this case the application compares the operating systems account types (UNIX, NT or NetWare):

- If the operating systems are different, the application merges the two accounts’ information into the same record. For example, if TME 10 User Administration finds an account john on an NT machine and an account john on a UNIX machine, it will generate a unique record for the login john, containing both the NT and UNIX information. For more information on how TME 10 User Administration merges two user accounts, refer to, “User Merge when Populating a User Profile” on page 140.
- If they are the same operating system account types, TME 10 User Administration does not populate the second user account and returns an error.

Let’s create a profile manager (AIX_Manager) containing the user profile AIX_Users and define the subscribers to that profile manager as shown in Figure 96.

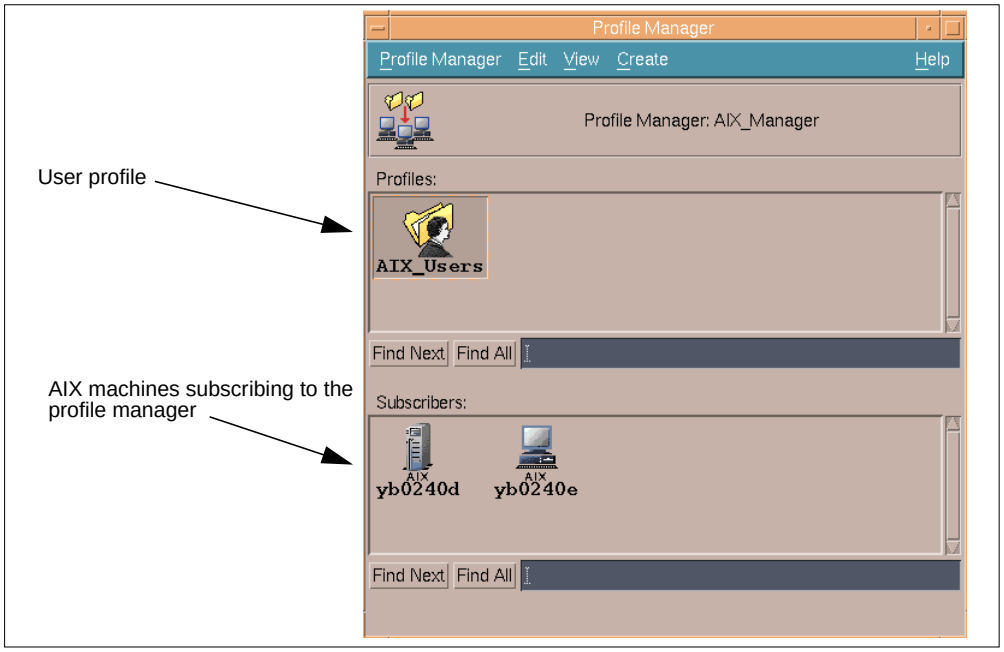


Figure 96. Profile Manager with two Subscribers

At this step the AIX_Users profile is empty. We need to populate it with the users defined in the subscribers yb0240d and yb0240e. Only records complying with the validation policies will be added to the user profile.

Before starting the operation, we are already sure that some error situation is going to occur because when the application finds two accounts with the same user name on the same type of operating system, it returns an error. In our case, we can be sure that this situation will occur at least for the standard AIX user accounts. Both machines have users root, daemon, bin, nobody, sys, adm, uucp, and lpd defined. For these users, only the first occurence of the user account will be populated. This is fine since these system users have exactly the same characteristics (same attributes).

However, you should check carefully all other users having a similar login name. These users can correspond to the same person or to two different persons. If they correspond to the same person, you might check the users attributes and see if they are the same or not. If they are not the same, the application will not merge them automatically; the first user account will be populated, and the second will be rejected. If the two user accounts do not correspond to the same person, you will need to modify the login name of one of the users account and populate again with the append option.

Now we can go ahead and double-click on the **AIX_Users** icon (or select **Open User Profile** from the icon's pop-up menu) to get the *User Profile Properties* window. Select **Profile**, then **Populate.** The following window should come up:

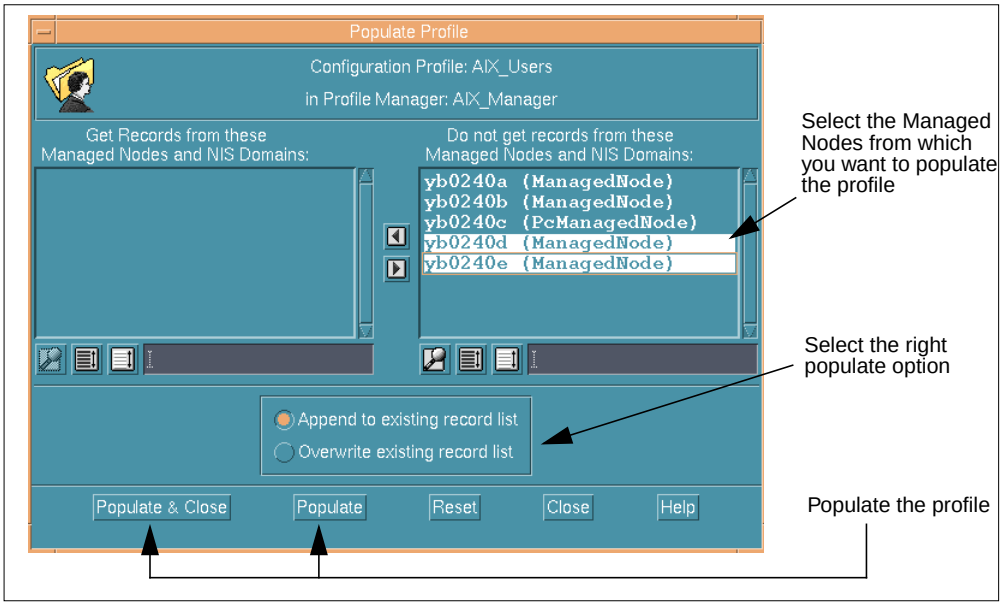


Figure 97. Populate Profile Dialog

Select yb0240d and yb0240e as managed nodes from which to retrieve user information. Choose the populate by pressing the appropriate radio button:

- **Append to existing record list:**

  This option adds user definitions retrieved from the managed nodes system files to the user profile. This option is very useful when you decide to populate a profile while keeping the records already defined in it. An example is when a new subscriber is added to the profile manager. You probably want to add the users defined on this managed node to your user profile and at the same time keep the records that already exist.

> **Attention!**
>
> If you try to add a record that already exists in the user profile, you will get an error. For example, if you have a UNIX user john in the user profile and another user john on a UNIX managed node from which you are populating, you will get an error window warning you that the user john (of the managed node) has not been added to the user profile.
>
> The information is successfully merged if the accounts belong to different operating systems.

- **Overwrite existing record list**:

  This option replaces the user records in the profile with the new records retrieved from the subcribers's system files.

> **Attention!**
>
> Be very careful when using this option because all existing records in the user profile will be lost and overwritten by the new ones. Be sure that your user profile does not contain relevant information before using this option.

When populating for the first time, we are not concerned by this option because the profile is empty.

Now, as shown in Figure 97 on page 159, click the **Populate & Close** button. You should get the following window:

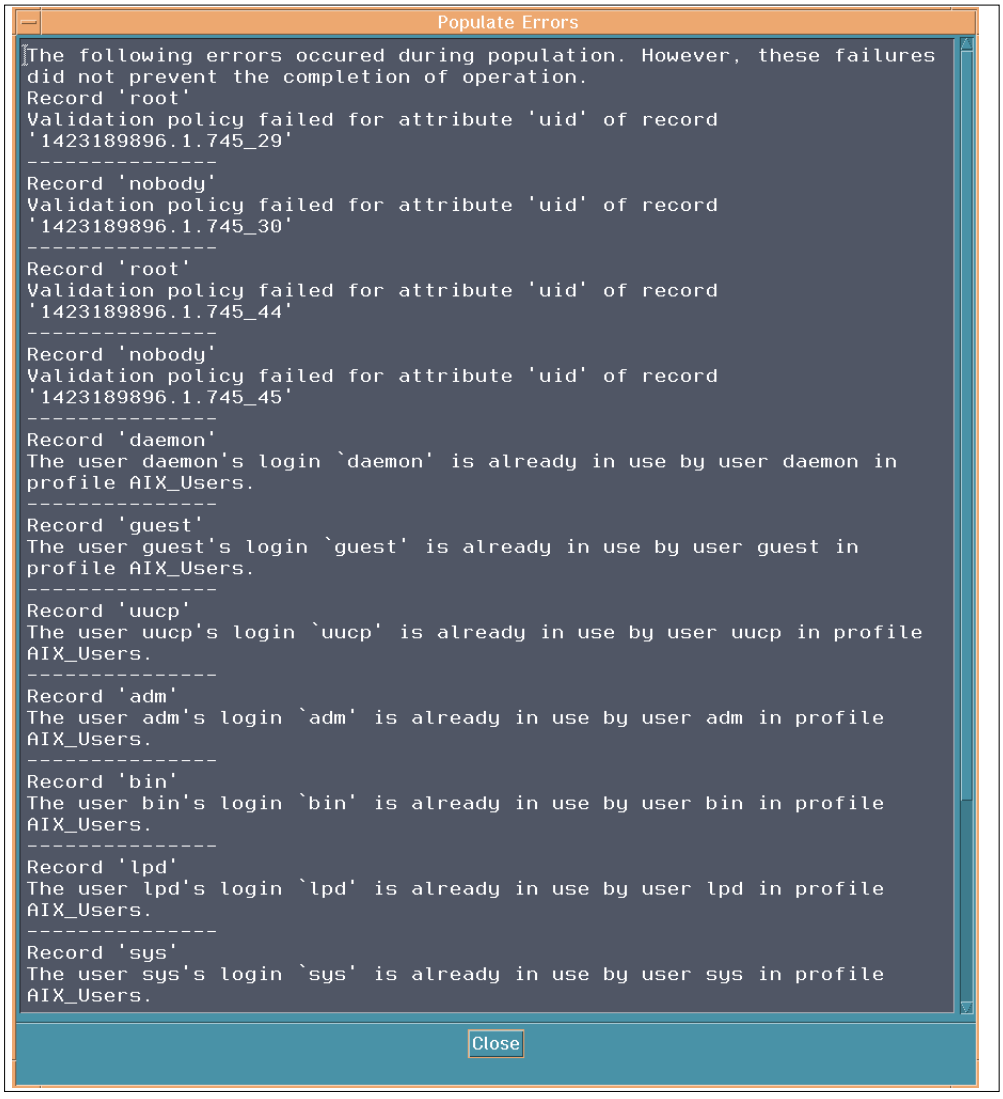


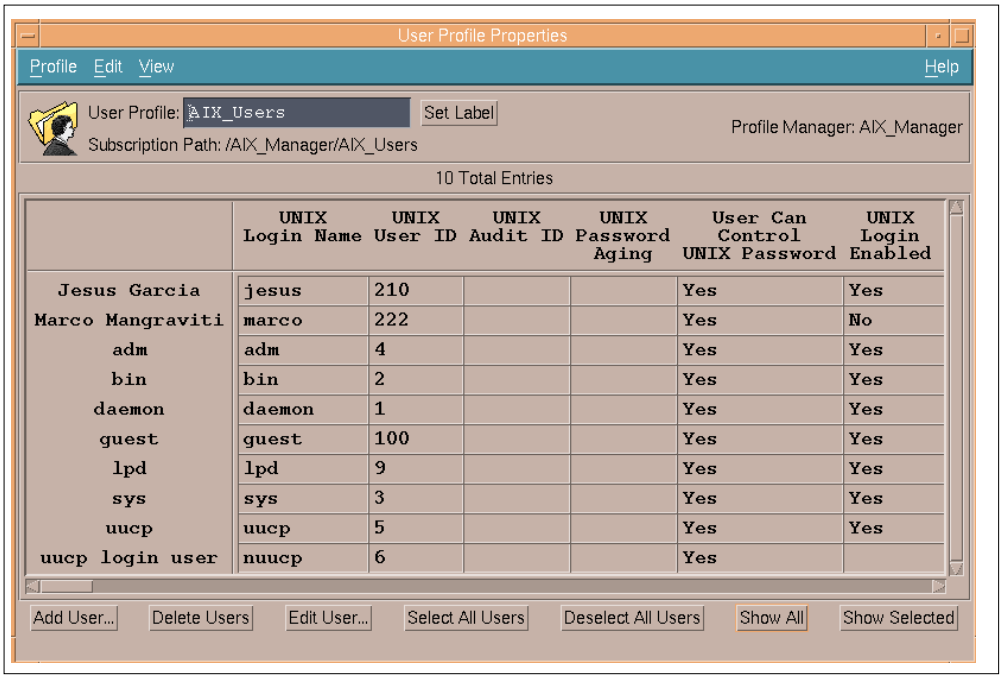
Figure 98. Populate Errors Window

In the first four entries the window warns you that users root and nobody have failed the validation policy and have not been added to the profile. In fact, the root UID is 0 and nobody UID is -2, but the validation policy checks for users with UID greater than 0.

If you want root or nobody to be included, you have to disable the validation policies or change them by editing the validation policies script. For more infomation on how to edit and change the validation policies, you can refer to 5.6.2.2, “Validation Policies” on page 138.

The other messages are error messages generated by AIX system users having the same login name (remember that the application uses the login name as a key to determine if there is a match between two systems).

The user profile is now populated as shown in Figure 99 on page 161.



	UNIX Login Name	UNIX User ID	UNIX Audit ID	UNIX Password Aging	User Can Control UNIX Password	UNIX Login Enabled
Jesus Garcia	jesus	210			Yes	Yes
Marco Mangraviti	marco	222			Yes	No
adm	adm	4			Yes	Yes
bin	bin	2			Yes	Yes
daemon	daemon	1			Yes	Yes
guest	guest	100			Yes	Yes
lpd	lpd	9			Yes	Yes
sys	sys	3			Yes	Yes
uucp	uucp	5			Yes	Yes
uucp login user	nuucp	6			Yes	

Figure 99. AIX_Users Profile after the Populate Operation

We find that all the users defined in the AIX machines have been added to the user profile. It is interesting to check the consistency of the profile against the system file, /etc/passwd, on the AIX machines. Let's consider the following figure:

Figure 100. /etc/passwd Files on Subscribers

You can see in Figure 100 that the system user accounts matches on the two systems. These means that you can ignore the populate errors for these user accounts.

Note: When the user profile is populated, TME 10 User Administration is not yet really managing those users. If you add, modify or delete a user from the profile, the endpoint systems will not be affected by this operation until you distribute the profile to these endpoints

Attention!

A serious problem can occur when populating from two machines having the same login name for two different users. For example, the user Kevin Smith is defined with user name kevin on yb0240d, and the user Kevin Taylor is also defined as kevin on yb0240e. In this case the second user will not be populated. If you do not pay attention to the corresponding error, you may loose Kevin Taylor's information. Thus, you need to carefully check all populate errors and analyze them. You might need to change Kevin Taylor's login name and eventually repeat the populate operation.

6.2.2 Merging User Records

TME 10 User Administration allows you to merge two user records. This is useful if a user has two different login name on two different system. Once the profile is populated, the users will have two different user records. The user information stored in the first record is treated as the master record. The second record is treated as a source record and is selectively merged into the master record (the terms *first* and *second* are referred to the order in which the records appear in the command line operation `wmrgusrs`).

About Merging

Merging user records is only possible from the command line. It is not possible from the desktop.

Once two records are merged, the source record is deleted from the profile. The records to be merged can be in the same user profile or in different user profiles.

Note

You cannot merge two records from two different profiles.

Remember that if the records to be merged are in different user profiles, such profiles must be in the same TME 10 Management Region, or there must be a one-way or two-way connection between these regions.

Let's consider the following example. Two accounts have been created for John Smith on the yb0240d and yb0240e AIX machines: john on yb0240d and johnny on yb0240e. We want to merge these user accounts into one account that will represent the user John Smith on both machines.

On the window shown in Figure 96 on page 158, double-click on the AIX_Users icon to open the user profile. Then from the User Profile Properties window, select **Profile**, then **Populate**. You are then prompted with the window shown in Figure 97 on page 159. In this case choose the **Append to existing record list** populate option, and the two AIX machines as endpoints from which to populate. Then click the **Populate and Close** button.

The User Profile Properties window will show two new accounts, john and johnny, belonging to the same user, John Smith:

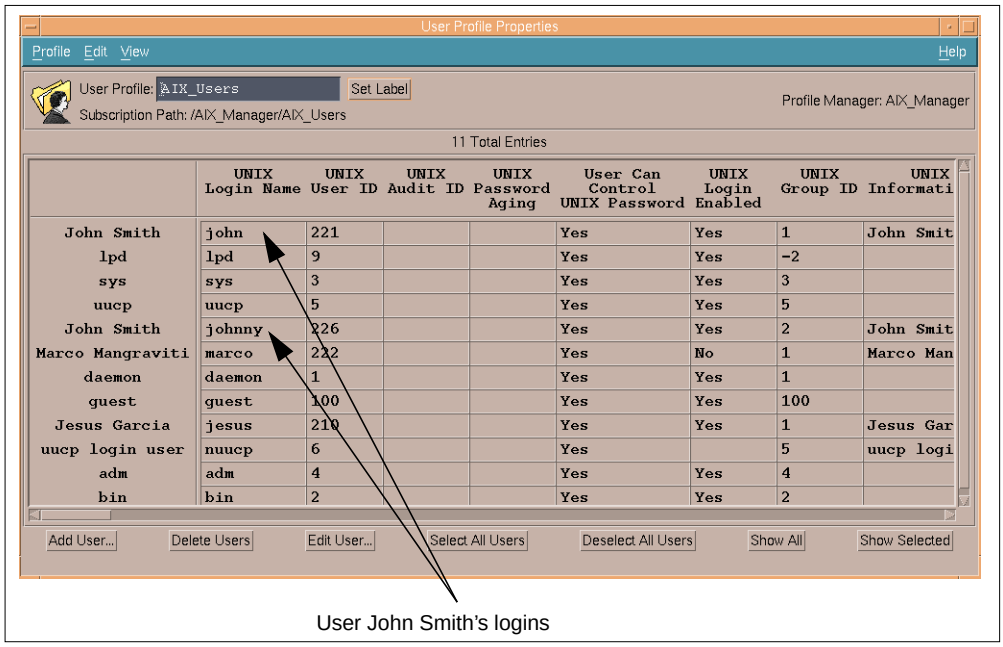


Figure 101. User Profile Properties Dialog

We need to establish a master and a source record. Remember that when the merging operation occurs, the AIX account information of the master record OVERRIDES the AIX account information of the source record. This means that if you have a C Shell interpreter for the master record and a Korn Shell interpreter for the source record, at the end of the merging operation you will have the common account with a C Shell interpreter. If you the master record has UNIX account information only and the source record has for example both UNIX account and NT account information, the master record overrides the UNIX account information in the source record and the NT account information from the source record is added to the master record.

To merge the records you must to use the `wmrgusrs` command. This command has two options: `-d`, that allows you to delete the home directory of the source user record when the profile is distributed back to the endpoints, and `-l`, that allows you to leave the home directory of the source user record.

Note

The `-d` and `-l` options of the `wmrgusrs` command are are specific to UNIX accounts.

We select the user account john as the master record, and issue the following command:

```
wmrgusrs -l @UserProfile:AIX_Users john @UserProfile:AIX_Users johnny
```

Figure 102 shows the output of that command:

```
#wmrgusrs -l @UserProfile:AIX_Users john @UserProfile:AIX_Users johnny
User 'johnny' has been successfully merged into user 'john' in profile
@UserProfile:AIX_Users.
```

Figure 102. Merge Operation Output

Now we can check the effect of the merge operation on the user profile. Open the User Profile Properties dialog, the following window should appear:

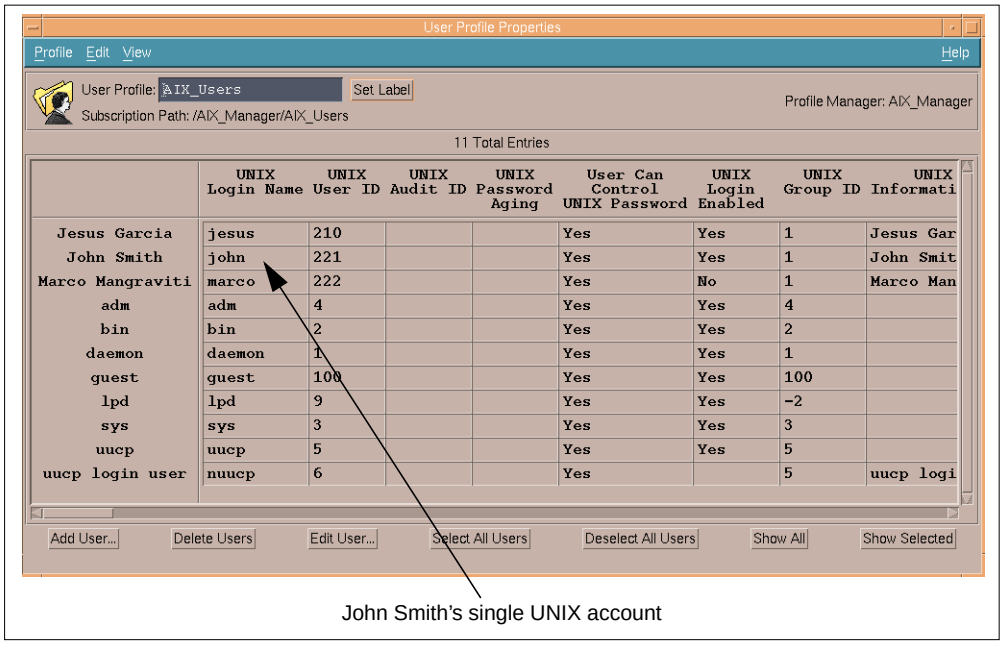


Figure 103. AIX_Users Profile after the Merge Operation

Tip

If your User Profile Properties window does not show up the result of the merge operation, you might need to select **View**, then **Refresh**.

The last step is to distribute the user profile in order to make effective the modifications performed on it.

Note that if you want the user johnny to retrieve his directories and files, you might need to change the ownership of all directories and files he owned on the machines where he was defined.

6.2.3 Distributing a User Profile

After creating new user records, editing existing user records or deleting user records and in general after performing any operation on the user profile, you need to distribute the user profile to the endpoints to make effective the user administration operations you performed. Once the profile has been distributed to all subscribers levels, the system files at systems are really up-to-date, and the user's home directories (local to host or remotely mounted) are created.

Before continuing to explain the distribute function, it is useful to clarify some important concepts. The User Profile Properties window shows the content of the AIX_Users profile. This profile is the top-level user profile. We called it top level because that user profile is kept at the profile manager level. It is the original version of the profile. After distribution, a copy of this profile is kept at the subscriber level. In the rest of this chapter, we will deal with three types of data:

- The top-level user profile (the original version of the profile)
- The copy of the user profile at the subscriber level
- The system files (for example /etc/passwd)

Figure 104 shows the simplest possible hierarchy, which is made up of a user profile and one level of subscribers.

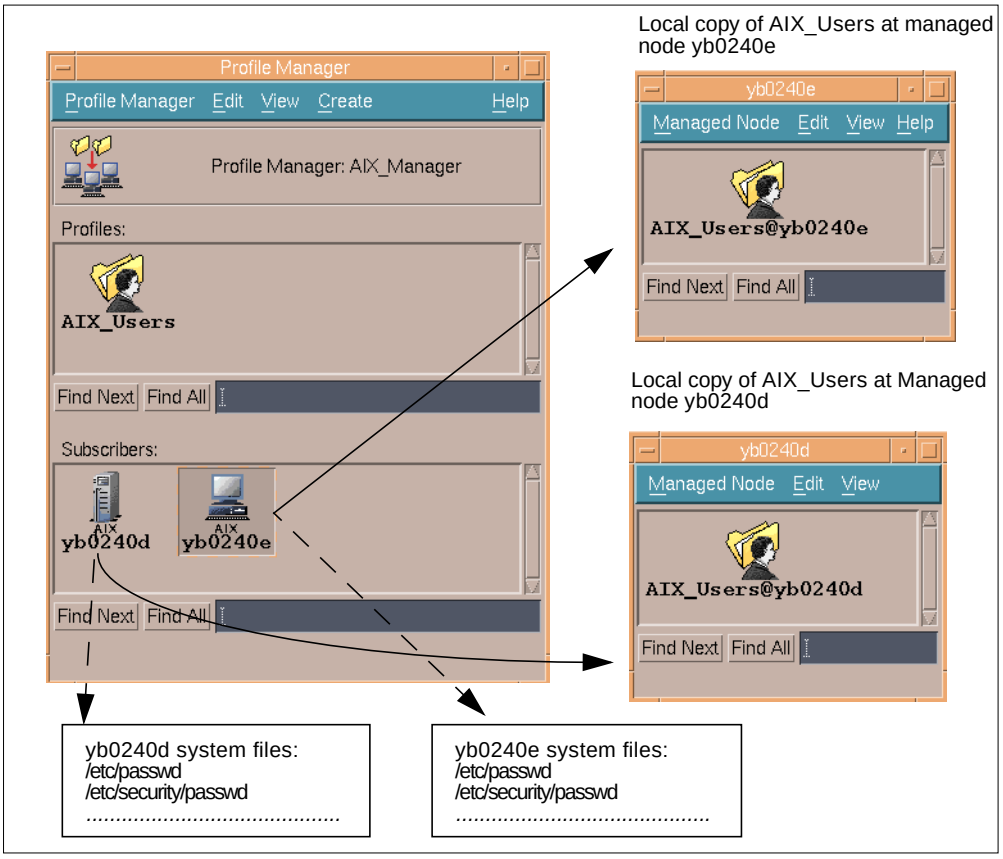


Figure 104. A Simple Profile Manager Hierarchy

In our example you can see the top-level user profile AIX_Users, and two local copies of this profile, AIX_Users@yb0240e and AIX_Users@yb0240d.

Having a copy of the profile at the subscriber level allows a local administrator to perform some customizations on these local copies and eventually distribute them to the system files. We could, for example, define an administrator for yb0240e and an administrator for yb0240d responsible for setting only some specific user attributes on these machines.

Before distributing a profile, we need to understand what type of distribution to perform:

- A distribution that updates only the copies of the user profile stored at the subscribers.
- A distribution that updates the local copies of the user profile AND the sytem files on the target machines.

Note

These concepts are valid even if the subscriber is another profile manager. In this case it is possible to:

- Distribute a copy of the profile to the profile manager without sending a copy to the managed nodes that subscribed to this profile manager.

or

- Distribute a copy of the profile to the profile manager AND to the subscribers of the profile manager AND at the same time update the subscribers system files

In our example, from the User Profile Properties menu, click on **Profile**, then on **Distribute**. The following window will appear:

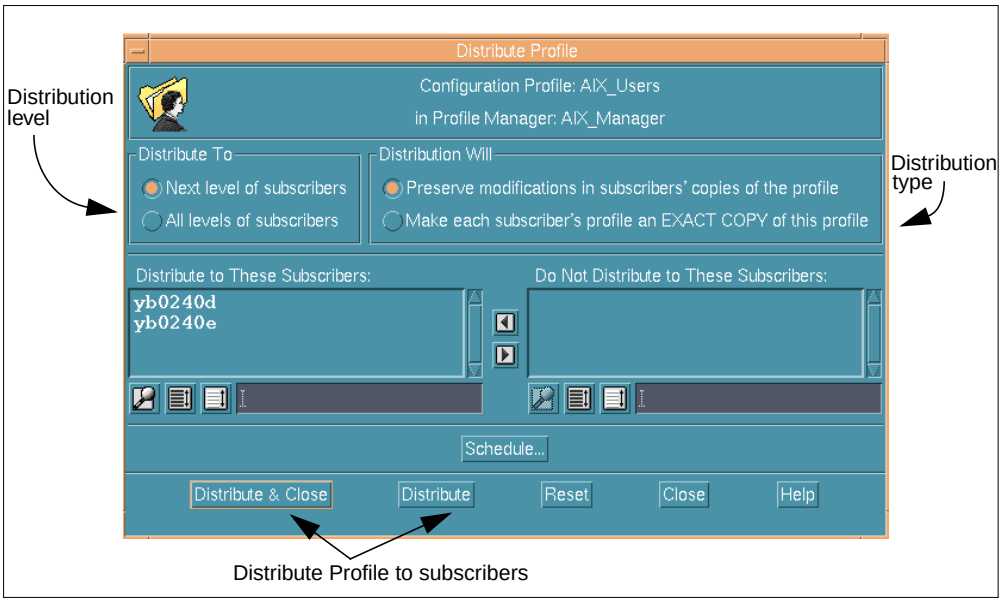


Figure 105. Distribute Profile Dialog

We can choose to distribute the top-level user profile to the **Next level of subscribers** or to **All levels of subscribers**.

By choosing the **Next level of subscribers** radio button in the Distribute To field, you send a copy of the profile to the next level of subscribers, creating a copy of the profile at the subscriber level, but NOT UPDATING any system files on the managed nodes.

Note

In our example the next level of subscribers is the managed node level. In this case the profile is distributed only to the managed nodes, and the actual system files are not modified. This means that we will get a copy of AIX_Users distributed to AIX_Users@yb0240e and to AIX_Users@yb0240d.

The only way to update the system files if you used the Next level of subscribers option is to distribute the profile from the managed nodes themselves. In our example this means to open the managed node icon (double-clicking on it or from its pop-up menu), open the AIX_Users@yb0240e or AIX_Users@yb0240d icon and distribute to the next level of subscribers.

The **All levels of subscribers** option sends a copy of the user profile to the next level of subscribers. If a subscriber is a profile manager, it also sends a copy to the profile manager's subscribers. Also, all the system files are updated. Therefore, this option changes all of the lower-level copies of the profile in the hierarchy. So if you want to get both the copies of the profile and the endpoints system files updated, choose the **All levels of subscribers** radio button.

The second important choice is the distribution type:

- **Preserve modifications in subscribers' copies of the profile:** Select this option if you want to keep all the changes that a local administrator might have made to the local copy of the user profile.
- **Make each subscriber's profile an EXACT COPY of this profile**: Select this option if you do not want to keep any local customization made in the user profile at the subscriber's level.

Attention!

The danger with the Make each subscriber's profile an EXACT COPY of this profile option is that the user profile you are distributing can contain a subset of the users defined on the system. Thus, making an exact copy of the user profile will delete users.

The choice of the subscribers to which distribute the user profile can be defined on a user-by-user basis. In fact the list of subscribers is a common attribute of the user. The Subscriber Information option allows you to choose the endpoints which distribute a given user. From the User Profile Properties window shown in Figure 103 on page 164, double-click on the user to which you want to set a list of subscribers. The following window appears:

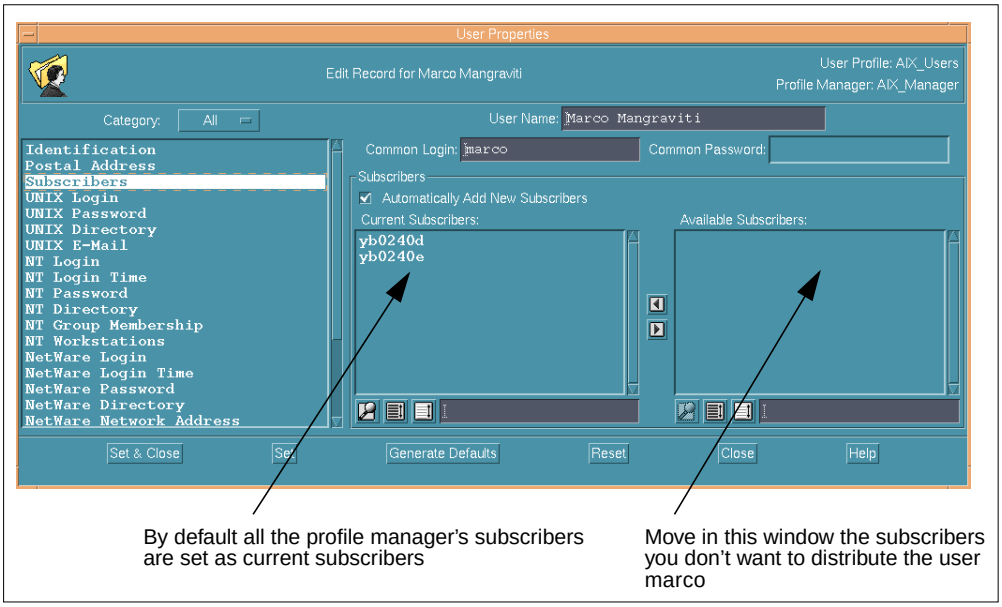


Figure 106. Subscribers For User marco

You can move a subscriber from the *Current Subscribers* list to the *Available subscribers* list. This operation prevents the record of a given user to be distributed to the subscribers not belonging to the *Current Subscribers* list. The checkbox above the *Current Subscribers* list sets the user attribute *Subscribers* to automatically add new subscribers as they are added. It may be disabled if you don't want the user profile automatically distributed to every new subscriber.

A Note About Scheduling

The distribution of a large user profile made up of, for example, 200 users will probably need to be scheduled overnight or in light workload periods. By simply clicking on the **Schedule** button on the Profile Distribution dialog, you are prompted with the Schedule Job window.

Attention!

The amount of time required to distribute a user profile depends upon the size of the system configuration file. During a distribute, the system file is essentially populated into a temporary table; then the contents of the distributed profile are merged into the table. Finally, this table is written out to the system file. So distributing (with the preserve modifications option) a profile with one user to a system file containing 2000 user records could take more time than you might expect.

6.2.4 Adding, Editing and Deleting Users

This section explains the steps necessary to add user records to a profile and edit UNIX attributes for that user record.

6.2.4.1 Adding a User

Adding a user account begins with adding a user record to the user profile, then distributing that profile in order to create the user's account on the UNIX systems that you are managing. From the User Profile Properties window, click on the **Add User..** button to get the following window:

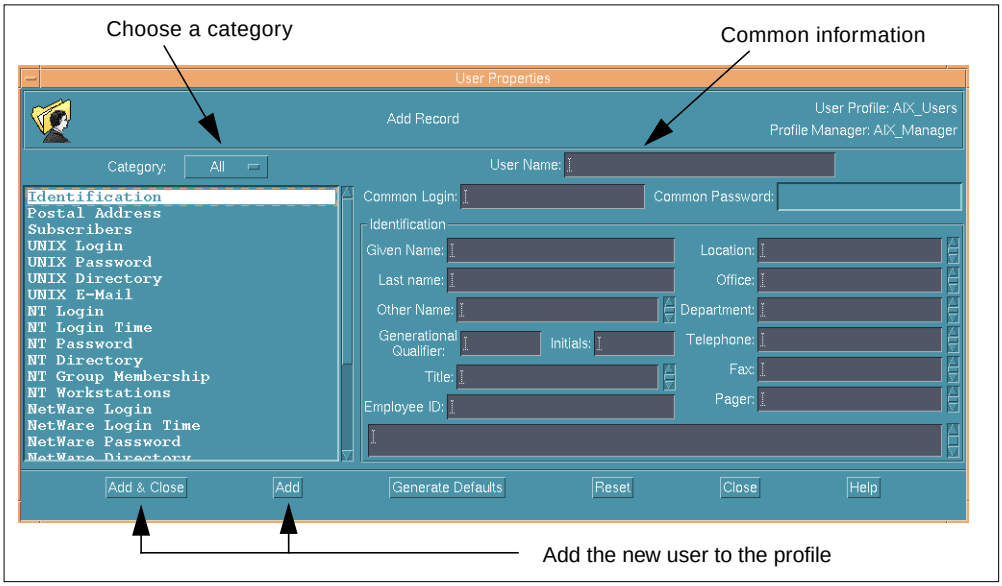


Figure 107. Add Record Window

Several fields can be filled out at this step. The following sections describe those fields.

Common User Information

Figure 107 on page 169 is the main window you get when adding a user record. By choosing a category from the *Category* list, you can narrow the number of choices in terms of operating system attributes.

An important product feature is that you can define in a single action all the possible user attributes: general, UNIX, NT and NetWare. This means that you can define the user once for all platforms, and if that user needs access to systems of multiple types you can administer the access in a centralized and consistent way. You can simply enter the user name in the User Name field and click on **Generate Defaults** to have a common user login defined on UNIX, Windows NT, Netware and RACF.

Note About RACF

RACF does not provide default policies in this release (3.1) of TME 10 User Administration.

This new user will have the attributes set according to the default policies. Simply by editing the default policies, the administrator can set common conventions for every new user he/she will add to the user profile. It is possible, for example, to establish a consistent naming convention that avoids login name duplications.

In general, when you create a new record to a profile, you can:

- Manually fill out all the fields corresponding to user attributes
- Use default policies to generate defaults attributes values
- Do both

UNIX Login

Let us consider the specific case of a UNIX user creation. We assume it will be named Mike Smith, with login name mike. We want to set only some attributes for this user: UID, Login Name, Shell, Password, E-Mail and home directory, and use the default values for setting the remaining attributes.

Note: If you just want to create a UNIX user account and not fill out all the default attributes for Windows NT or NetWare, you can disable default policies for Windows NT and NetWare with the `wsetdefpol` command:

```
wsetdefpol DISABLED NT AIX_Users

wsetdefpol DISABLED NW AIX_Users
```

If you choose **UNIX** from the Category list, you will be prompted with the first UNIX specific dialog: the **UNIX Login,** as shown in the following figure:

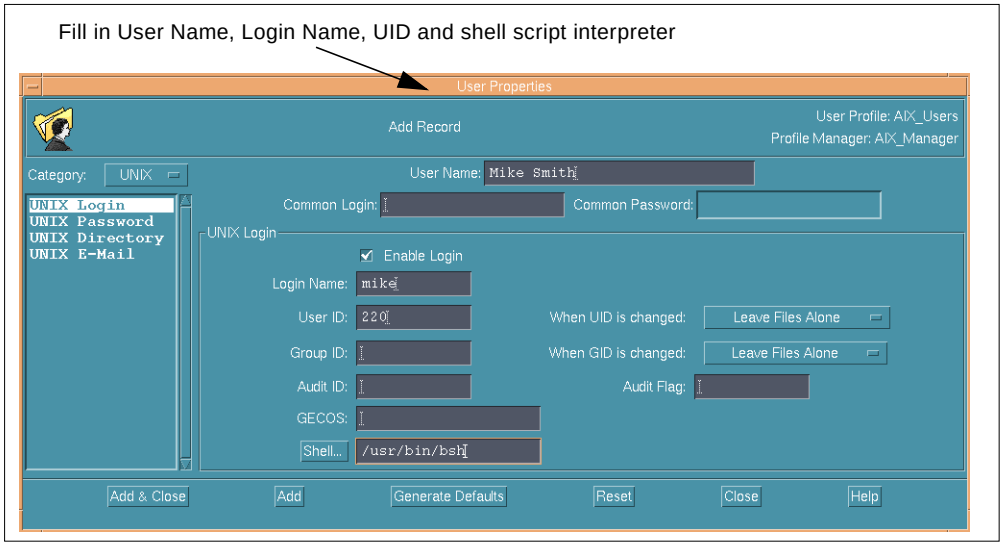


Figure 108. UNIX Login Window

In our example, we choose to have a Login Name=mike, UID=220 and to use the Bourne Shell interpreter. It is also possible to perform the following operations:

- Enable or disable the UNIX login
- Enter the user real name in the GECOS field (TME 10 User Administration uses the information in this field as the user's real name if there is no default policy set).
- Enter the audit identification number for the user. This information is only used by HP-UX running C2 security.
- Enter the value for the audit flag (1 enables and 0 disables auditing for this user).

UNIX Password

The next option in the Category scrolling list for the UNIX operating system is the *UNIX Password*. If you select **UNIX Password** you will get the following window:

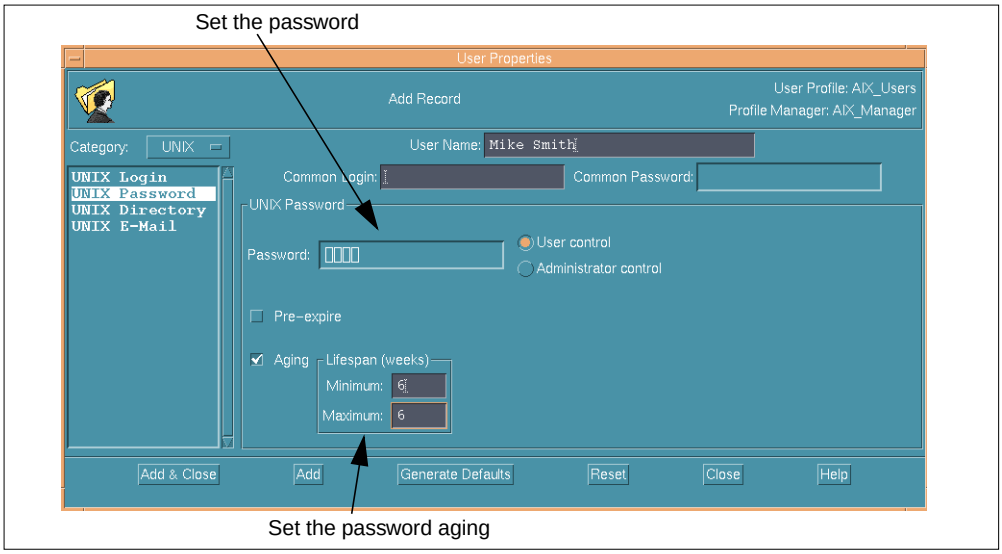


Figure 109. UNIX Password Window

We decided to set a password active for six weeks by entering the password minimum lifespan and the password maximum lifespan. You could even choose to activate the password pre-expiration. When pre-expiration is set, the first time the user logs in after you distribute the user profile, the user will be prompted to change his/her password.

By choosing a password aging of six weeks, you prohibit the new created user from changing his/her own password before this time is elapsed. Practically, this means that if the user mike attempts to change the password issuing `passwd` on his system, he will receive the following message from the operating system:

```
A minimum of 6 elapsed weeks between changes, 3004-709 Error changing password
for "mike"
```

Another important consideration is that by selecting the **User control** radio button the user password can be changed only if:

- The user changes his or her own password.
- The administrator changes the user password in the user profile and distribute it to the subscribers.

If the user has user control, the user can change his password in two ways.

- He can use the `passwd` command. This will change the password on the system he is working on, but will not change the password in the copy of the user profile at the subscriber level and will not change it in the top-level profile.

  Note that in this case, the new password stored in the system files will not be overwritten by a distribution of the profile, even with the option Distribute to All levels.

- He can use the `wpasswd -l` command. This will change the password in both the system files and in all the user profiles where this user is defined.

By selecting the **Administrator control** radio button, the user password may only be changed if the administrator distributes a profile with a new password. A user attempt to change the password with the `passwd` command will produce the following output:

```
You are not authorized to change "mike's" password
Error changing password for "mike" : You do not have permission
```

Figure 110. Error Output Using the passwd Command

Therefore the user is not enabled to change the password.

A similar error message will show up if the user tries to change the password with the `wpasswd` command.

```
wpasswd
Old password:
New password:
Retype new password:
The password was NOT changed for user mike in the user profile AIX_Users:
-->  The modification of the password for the user mike in user profile AIX_Users
has failed because the user is not allowed to modify his/her password in that
profile.
The password was NOT changed for user mike in the user profile AIX_Users:
-->  The modification of the password for the user mike in user profile AIX_Users
has failed because the user is not allowed to modify his/her password in that
profile.
The password was NOT changed for user mike in the user profile AIX_Users:
-->  The modification of the password for the user mike in user profile AIX_Users
has failed because the user is not allowed to modify his/her password in that
profile.
The password was NOT changed for user mikein the user profile AIX_Users:
-->  The modification of the password for the user mike in user profile AIX_Users
has failed because the user is not allowed to modify his/her password in that
profile.
Password could not be changed in some profiles.
```

Note About Password Setting

If you populate a profile or if you create a new user, the first distribute writes out the password. After that, distribution should not change the password unless:

- The password is changed in the profile via the GUI by the administrator and the profile is distributed
- The password is changed by the administrator with the `wpasswd -l` command or the `wsetusr -p <password>` command.
- The password is changed by the user with the `wpasswd -l` command.

Attention!

You might want to replace the `passwd` command with the `wpasswd` command to avoid retraining users to use the `wpasswd` command instead of the `passwd` command.

We do not recommend replacing the `passwd` command with the `wpasswd` command.

This is NOT recommended at all for several reasons:

- `wpasswd` will not run if the oserv daemon is not running on the local host or if the TMR server is down.
- You may need to change the UNIX passwords when the host you are working on is in single-user mode
- You may need to change the UNIX password when the oserv daemon is down

Replacing `passwd` with `wpasswd` would required to develop a very clever script that would need to:

- Do the right thing if the oserv daemon is down
- Do the right thing if the system is in single-user mode
- Do the right thing if the TMR connection is down (in the case the TMR is connected to another central TMR)
- Handle local accounts not managed by User Administration such as root, kroot
- Handle expired passwords issues as well as logging in issues
- Do the right thing if invoked by a Tivoli administrator who did not have admin role for the user profiles. How would he change his own password?
- Do the right thing if the UNIX password and the Tivoli password were different
- Handle properly interrupts

This list is not exhaustive. In summary, `wpasswd` is not designed to replace the `passwd` command.

Home Directory

The next step is to set the user' home directory. We choose to have it local to the host (you may choose a remotely mounted home directory) at `/home/mike`. Select **UNIX Directory** from the Category scrolling list to get the following window:

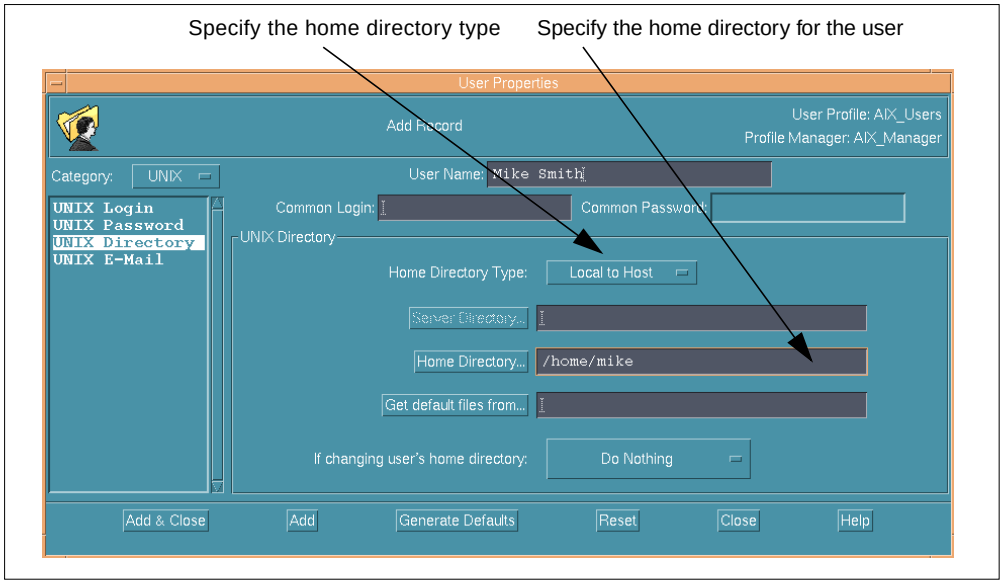


Figure 111. UNIX Directory Specification Dialog

We set the **Home Directory Type** to *Local to Host,* note that this option will automatically create the home directory on the AIX machine when the profile is distributed to all levels of subscribers. The home directory is created when the system files are updated. With the option **Get default files from..** you can specify a directory from which to get the defaults file for a new user, for example a customized .profile, .Xdefaults and so on.

Note About Remotely Mounted Directory

If you distribute a user record to the next level of subscribers with the **Remotely Mounted** home directory option, the directory for that user is created on the server machine even though the system files are not yet updated.

E-mail

The next step is to set the user's E-mail. Select **UNIX E-Mail** to get the following window:

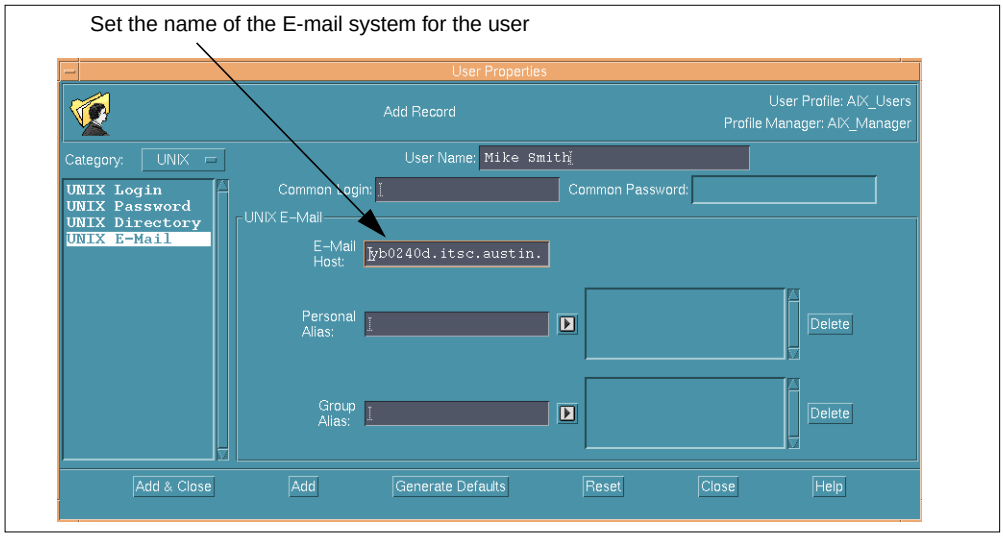


Figure 112. UNIX E-Mail Dialog

We set the name of the system on which the user will receive E-mail to yb0240.itsc.austin.ibm.com. Note that no default value is provided for this attribute (see the script body of the default policy). The only way to set an E-mail system is to enter the name in the field when the user is created or to change the default policy by editing the script. We could even select a personal or group E-mail alias for the user.

Other Attributes

The last step is to set values for attributes we did not manually edit. You can do this by simply clicking on the **Generate Defaults** button.

When all the attributes are set up, just click on the **Add & Close** button to have the new user added to the profile.

Note About Records Creation

When you click on the **Generate Defaults** or **Add** button, the default policies are applied to get the attributes values. The only time these policies are not applied is when you have already entered a value for an attribute (that value will not be overwritten by the default value) or set the default policies to *None*.

The only REQUIRED value to specify for a new record is the *User Name.*

6.2.4.2 Editing a User Record

The same procedures used to set the new user properties may be applied to edit an existing user. You simply need to select the user and click on the **Edit User** button or double-click on the row corresponding to the user record in the User Profile Properties window.

6.2.4.3 Deleting a User

To delete a user, you must select the user record in the User Profile Properties window and then click on the **Delete User** button. When performing this operation, you will be prompted with a window that allows you to delete the user's

home directory or to leave the user home directory as is when the profile is distributed. Obviously, the user information is not updated in any subscriber's system files until you distribute the profile.

Note About Remotely Mounted Directory

If the user home directory is a remotely mounted home directory and if you choose the Delete Home Directory option, the home directory will be deleted even if you only distribute to the next level of subscribers.

6.2.5 Synchronizing System Files with User Profiles

If a system administrator, having root access to a UNIX machine, adds or deletes a user on the system, the user profile will no longer be directly consistent with the system files that it manages. The synchronize function provides a way to keep the consistency between a user profile and system files by showing you which records do not match the system files entries. The synchronize function allows you to modify the user profile to match the system files.

About Synchronization

The synchronize function, accessible from the desktop, updates the endpoint's copy of the user profile. Do not expect it to update the top level user profile, because this is another operation that is documented later in this chapter.

Let us consider the following example:

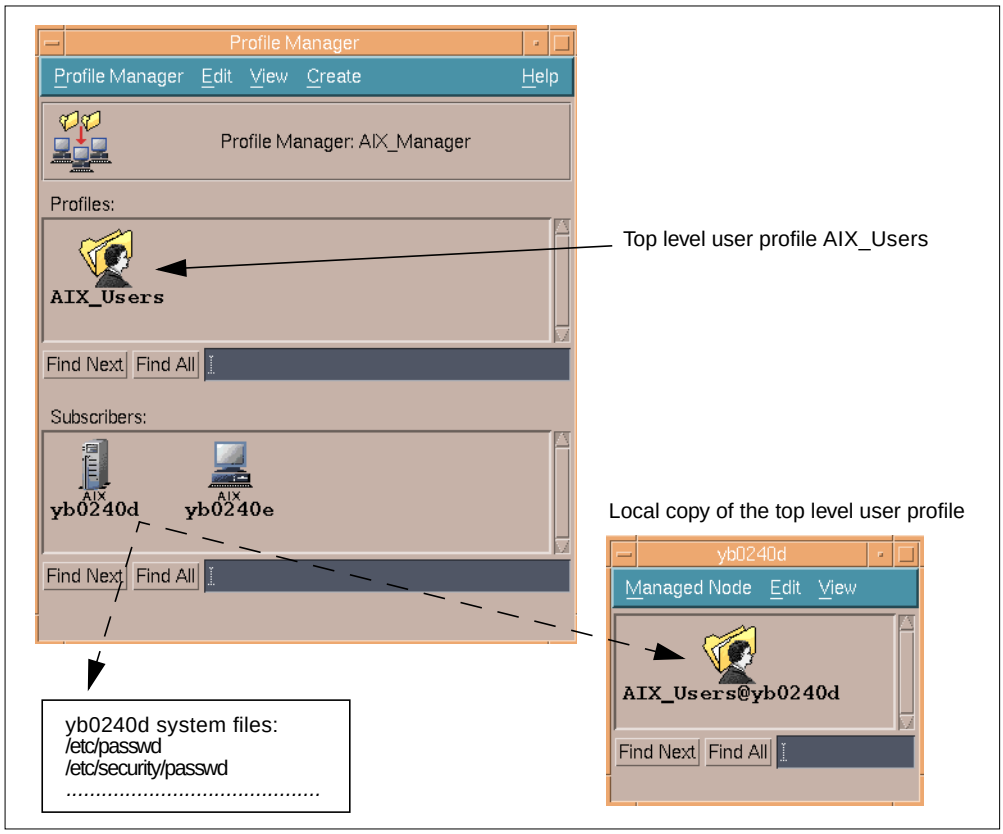


Figure 113. Synchronizing a User Profile

If a system administrator adds a new UNIX login directly on machine yb0240d, the system file /etc/passwd has one more entry than the AIX_Users@yb0240d user profile. The synchronize function allows you to reconcile that.

Attention!

TME 10 User Administration synchronization does not synchronize user passwords, since passwords are usually managed by users.

After manually adding the new user, in our case auditor, the /etc/passwd file on yb0240d is updated with the new user entry. Therefore we have a discrepancy between the system files and both the local user profile and the top level user profile.

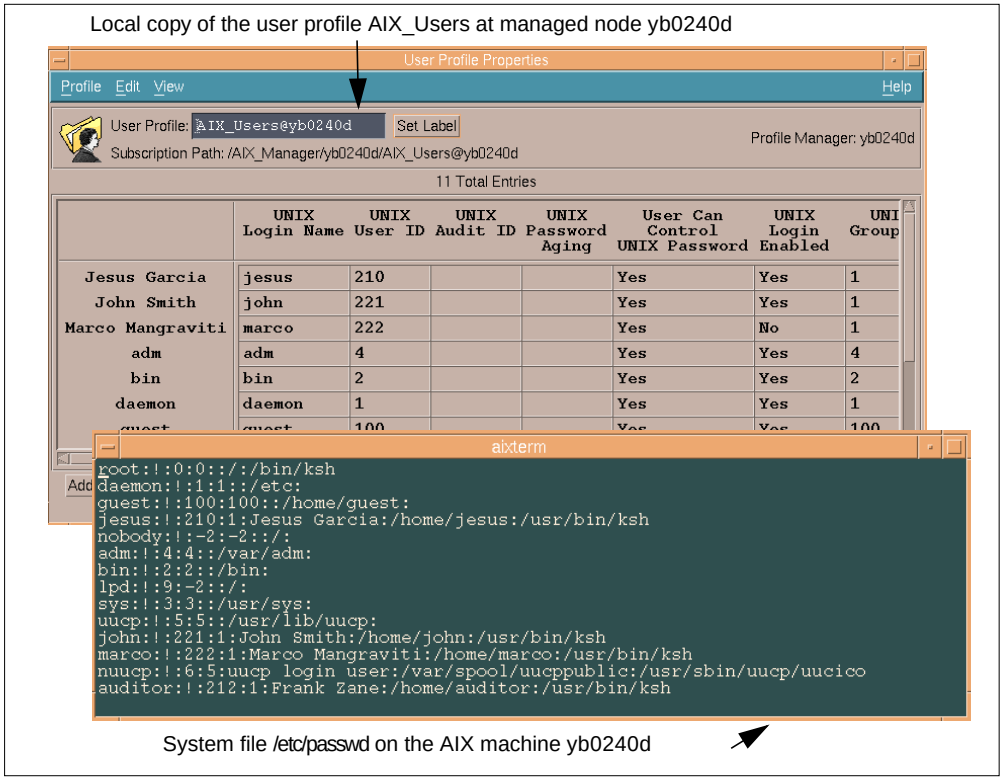


Figure 114. Local Copy of User Profile vs. System File /etc/passwd

To synchronize /etc/passwd with AIX_Users@yb0240d, select **Synchronize** from the managed node's icon pop-up menu or from the local User Profile Properties pull-down menu. You will get the list of all the profiles available for the managed node.

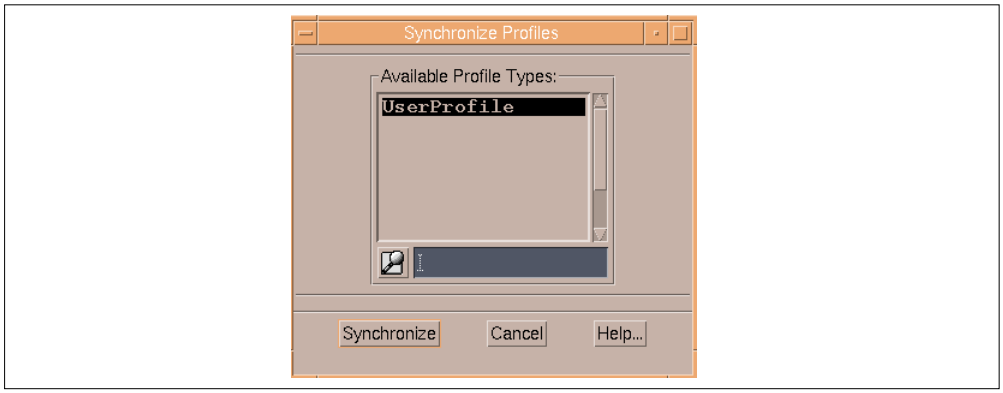


Figure 115. Available Profiles for the Managed Node yb0240d

A managed node may have many available profile types. It may be a subscriber of user profiles, group profiles, sentry profiles and so on. In our case we have only one available type of profile.

A Note about New Subscribers

If you add a managed node to a profile manager by putting it in the list of subscribers, you may expect to have already a copy of the profiles on this managed node. This is true only AFTER you distribute the profiles to that managed node. Before distribution, no local copy of the profiles is stored on the managed node.

On Figure 115, click on the **Synchronize** button to get the discrepancies between the user profile and system files, as shown in the following window:

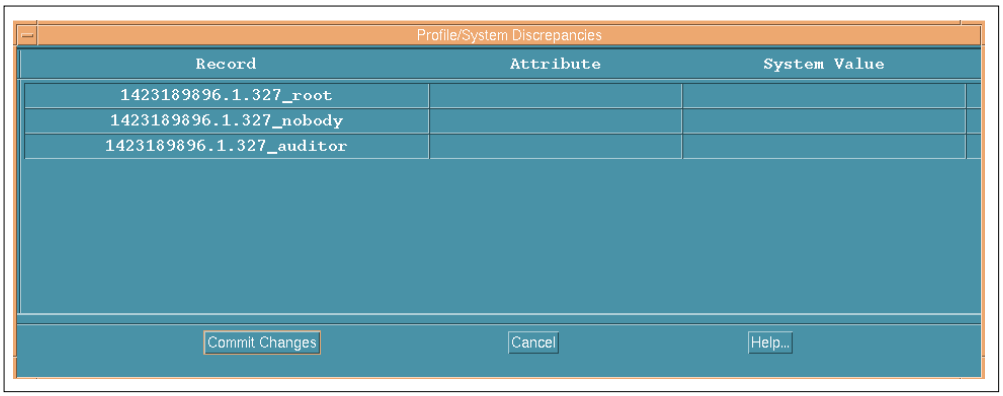


Figure 116. Profile/System Discrepancies Window

We find in this window the users root and nobody. This is normal since these two users were not added to the user profile when we populated it, because they did not pass the validation policies. We also find the manually added user auditor. You can click on the **Close** button and make the changes by manually adding the user to the user profile or click on the **Commit Changes** button to copy the system files information into the user profile. Click on **Commit Changes** to get the following window:

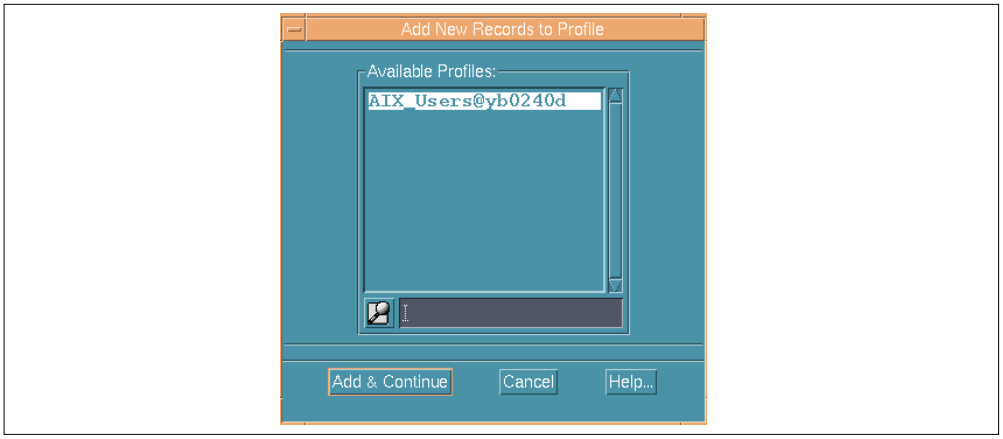


Figure 117. Add New Records to Profile Window

This window allows you to choose the user profile to update. Select **Add & Continue:**

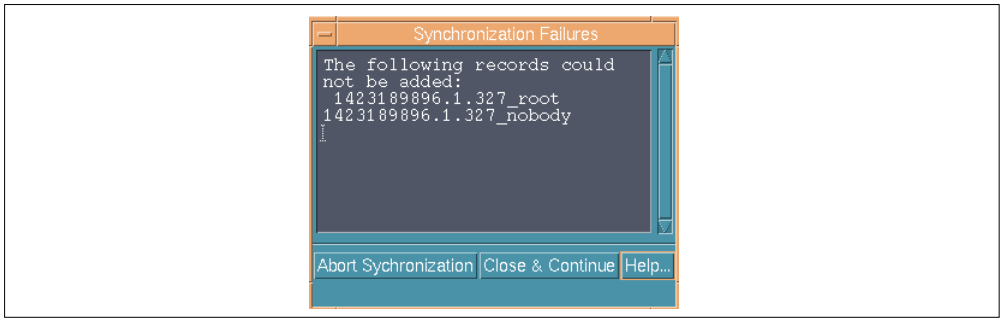


Figure 118. Synchronization Failures Window

This window warns you that users root and nobody have not been added to the user profile (because as in the population operation, the validation policy prevents us from adding these users). Press **Close & Continue** to finish the operation. The AIX_Users@yb0240d is now updated with the user auditor as shown in the following figure:

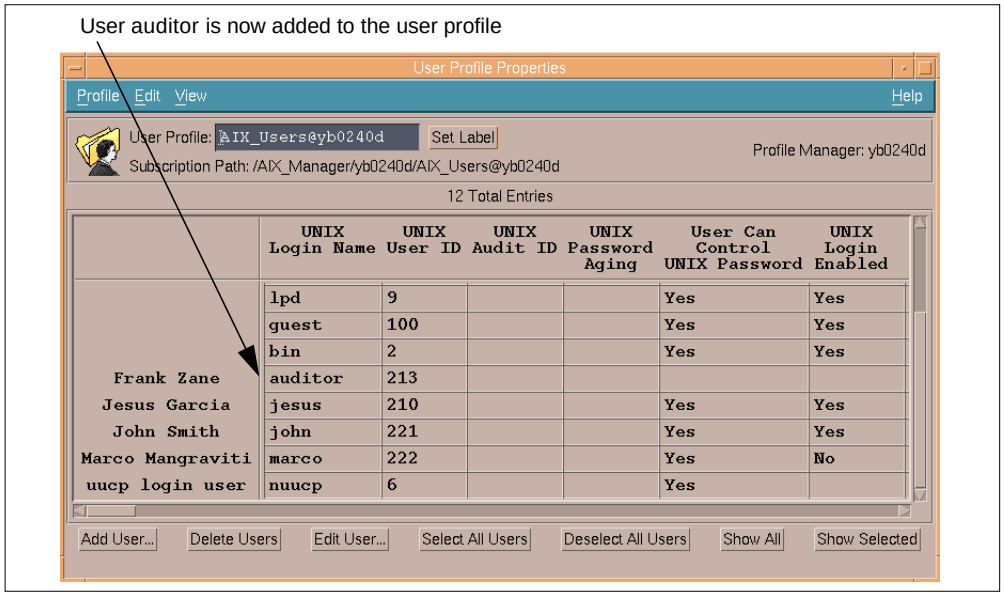


Figure 119. Updated AIX_Users@yb0240d User Profile

Attention!

We noticed that users added into the AIX system files without specifying a GECOS name are not synchronized.

The **Synchronize** command allows you to keep consistency between system files and a local copy of a profile. To give the top level administrator an updated view of the subscribers' system files, you might want to keep consistent the copy of the profile at the subscriber level and the top level profile.

The top level user profile update must be performed by using the command line. This operation cannot be performed from the GUI. Let us consider the previous example. What we want to do is to add the user auditor to the top level user

profile AIX_Users in the profile manager AIX_Manager. To do that, issue the following command:

```
wchkusrs -s @UserProfile:AIX_Users -u @UserProfile:AIX_Users
@ManagedNode:yb0240d
```

where :

`-s` is to specify the source profile (the profile to compare with the system files);

`-u` is to specify the profile to update (it may be different from the source profile);

`@ManagedNode:<Managed_Node_Name>` is to specify the subscriber to synchronize with.

By issuing the command, we get the following output:

```
#wchkusrs -s @UserProfile:AIX_Users -u @UserProfile:AIX_Users @ManagedNode:yb0240d
Checking endpoint @ManagedNode:yb0240d..
These users were found in the system but not in the database:
root
nobody
auditor
The following records in the profile @UserProfile:AIX_Users could not be modified
or added:
root
nobody
These differences have been updated in the profile
```

Figure 120. Updating the Top Level User Profile

Once again we find that users root and nobody have not been added, which is normal according to the validation policies. The user auditor has been successfully added to the top level user profile, as shown in the following figure:

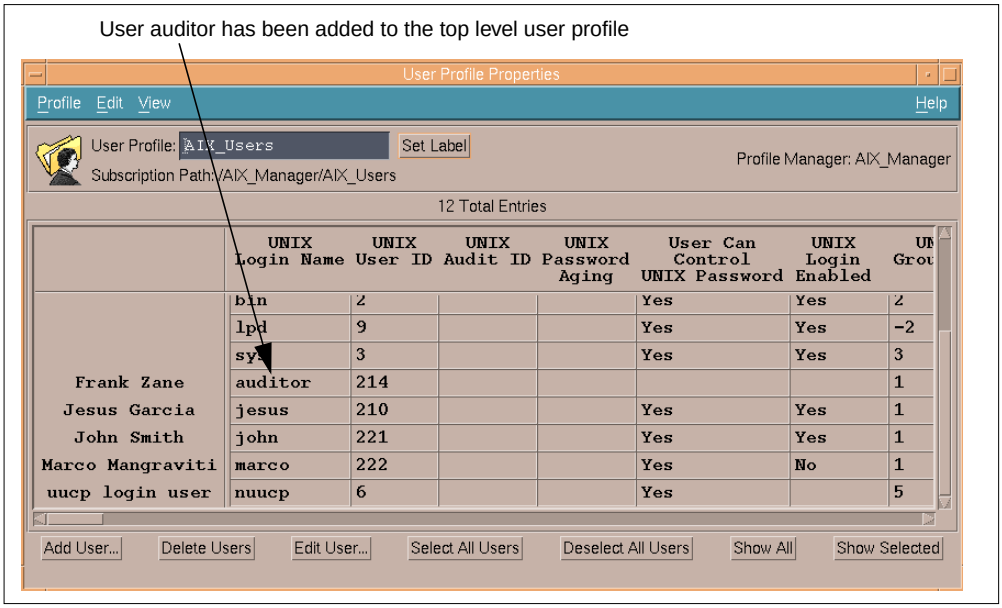


Figure 121. Top Level User Profile after Update

6.2.6 Setting Up a Group Profile

As the user profile, the group profile must be added to a profile manager and added to the Policy Region as a Managed Resource. We find again a set of default policies and a set of validation policies. Default policies define default values used when you create a new group profile record; validation policies specify allowed values when you create or modify a group profile record.

A Note About the Product

TME 10 User Administration only manages UNIX groups with group profiles. Windows NT groups and NetWare groups are not supported.

We created a new group profile in the profile manager AIX_Manager, as we did for the user profile.

6.2.7 Populating a Group Profile

After creating a group profile, you can populate it from endpoint systems with existing groups. Let us consider the following example:

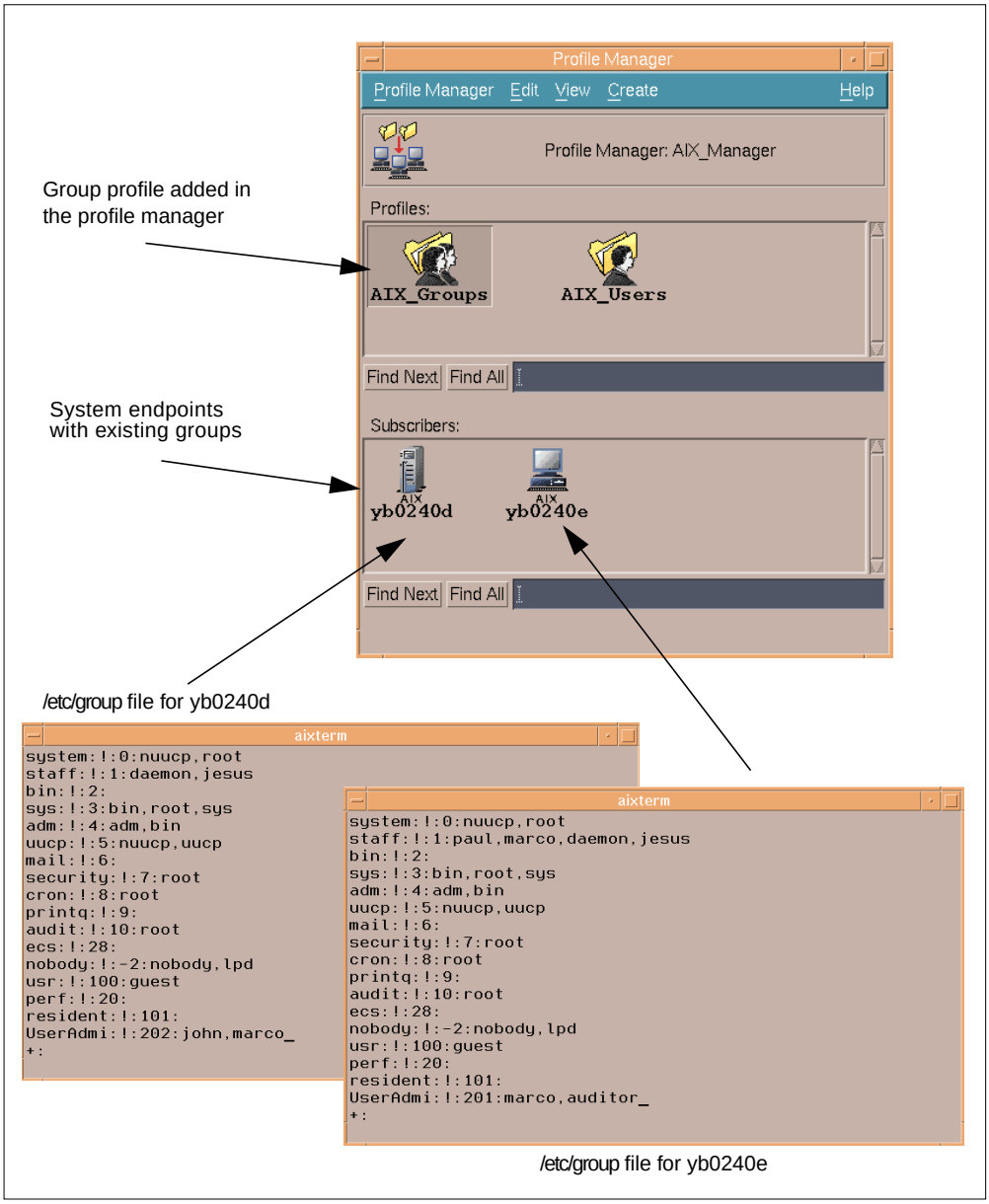


Figure 122. Profile Manager AIX_Manager

In this example, the group UserAdmi is defined on both machines. Note that the GID for that group and the list of users belonging to that group are different. A similar situation occurs for the group staff, we have a different set of users belonging to that group on the two AIX machines. We want to populate from both endpoints and analyze the group profile once populated.

Double-click on the **AIX_Groups** icon, to open the group profile, then from the Group Profile Properties window pull-down menu select **Profile**, then **Populate.** You will then be prompted with the following window similar to the one for user profiles.

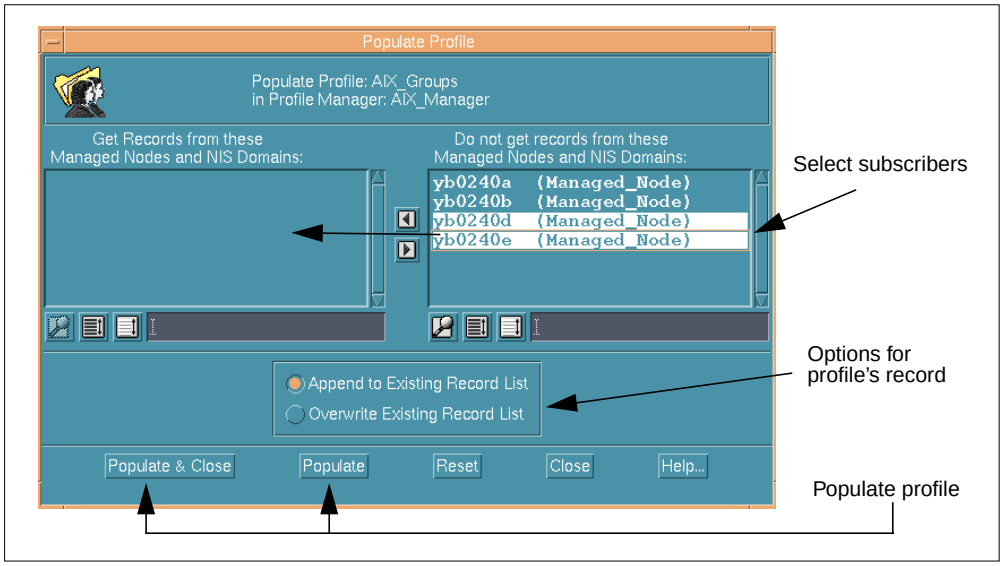


Figure 123. Populate Profile Dialog

Select the subscribers from which to populate the profile. Select also one of the options **Append to existing record list**, and **Overwrite the existing record list.** These options give you the ability to modify the existing list of records by simply adding the new groups discovered on the subscribers or to completely overwrite it. When populating for the first time, this option is not relevant because the group profile is empty.

In our example, we populate the group profile from yb0240d and yb0240e systems. After clicking on the **Populate** button, you get the following window:

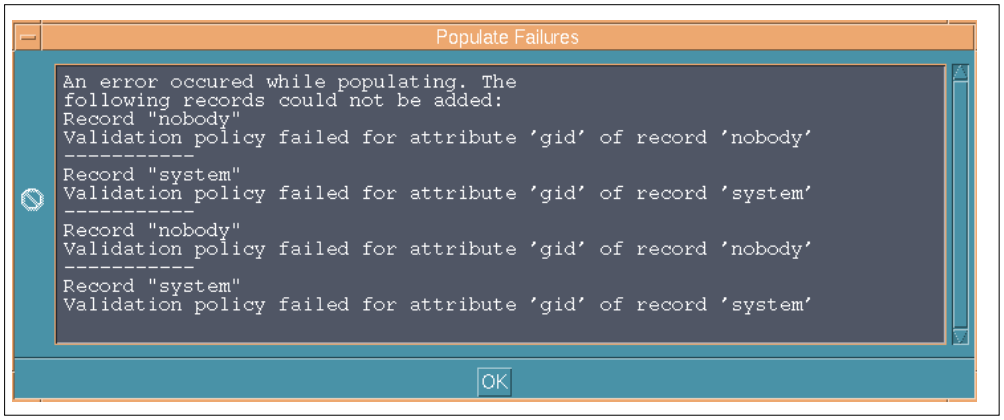


Figure 124. Populate Failures Window

This window warns you that the group accounts system and nobody have failed to pass the validation policy for the attribute Group Identifier. Looking at the validation policy script's body for the attribute GID, we find out that the system's GID and the nobody's GID are outside the range of GID values allowed by the policy. Once again, if you want to have such users included in your group profile you have either to edit the script body of the validation policy and modify the range of allowed GID values or disable the validation policy.

We get the following group profile:

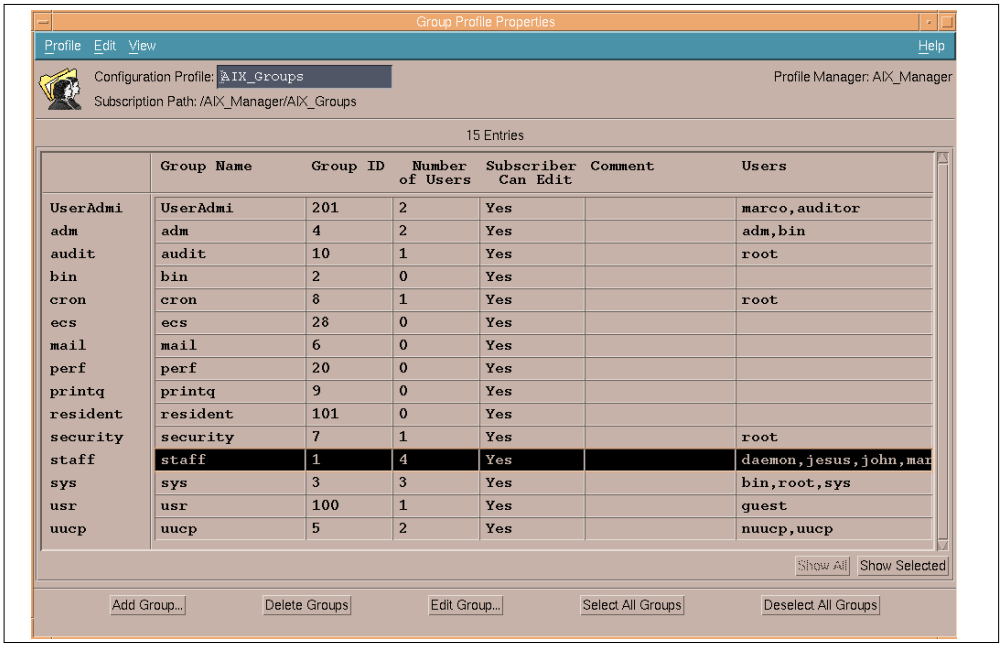


Figure 125. Group Profile Properties Window

This window shows that group staff has GID 201 and has only marco and auditor as members. The populate operation did not pick up the user john that was a member of staff on yb0240d system. This means that populating from two (or more) machines having similar group names can lead to some loss of information if you do not pay attention to it.

Attention!

When populating a group profile from several UNIX systems, groups having the same group name on different machines can cause problems. You must carefully check the attributes of these groups so you do not lose any information.

No merging operation is provided by TME 10 User Administration for group accounts.

Once again (as for the user accounts), the only case in which matching group accounts do not cause any problem is when the groups definition are exactly the same (groups have equal lines in the /etc/group file).

6.2.8 Distributing a Group Profile

After creating new groups, editing existing groups and deleting groups, and in general after performing operations on the group profile, you need to distribute the group profile to its subscribers to make effective your group administration operations. It is only after distribution that the sytem files on the endpoint systems are really up-to-date.

Once again, we find the three types of data already seen for user profile:

- The top level group profile which is the original profile
- The copy of the group profile (stored on the subscriber itself)
- The system files (for example /etc/group)

In our example, after the first distribution, we found the following situation shown in Figure 126.

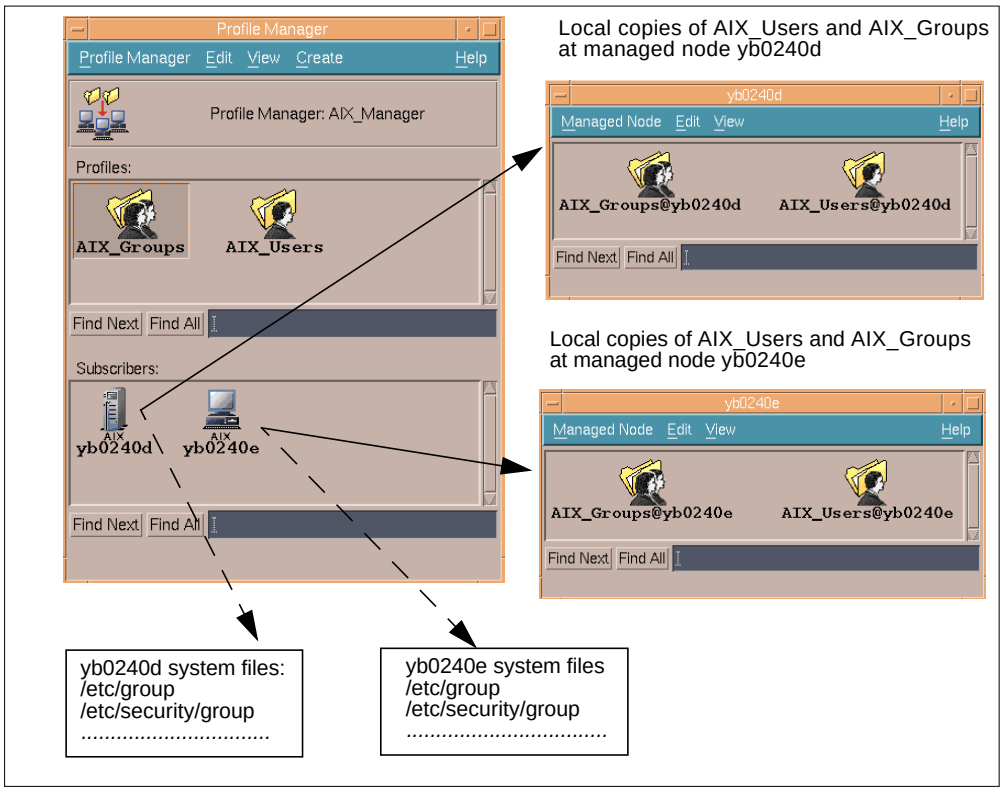


Figure 126. User and Group Management with User and Group Profiles

The local copies of the group profile allow a local administrator to perform some customizations on them and eventually distribute them in order to update the system files.

The distribution options are exactly equal to those already seen for user profile, with the same meaning. Once again you have to be careful not to erase the standard AIX group accounts from the subscribers' machines and not to erase some other administrator's work. Therefore, pay particular attention when you plan to distribute with the option **Make each subscriber's profile an EXACT COPY of this profile**.

6.2.9 Adding, Editing, Deleting a Group

The first operation you must carry on to add a group on a set of systems is to add a group record in the group profile. Select **Add Group** from the Edit pull-down menu of the Group Profile Properties window, or press the **Add Group** button to display the Add Record To Profile dialog, as shown in Figure 127.

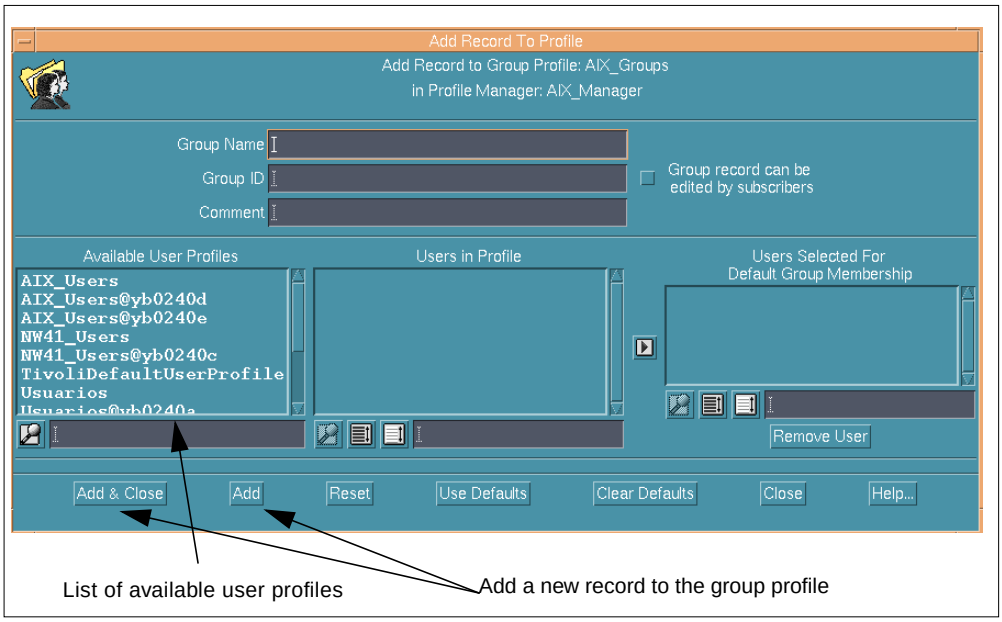


Figure 127. Add Record to Profile Dialog

You can add the following types of information to each group record:

- Group Name
- Group ID
- Comments about the group
- Group members
- Whether subscribers can change the record

You can find also a list of buttons that allow you to :

- Reset the dialog to the last saved state (**Reset** button)
- Keep the values you entered and add values defined by the default policies for the fields you did not fill (**Use Defaults** button)
- Clear the default values and enable all the fields of the dialog (**Clear Defaults** button)

Let us consider the following example. We want to create a new group comprising users marco and john. We fill out the Group Name field with the name of the group and use the default policies for the GID. Then we click on the AIX_Users user profile in the Available User Profiles list to retrieve the list of the available users in the profile.

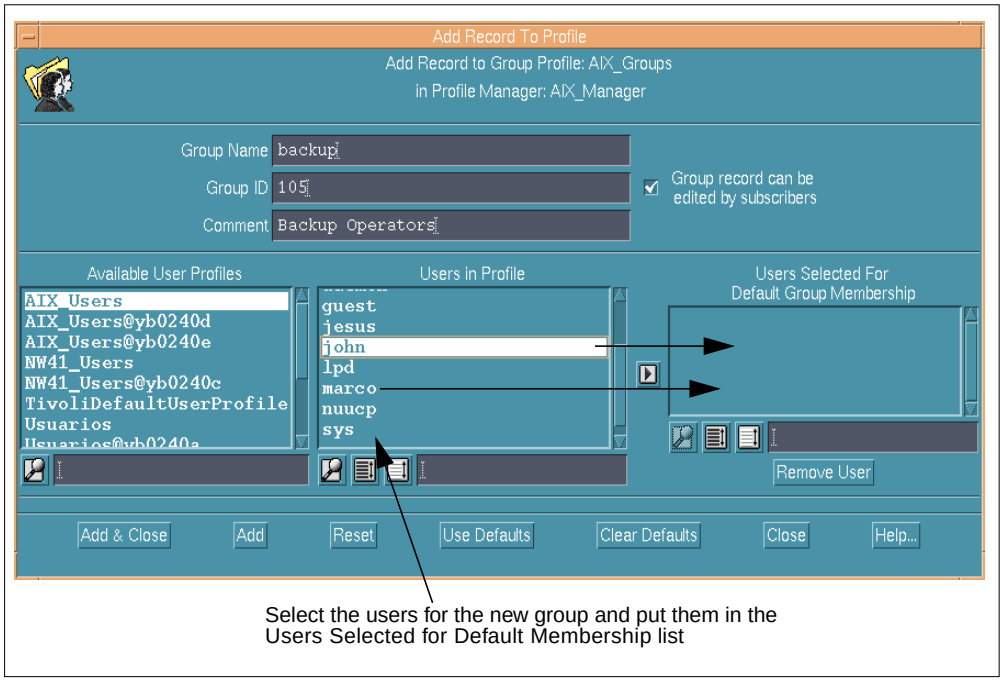


Figure 128. Adding a New Group

We choose the users for the new group and put them in the Users Selected for Default Membership list. We add a short comment for the group and then we click on the **Add & Close** button to get the group profile updated with the new group.

To edit an existing group, you can double-click on the row corresponding to the group or select the group and click on the **Edit Group** button shown in Figure 125 on page 185. You will be prompted with the window shown in Figure 128 on page 188, with the fields already filled and ready to be edited.

To delete a group from the group profile database, select the group and click the **Delete Groups** button shown in Figure 125 on page 185.

6.2.10 Synchronizing System Files with Group Profiles

If a user, having root access to a UNIX machine, directly adds or deletes a group, the group profile will no longer be consistent with the system files. The synchronize function provides a way to keep the group profile consistent with the system files by showing you which records do not match the system files entries and eventually modifying the appropriate group profile to match them.

As already explained for the user profiles, the synchronize function updates the the copy of the group profile stored at the endpoint. It does not update the top level group profile.

Let's consider the following example. In the profile manager shown in Figure 126 on page 186, we manually add a new group, called operator, to the UNIX machine yb0240d. This leads to a discrepancy between the system files and the group profiles (both the local copy and the top-level group profile), as shown in the following figure:

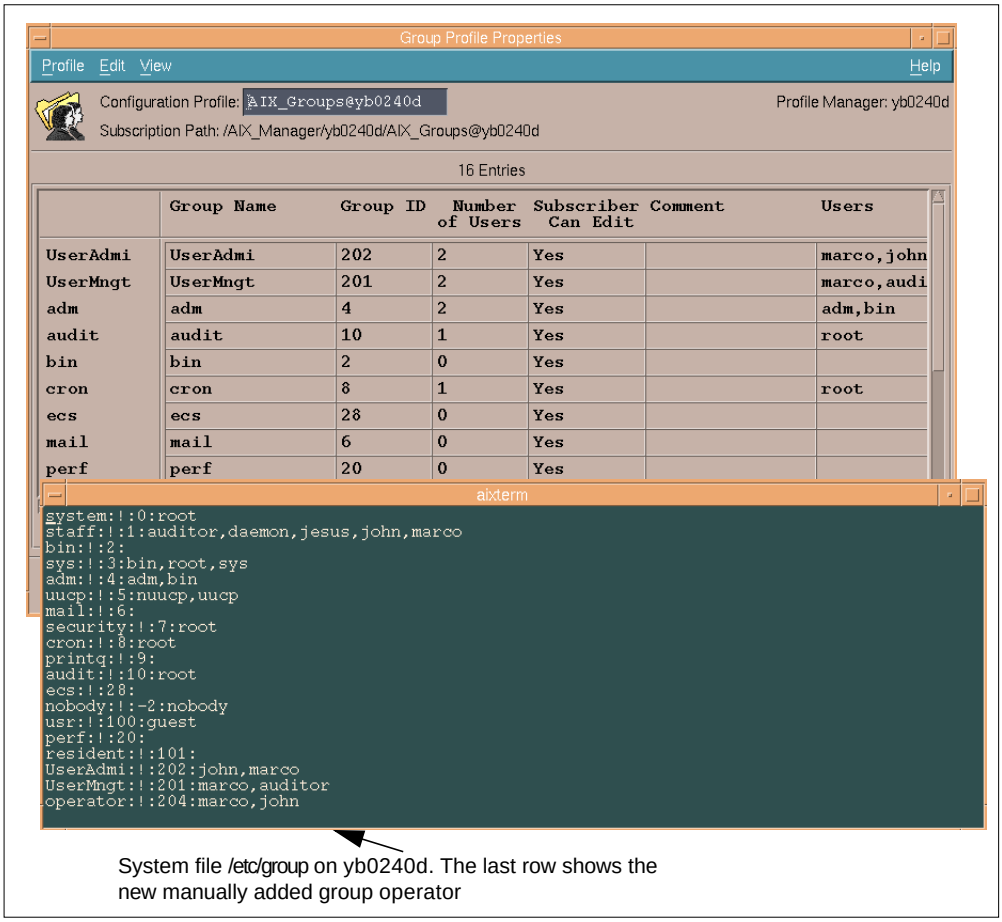


Figure 129. Local Copy of Group Profile vs. the /etc/group System File

Synchronizing means adding that group to the local copy of the group profile, and eliminating the discrepancy between /etc/group and AIX_Groups@yb0240d. Select **Synchronize** from the managed node icon pop-up menu or from the local User Profile Properties pull-down menu. You will get the list of all the profiles available for the managed node:

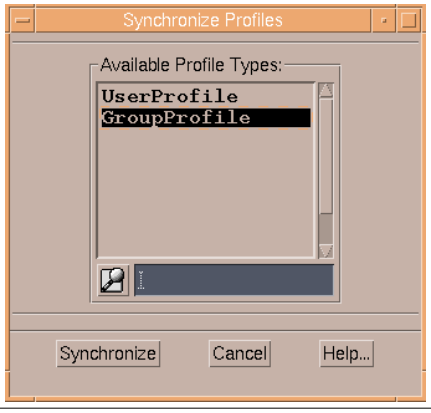


Figure 130. Available Profiles for the Managed Node yb0240d

Click on the **Synchronize** button to get the discrepancies between the group profile and system files, as shown in the following window:

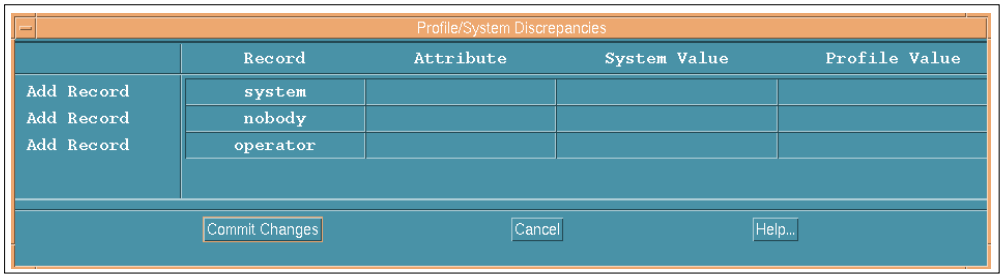


Figure 131. Profile/System Discrepancies Window

In this window, we find the groups system and nobody that have not been added during the populate operation (because they failed the validation policy) and the manually added group operator. The first column shows the actions to do in order to eliminate the discrepancies: Add Record in our case. You can click on the **Close** button and perform the required changes manually by adding the group operator to the group profile or click on the **Commit Changes** button to copy the system files information into the group profile. Click the **Commit Changes** button to get the following window:

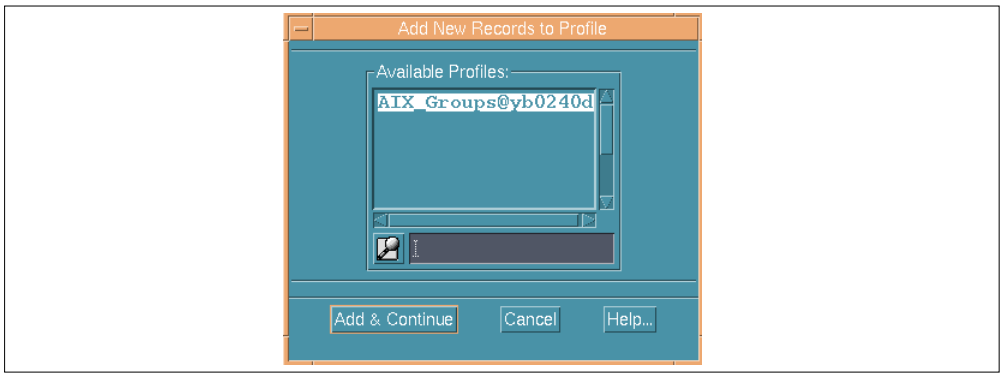


Figure 132. Committing the Changes

This window allows you to choose the group profile you want to update in the profile manager. Click on **Add & Continue**:

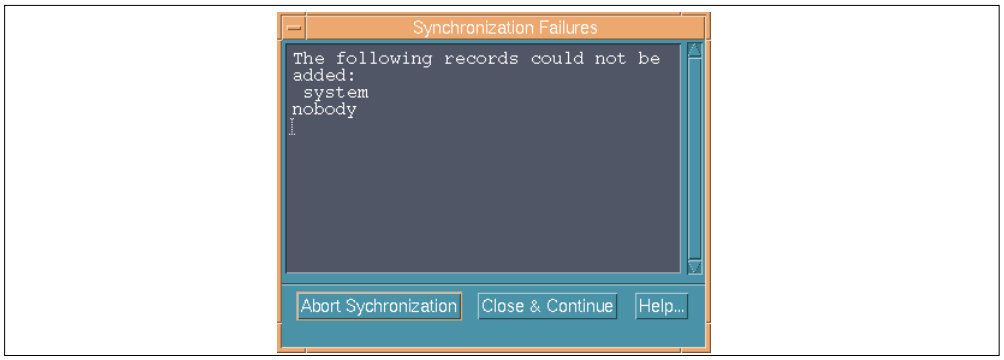


Figure 133. Synchronization Failures Window

The Synchronization Failures window warns you that the groups system and nobody have not been added to the group profile. This is normal since the validation policies prevents adding these groups. Press the **Close & Continue** button to finish the operation. The AIX_Groups@yb0240d profile is now updated with the group operator as shown in the following figure:

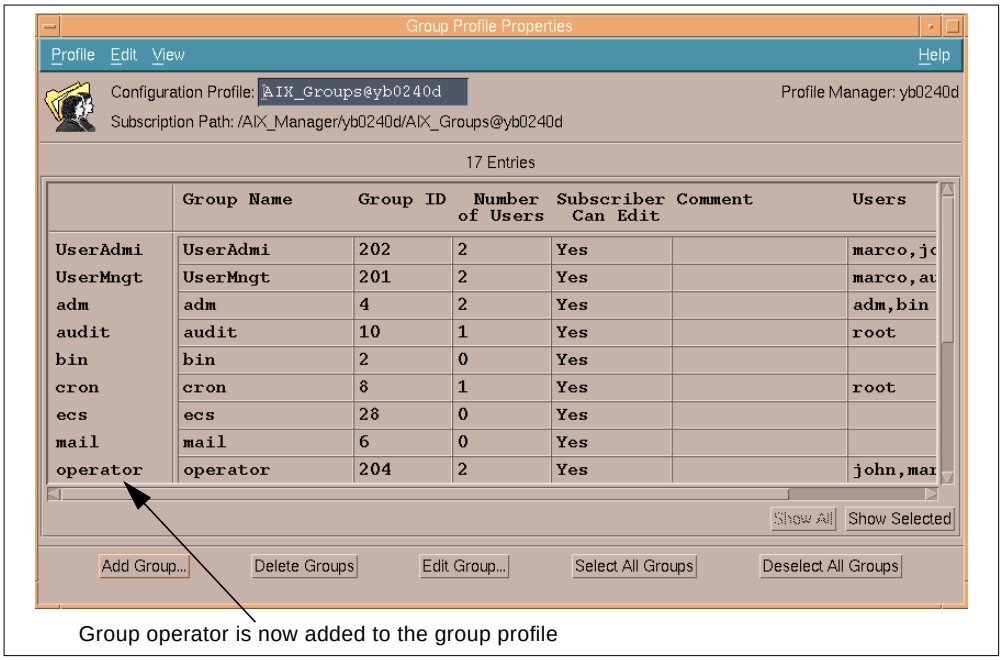


Figure 134. Updated AIX_Groups@yb0240d Group Profile

The synchronize option allows you to keep consistent the system files and the local copy of the group profile. To give the top level administrator an updated view of the subscribers system files, it is also necessary to keep the consistency between the subscribers system files and the top level group profile.

The top level group profile can be updated with the command `wchkgrps`. There are no options on the GUI to perform that operation. Let us consider the previous example: we want to add the group operator to the top level group profile AIX_Groups. From the command line you must issue the following command:

```
wchkgrps -s @GroupProfile:AIX_Groups -u @GroupProfile:AIX_Groups
@ManagedNode:yb0240d
```

where :

`-s` is to specify the source profile (the profile to compare with the system files);

`-u` is to specify the profile to update (it may be different from the source profile);

`@ManagedNode:<Managed_Node_Name>` is to specify the subscriber's system files to synchronize with.

By issuing the command we get the following output:

```
# wchkgrps -s @GroupProfile:AIX_Groups -u @GroupProfile:AIX_Groups \
@ManagedNode:yb0240d
Checking endpoint @ManagedNode:yb0240d..
These groups were found in the system but not in the database:
Group Name: Gid : Members
system : 0 : root
nobody : -2 : nobody
operator : 204 : john marco
These differences have been updated in the profile
```

Figure 135. Updating the Top Level Group Profile

Although the command line output does not show it, once again you will find that the groups system and nobody have not been added (which is normal according to the validation policies). The group operator has been added to the top level group profile as shown in the following figure:

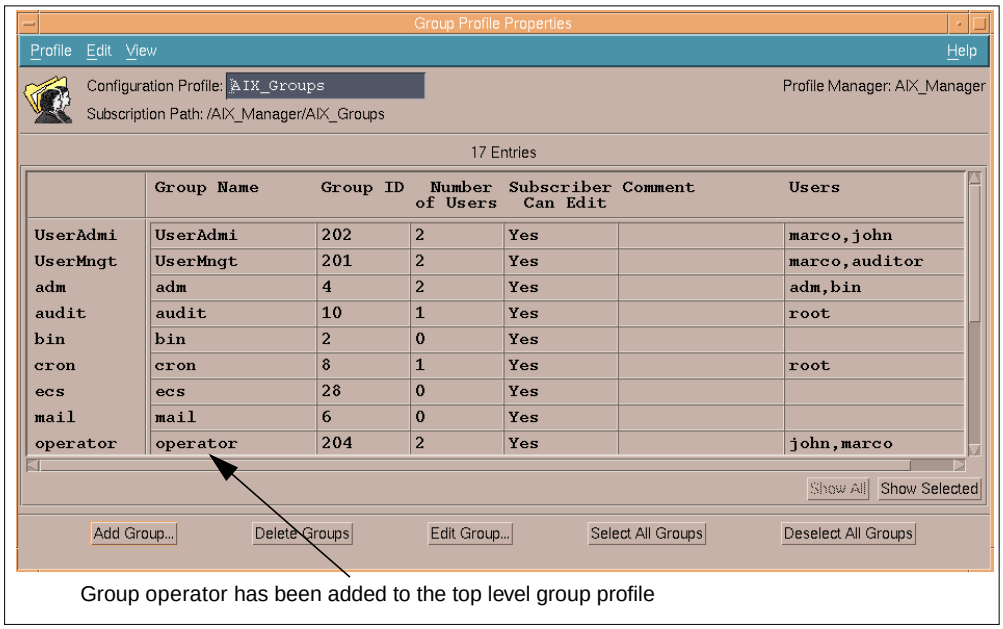


Figure 136. Updated Top Level Group Profile

6.3 Managing Network Information System Domains

Network Information System (NIS) maintains a common set of logins, groups and other information for a given set of hosts. This set of hosts is called an NIS domain. An NIS domain includes a master server, one or more client hosts and optionally one or more slave servers. The common information for the NIS domain is kept in the master server as a set of maps. The master server sends copies of maps to the slave servers (if existing in the NIS domain), and both master and slave servers provide common information to the client hosts that request it.

6.3.1 Creating an NIS Domain on the Desktop

In our lab environment we set a simple NIS domain, containing a master server (the yb0240d AIX machine) and a client host (the yb0240e AIX machine). We did not set any slave server.

Note

TME 10 User Administration does not create NIS domains. It simply allows you to create an object representing the domain and then manage NIS maps and map entries from the Tivoli desktop.

Be sure that your NIS master server is a managed node.

NIS domains are managed resources in the policy region to which they belong. So before defining an NIS domain on your desktop be sure that the resource *NisDomain* is included in the *Current Resources* list for your policy region as shown in the following figure:

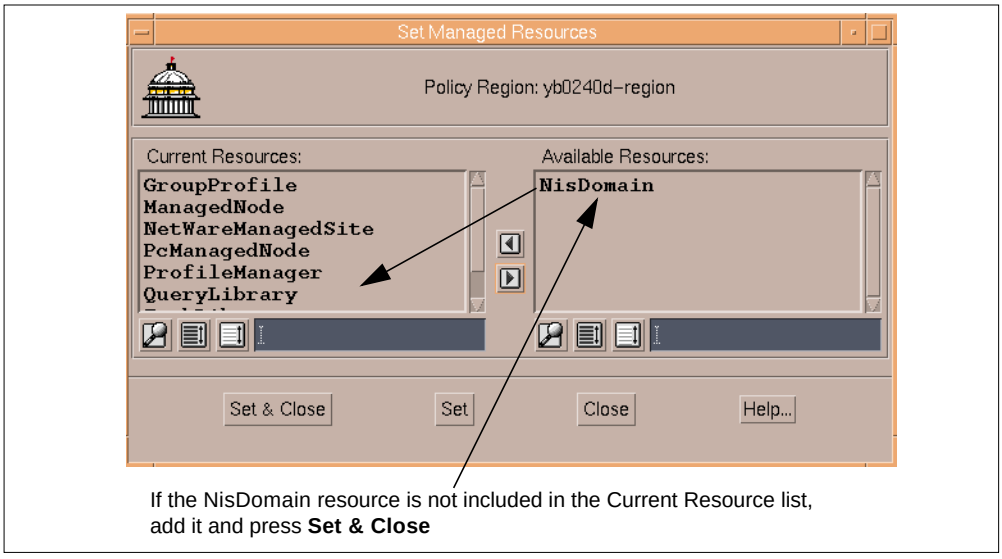


Figure 137. Set Managed Resources Dialog

Once you are sure that NisDomain is a TME 10 Managed Resource, you can add your NIS domain to the desktop. In the Policy Region window select **Create**, then **NISDomain...**, and you will get the following window:

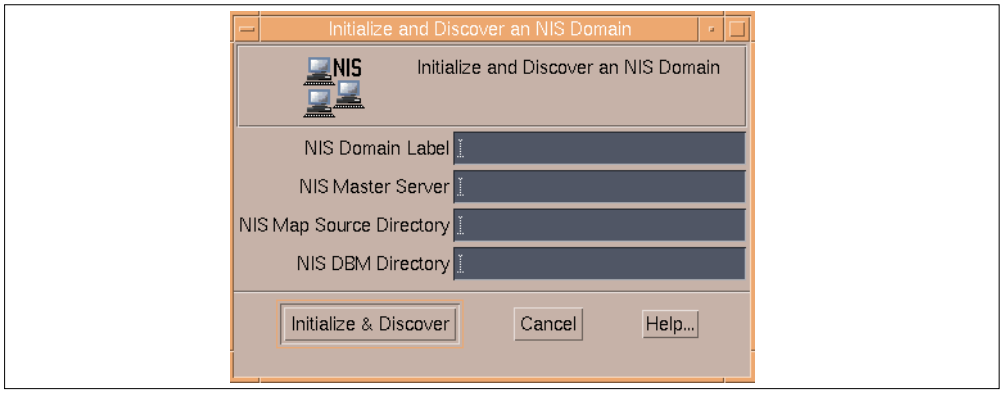


Figure 138. Initialize and Discover an NIS Domain Dialog

You then need to provide the following information in this window:

- NIS Domain Label: the label entered here is the label that will show up with the NIS icon on the TME 10 desktop
- NIS Master Server: specify here the host name of the NIS master server. Be sure that it is a managed node in the policy region and that it is already configured as an NIS master server.
- NIS Map Source Directory: specify here the path for the NIS source directory. The source files for the maps are in that directory.
- NIS DBM Directory: specify here the path of the directory containing the maps themselves. This directory must have a subdirectory with the same name as the NIS domain.

In our example, we filled out the window in the following way:

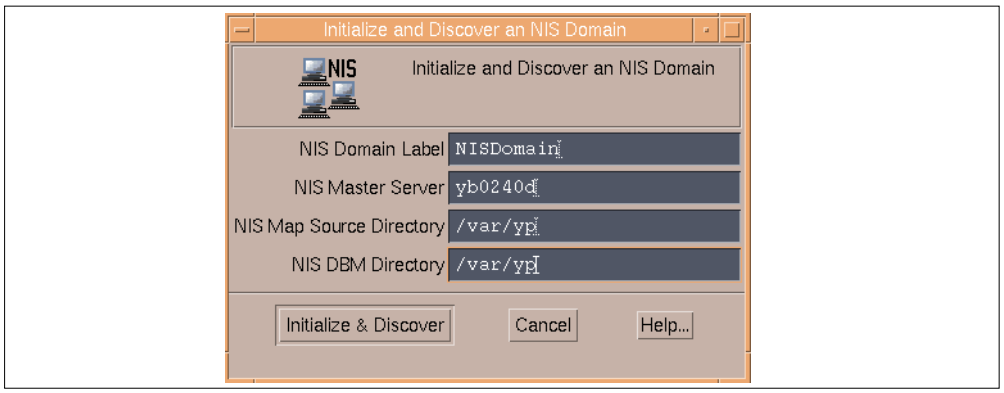


Figure 139. Initialize and Discover an NIS Domain

We labeled the domain as NISDomain on the desktop icon. We selected the managed node yb0240d as the master server (the machine must be already properly configured at this step). Then we specified the names of the directories in which the DBM directory and the source directory reside for the domain.

Note

The NIS Map Source Directory and the NIS DBM Directory can differ from one UNIX platform to another.

The NIS Map Source Directory is the top level NIS directory. Usually /var/yp or /etc/yp.

The NIS DBM Directory is the directory containing a subdirectory that contains the maps themselves. It is usually the same as the source directory.

Once all that information is provided, click on the **Initialize & Discover** button to allow TME 10 User Administration to find the NIS maps on the master server. You will then get the NIS domain icon added to the desktop.

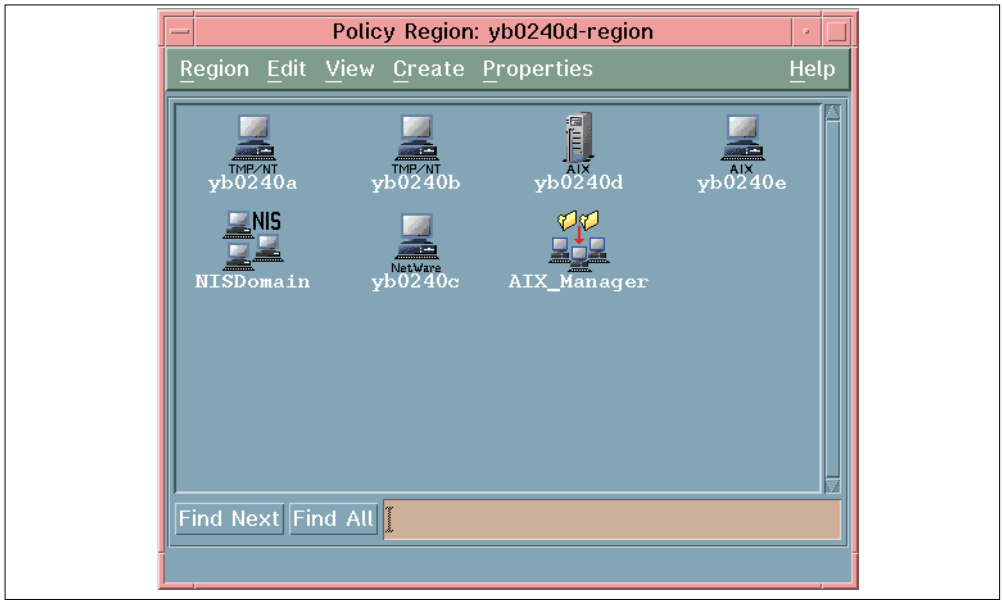


Figure 140. Policy Region with the NIS Domain Icon

6.3.2 Adding NIS passwd and group Maps

You can create an NIS map from the desktop and add it to the NIS database. Open the NIS Domain Properties window from the NIS icon's pop-up menu to get the following window:

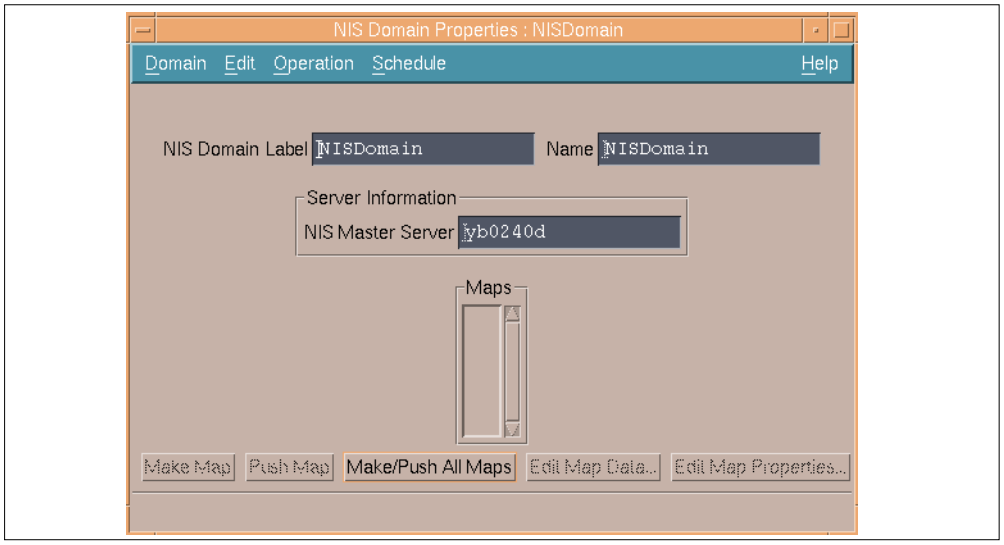


Figure 141. NIS Domain Properties Dialog

At this stage we do not have any map defined for the NIS domain. We want to define a map for the system file /etc/passwd and add it to the NIS database. Select **Edit** then **Add Map**, to get the NIS Map Properties window. Fill out that panel in the following way:

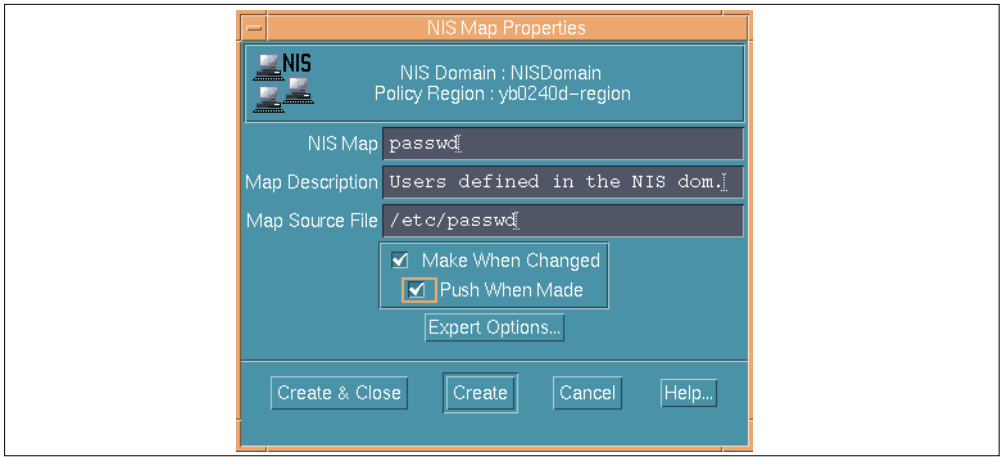


Figure 142. Adding the passwd Map to the NIS Domain

We mapped the system file /etc/passwd to the NIS map called passwd and chose to activate the following options:

- Make When Changed: This option will automatically run the make utility to generate an updated version of the NIS passwd map every time the system file /etc/passwd is modified. This means that the make utility will be automatically run after for example a user profile distribution to all levels to the NIS managed node.
- Push When Made: This option automatically pushes a copy of the map to the slave servers when the map is updated.

Now click on the **Create & Close** button to get the map passwd added to the NIS domain, as shown in the following figure:

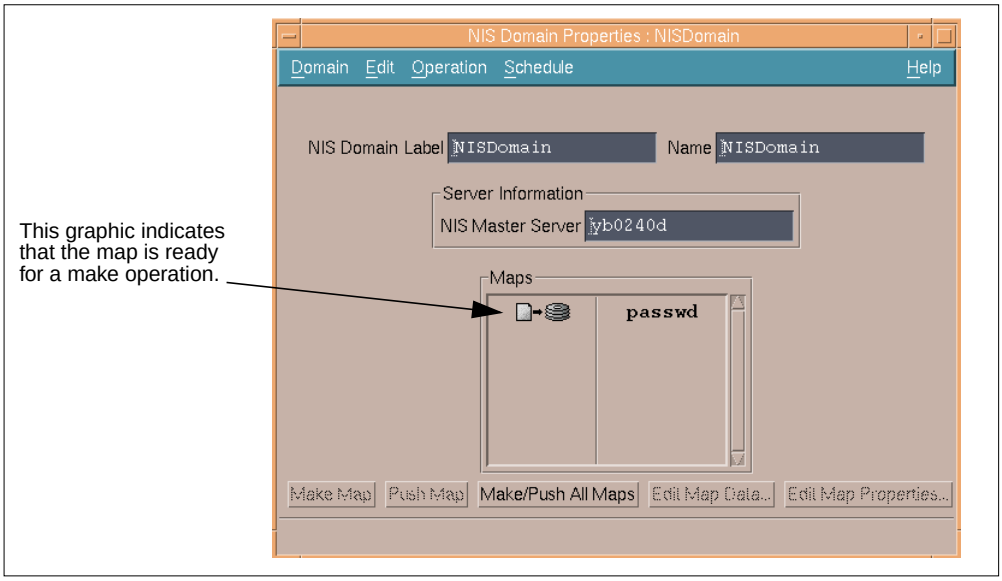


Figure 143. Making and Pushing the passwd Map

At this point you can make and push the map to get the master server and the slave servers databases updated.

Note: You will be required to save your domain configuration. You can do it by clicking on **Domain**, then **Save** from the NIS Domain Properties dialog.

At this point we can view the content of the map by clicking the **View Map Data** button. You will get the NIS Domain passwd Map window as shown in the following figure (along with the /etc/passwd file to check the consistency).

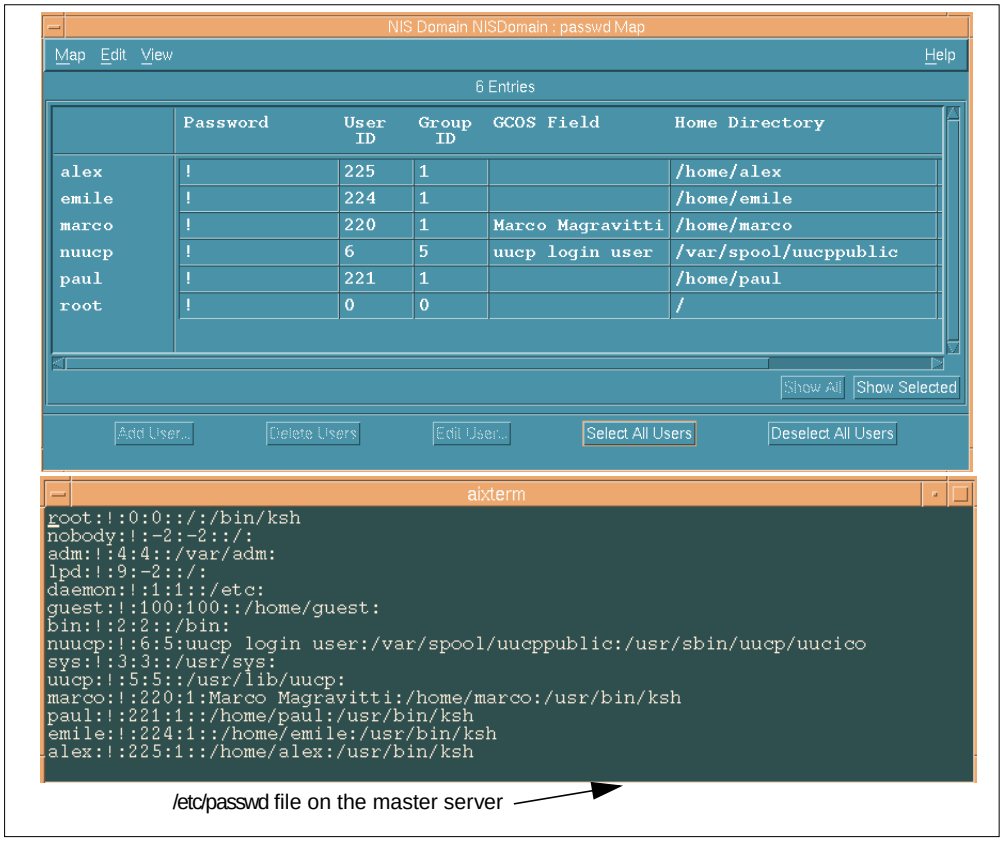


Figure 144. NIS Domain passwd Map vs. System File

Note

It is very important to understand that TME 10 User Administration does not provide full management capabilities for passwd, group and hosts maps. These maps cannot be edited and modified at this step. You notice that the Add User..., Delete Users and Edit Users buttons are not available. In fact, these maps are managed by TME 10 User Administration through the management by subscription mechanism. NIS domains are managed as managed nodes.

Therefore, you need to create a user and or group profile for the NIS domain, set the NIS domain as a subscriber of the corresponding profile manager and manage the users with the TME 10 User Administration functions such as Populate, Edit and Distribute that we used previously to manage standard UNIX users.

TME 10 User Administration provides full management capabilities for the following maps:

- aliases
- ethers
- netgroup
- netmasks
- networks

- protocols
- publickey
- rpc
- services

This means that it is possible, for example, to create a map for /etc/services and manage it directly by editing the NIS Domain Map window.

Once the passwd map has been successfully created, you can create the group map in order to fully administer users and groups on your NIS domain. Adding a group map is similar to adding the passwd map. Just go to the NIS Map Properties dialog (Figure 145).

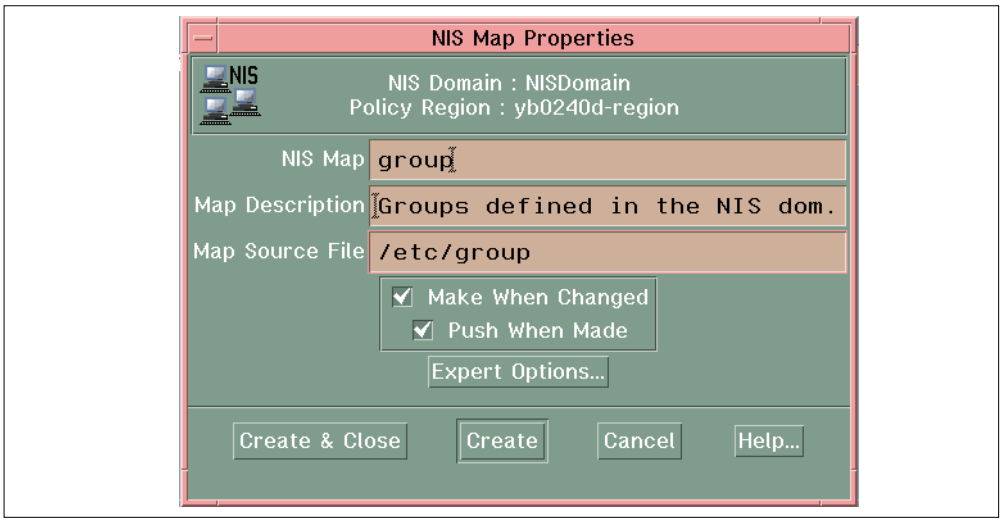


Figure 145. Adding the group Map to the NIS Domain

When the map is created, you should get the following window:

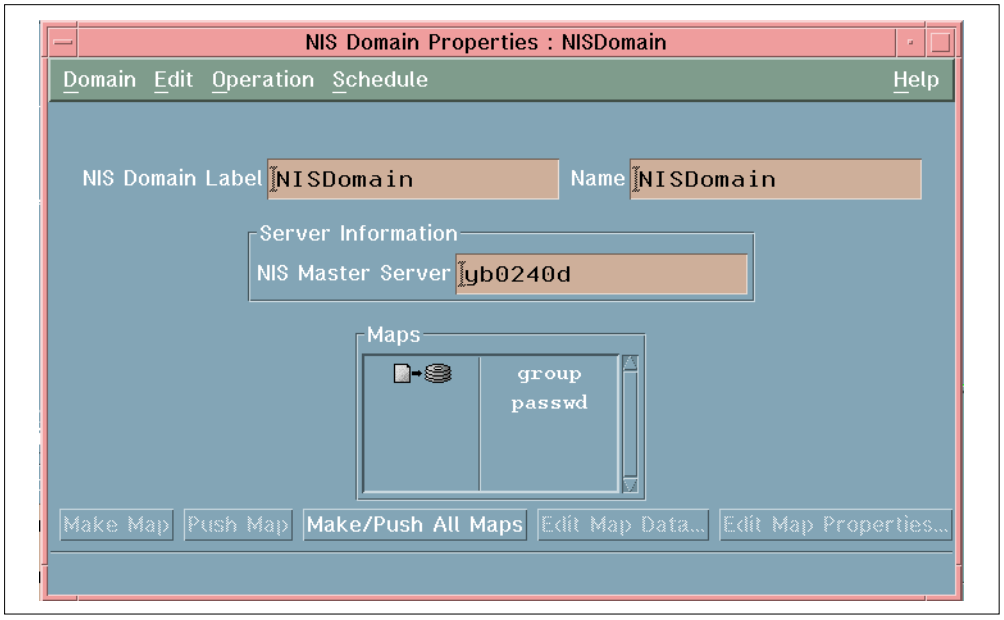


Figure 146. NIS Domain Properties Dialog

From this panel, you can make and push the group map.

6.3.3 Creating User and Group Profiles for the NIS Domain

In order to manage users and groups within the NIS domain, you must create a profile manager with a user profile and a group profile and set the NISDomain as a subscriber to that profile manager. In our example, we created a profile manager called NIS_Manager, a user profile called NIS_Users and a group profile called NIS_Groups ad shown in Figure 147.

Figure 147. Profile Manager NIS_Manager Containing NIS User and Group Profile

6.3.4 Populating User and Group Profiles

As any other user and group profiles, the two profile NIS_Users and NIS_Groups need to be populated from the existing users and groups defined on the NIS master server. You just need to select the NisDomain resource and move it to the **Get Records from these Managed Nodes and NIS Domains** in order to populate your profiles from the NIS domain.

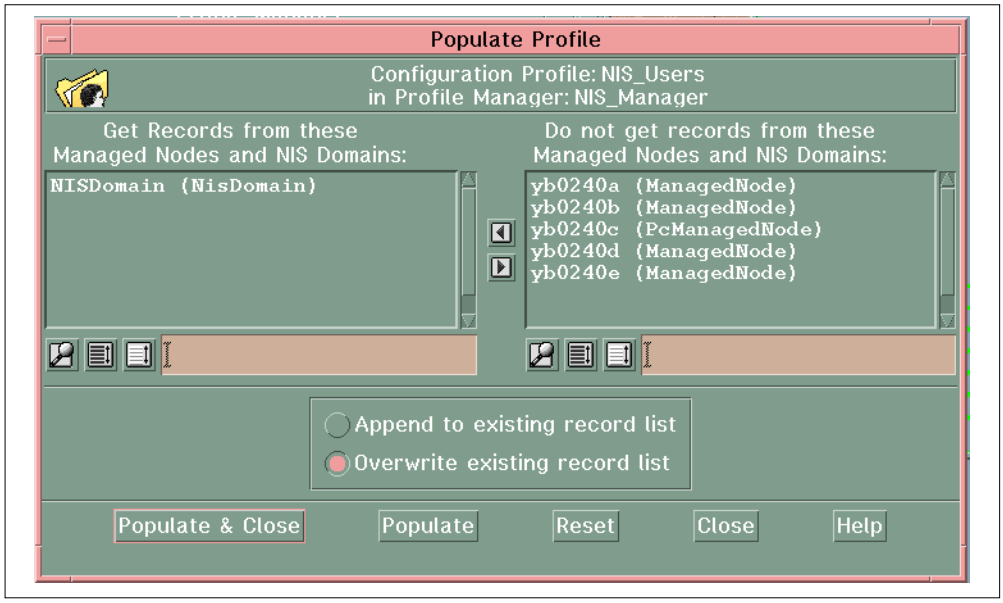


Figure 148. Populating User and Group Profiles from an NIS Domain

As other user profiles, user root and nobody failed the validation policies.

We populated in the same way the NIS_Groups profile. Groups nobody and system failed the validation poilicies which is normal. Note that the group profile must be saved before you can distribute it.

6.3.5 Distributing Profiles

Distributing a user or a group profile to a NIS domain is not different from distributing profiles to a managed node. You can distribute a profile to the next level or to all levels of subscribers. As for a managed node, the NIS domain keeps a copy of the profile at the managed node. That copy can be edited locally by an administrator. Accessing the NIS domain's copy of the profile can be done by selecting **Open** from the NIS icon's pull down menu. You should get the following dialog:

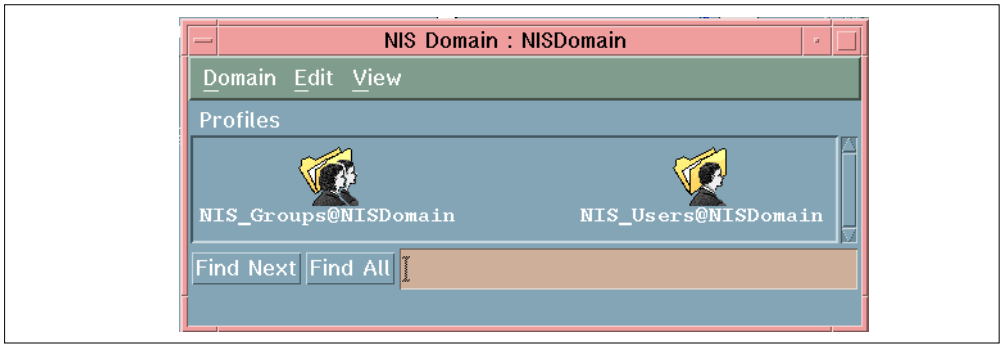


Figure 149. Profiles Stored at the NIS Domain Level

From the panel shown in Figure 149, you can open the user profile as well as the group profile for the NIS domain.

When we distributed either the user profile NIS_Users or the group profile NIS_Groups to the NIS domain called NISDomain with the option All levels of subscribers, we got the following error message:

```
The following errors occurred during this distribute:
->Distribute failed for subscriber 'NISDomain':
->The source path for the managed node and for the NIS endpoint are both
subscribed to profile managers with a group database. Distribution to these
endpoints are in conflict to the system file. Suggested solution is to set your
NIS domain to have its source directory differ from the source directory of the
managed node.
```

What happened if that the machine used as the NIS master server is also a managed node subscribing to a different profile manager (AIX_Manager)? This is why TME 10 User Administration detects a conflict. We just removed the yb0240d managed node from the list of subscribers in the AIX_Manager profile manager and we could distribute the profile to all levels. The distribution of the group profile worked fine as well.

Once the profile has been distributed to all levels, the system files /etc/passwd and /etc/group should have been modified. If you did not ask to run the make utility and push the maps, the NIS maps passwd and group are not yet updated. Only the system files /etc/passwd and /etc/groups have been modified at this step.

From the NIS domain icon's pull down menu, select **Domain Properties....** You should get the following window**:**

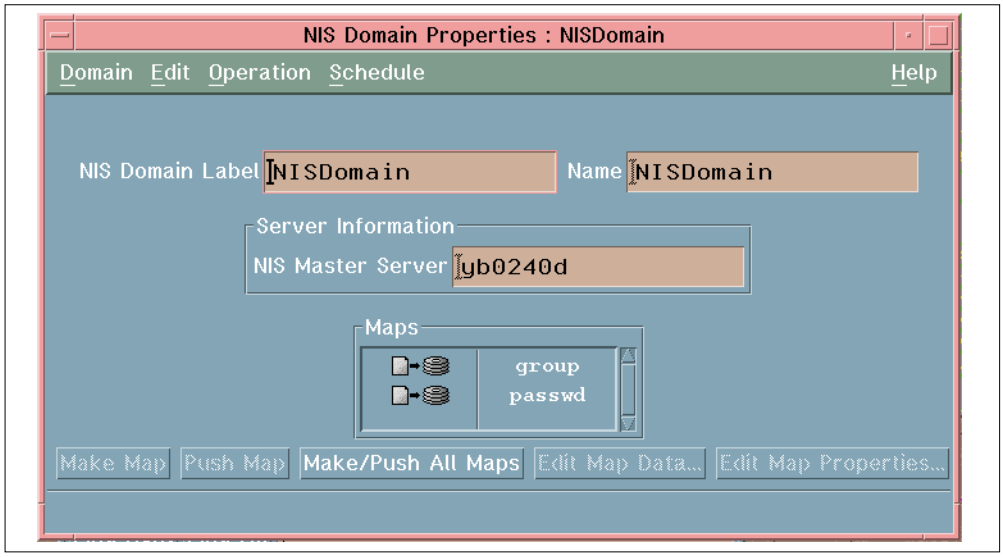


Figure 150. NIS Domain Properties

The two icons in the Maps area indicate that the maps are ready for a make operation. At this step you can click on **Make/Push All Maps**. This will make and push the two maps passwd and group in one step.

Since we are doing that operation for the first time, we prefer to select one of the map (passwd for example). You will notice that the buttons in the bottom of the window will be available.

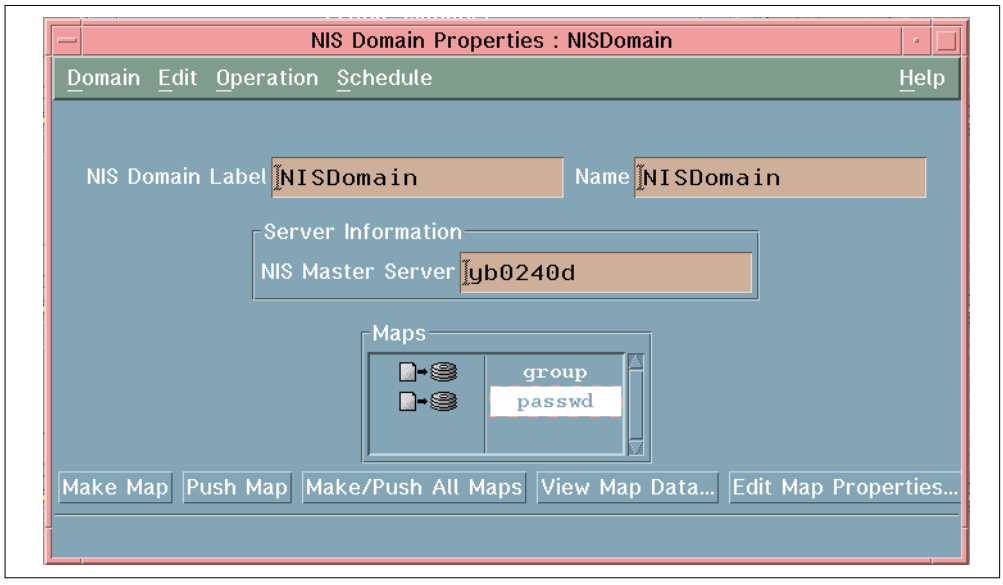


Figure 151. NIS Domain Properties

From this window, select **Make Map** to make the NIS map for passwd.

At this step, you might have an error message saying that it could not open the /usr/etc/yp/Makefile file. This is because the location of the Makefile used by the make command is different on your system as the one specified in the script

executed when you click on **Make Maps**. You can check that script by clicking on **Edit Map Properties...** then **Export Options...** You should get a dialog that allows you to modify the shell scripts that are run when you click on **Make Maps** or **Push Maps.**

Figure 152. Modifying the Make and Push Scripts

From the dialog in Figure 152, you can specify the right path for the Makefile used by the `make` command and the right path for the `yppush` command.

When the make has been run successfully for the passwd map, you should get the following window with a different icon in front of the passwd indicating that the map is ready for a push operation.

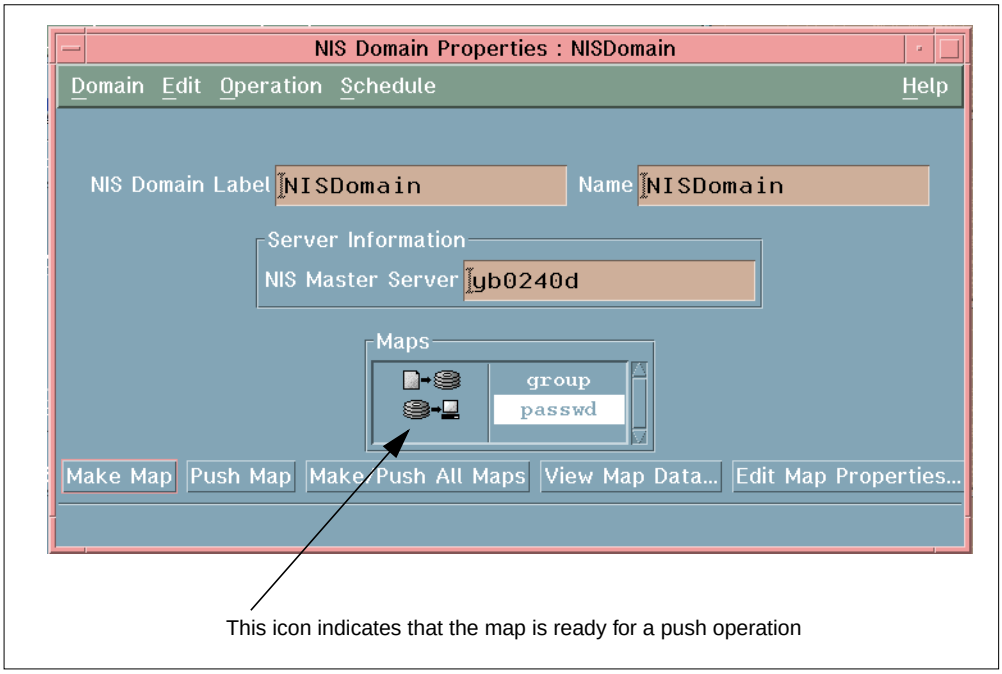


Figure 153. NIS Maps After a Make Operation

Once the make has been successful on the passwd and group maps, you can push the maps. After the push operation, the NIS Domain Properties windows should look like:

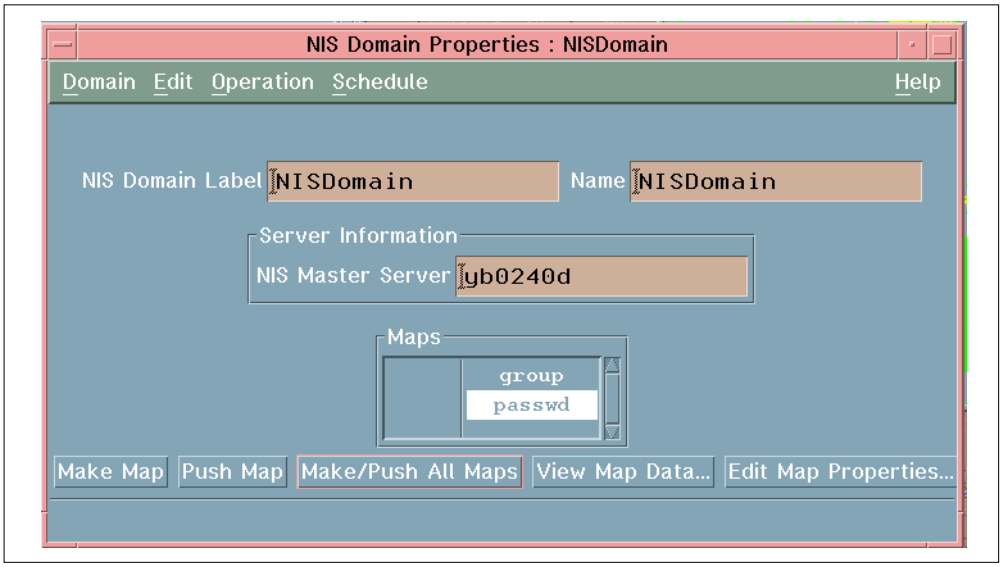


Figure 154. NIS Maps After a Push Operation

6.3.6 Synchronizing Profiles

If the system files have been directly modified, for example, /etc/passwd has been directly edited on the NIS master server, the copy of the profile stored at the NIS domain level and the top level profile (original profile) differs. As for a managed node, it is possible to synchronize the local copy of the profile with the system

files. You can access the local copy of the profile by selecting **Open** in the NIS icon's pull-down menu. Then select the profile you want to synchronize and click on **Domain**, **Synchronize**.

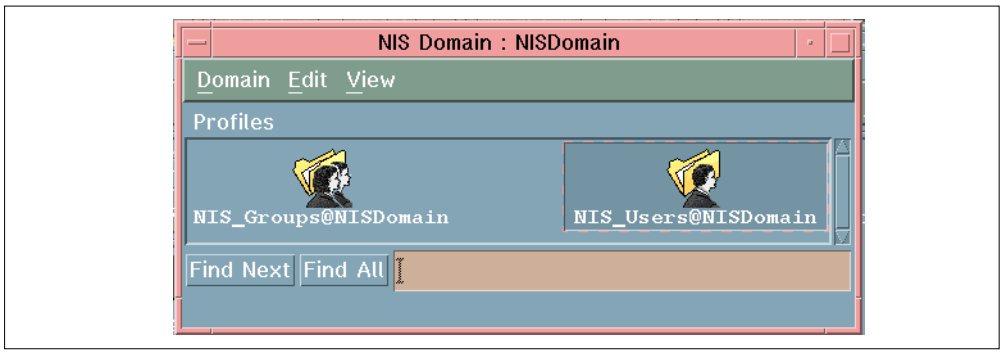


Figure 155. NIS Domain Local User and Group Profiles

Synchronization works the same as described earlier for regular UNIX users. For more information on the synchronize function, you can refer to section 6.2.5, "Synchronizing System Files with User Profiles" on page 176.

6.3.7 Creating Fake NIS Domains

Before using TME 10 User Administration to manage users and groups in an NIS domain, you might want to get familiar with TME 10 User Administration or perform some testing before actually managing an existing NIS domain. With TME 10 User Administration, it is possible to create a "fake" NIS domain. The fake NIS domain will undergo the same methods that an NIS domain will. The only difference is that there is no make or push file at the end, and there are no yp processes running. You will find below example commands you can use to create a fake NIS domain.

- Create the NIS source directory:

```
# mkdir /etc/yp/src
# cd /etc/yp/src
```

- Create the passwd and group files:

```
# head - 50 /etc/passwd > passwd
# head - 50 /etc/group > group
```

- Create the NIS DBM directory for the NIS fake domain:

```
# mkdir NIStest
```

- Create the NIS domain:

```
# wcrtdomain -c /etc/yp/src /etc/yp/src NIStest @yb0240d
@PolicyRegion:yb0240d-region
```

- Check if the wcrtdomain command has been successful:

```
# echo $?
```

  This command should return 0.

- List the source files for the maps:

```
# wlsmaps -s NIStest
group   /etc/yp/src/group
passwd  /etc/yp/src/passwd
```

- Create a new profile manager:

```
# wcrtprfmgr @PolicyRegion:yb0240d-region NIS_PM_Test
1423189896.1.773#TMF_CCMS::ProfileManager#      NIS_PM_Test
# echo $?
0
```

- Define the NIS domain as a subscriber to that profile manager:

```
# wsub @ProfileManager:NIS_PM_Test @NisDomain:NIStest
# echo $?
0
```

- Create a user profile and a group profile:

```
# wcrtprf @ProfileManager:NIS_PM_Test UserProfile Test_Users
1423189896.1.774#UserProfile#   Test_Users
# wcrtprf @ProfileManager:NIS_PM_Test GroupProfile Test_Groups
1423189896.1.776#GroupProfile#  Test_Groups
```

- Create some new users:

```
# wcrtusr -h /home/tracy -t MOUNTED -S overlook:/export/home/tracy -u 300
@UserProfile:Test_Users tracy
# wcrtusr -h /home/nathalie -t MOUNTED -S overlook:/export/home/nathalie -u
301 @UserProfile:Test_Users nathalie
```

  where:

  `-h /home/tracy` corresponds to the home directory path for the user

  `-t MOUNTED` corresponds to the home directory type (Local or Remote)

  `-S overlook` corresponds to the server path

- Create some new groups

```
# wcrtgrp -g 200 @GroupProfile:Test_Groups artists
# wcrtgrp -g 201 @GroupProfile:Test_Groups producers
```

- Distribute the user profile and the group profile to the fake NIS domain.

```
# wdistrib -m -l maintain @UserProfile:Test_Users @NisDomain:NIStest
# echo $?
# wdistrib -m -l maintain @GroupProfile:Test_Groups @NisDomain:NIStest
# echo $?
```

- After distribution, you can check the files passwd and group located in /etc/yp/src to see if the users and groups have been properly added.

6.4 Managing Windows NT Users

This chapter describes the TME 10 User Administration functions that allow you to manage user accounts on NT systems.

6.4.1 Populating a User Profile

Populate is the function of retrieving user definitions from system files and adding them as records into a profile.

To illustrate this, we used as an example two Windows NT systems. One is set up as a Primary Domain Controller (actually the Domain is made up of just one system, the PDC itself). The second one is set up as a Workgroup, it does not belong to the Domain. This example allows us to test populating from a Domain and from a Workgroup. We created a profile manager called NT_Manager containing a user profile NT_Users.

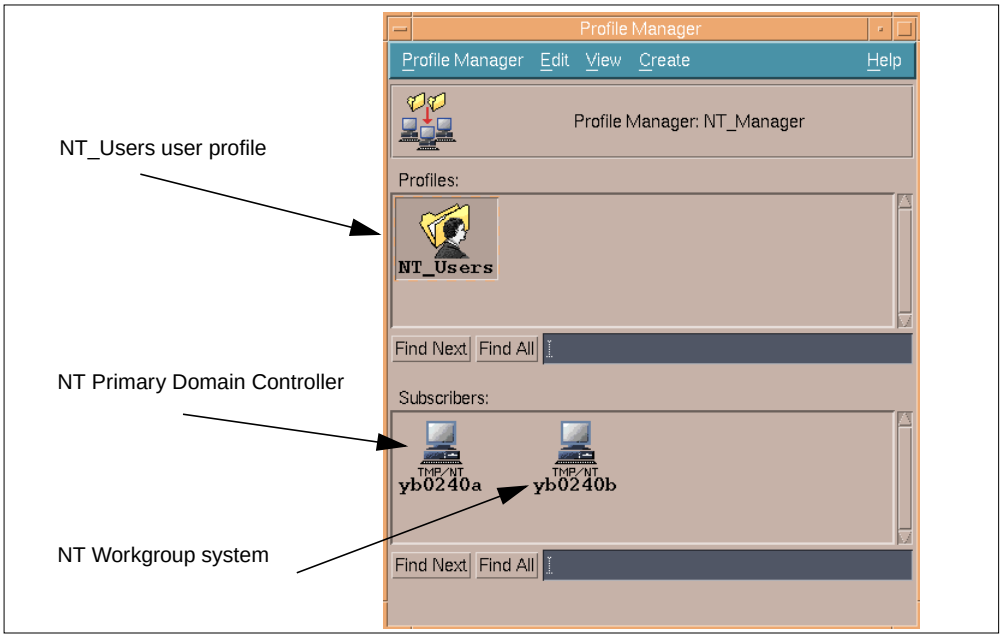


Figure 156. Profile Manager with Two Subscribers

The two subscribers to that profile are yb0240a (PDC) and yb0240b (Workgroup). The NT_Users user profile needs to be populated with the users defined in the user account database located on the PDC and those defined in the local user account database on the Workgroup machine. This means that the application must retrieve the domain users defined on yb0240a and the local accounts defined on the workgroup machine yb0240b.

That information is then put in the NT_Users user profile, according to the validation policies enforced on it. Only records complying with the validation policies will be added to the user profile.

The same considerations we found for UNIX users are enforced for NT users. When populating a user profile, if two user accounts have the same login name on two different user account databases (in our example, the one on the PDC and the one on the workgroup machine) you will get an error when TME 10 tries to

populate the second user. This error will be indicated in the Populate Errors window. Therefore, you will be able to:

- Locate the problem.
- Check if the users are actually the same. Two different users might have the same login account on two different systems.
- If the two users are the same, check if some attributes are different. If some attributes are different, you might want to merge the two users.
- If the two users are different, you might want to change the login name of the second user (which has not been populated) in the system files and then synchronize the profile with the system files or populate again with the append option.

Attention!

All populate errors should be carefully checked in order to avoid losing important user information.

To populate, double click on the NT_Users icon (or select **Open User Profile** from the icon's pop-up menu) to get the *User Profile Properties* window. From the pull down menu select **Profile** then **Populate.** You will get the following window:

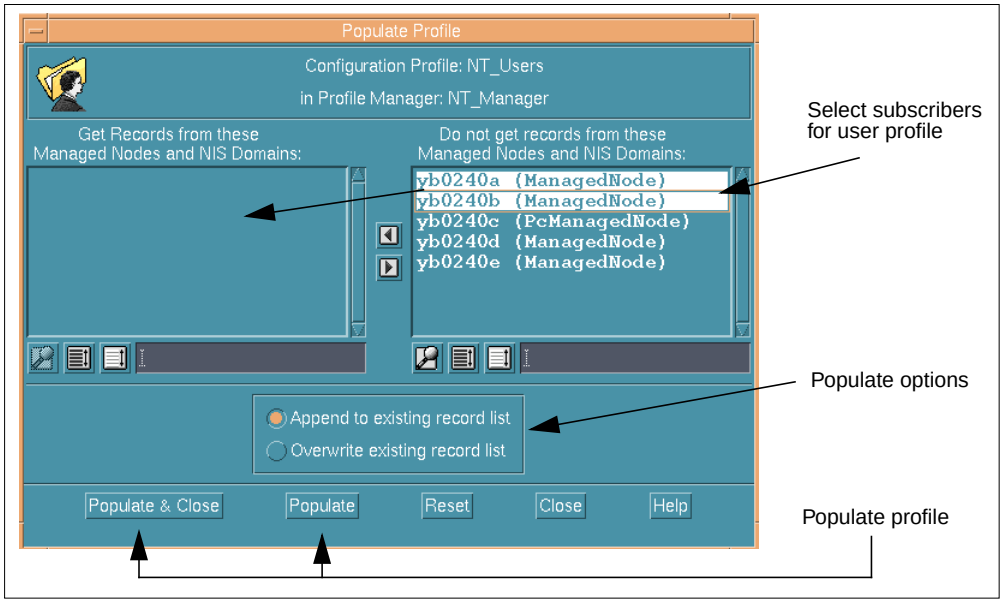


Figure 157. Populate Profile Dialog

Select yb0240a and yb0240b as Managed Nodes from which to retrieve user information. Since you are populating the user profile for the first time, you can choose any of the two populate options: Append to existing record list or Overwrite existing record list. Then click **Populate & Close** to get the Populate Errors window:

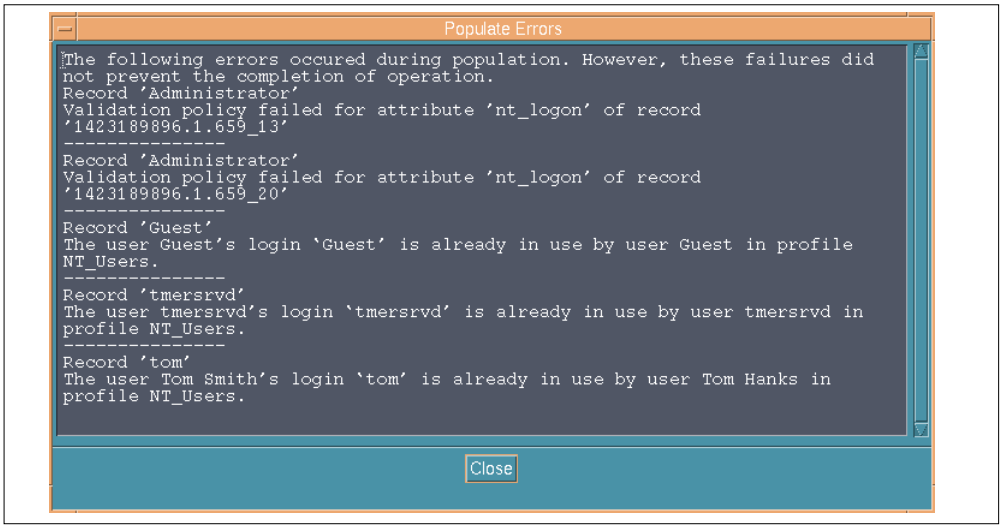


Figure 158. Populate Errors Window

In the first two entries the window warns you that the record Administrator has failed to pass the validation policy and has not been added to the user profile. This user failed this validation policy twice because it is defined on both systems. If you want the user Administrator to be included you need to disable the validation policy or change it by editing the shell script body corresponding to that validation policy. The other entries shown in the window are error messages due to NT accounts having the same login name on both systems. TME 10 User Administration populates the first user from the first system and then warns you that this user already exists in the user profile when populating from the second system. In our case we have an error for users Guest, tmesrvd and tom.

Attention!

When two user login names are matching, User Administration populates the first one, tries to populates the second one and gives an error message for the second one. This is fine if the two users are the same and have exactly the same attributes. However, if the login name corresponds to two different users, or if the users have different attributes, you might want to check all the users that failed the population.

In the case of tmservd and Guest, these users have exactly the same characteristics on both systems. In the case of tom, this login name corresponds to two different user accounts belonging to two different persons.

We changed the login name tom on yb0240b to toms then populate again with the **Overwrite existing record list** option to get the correct user profile population.

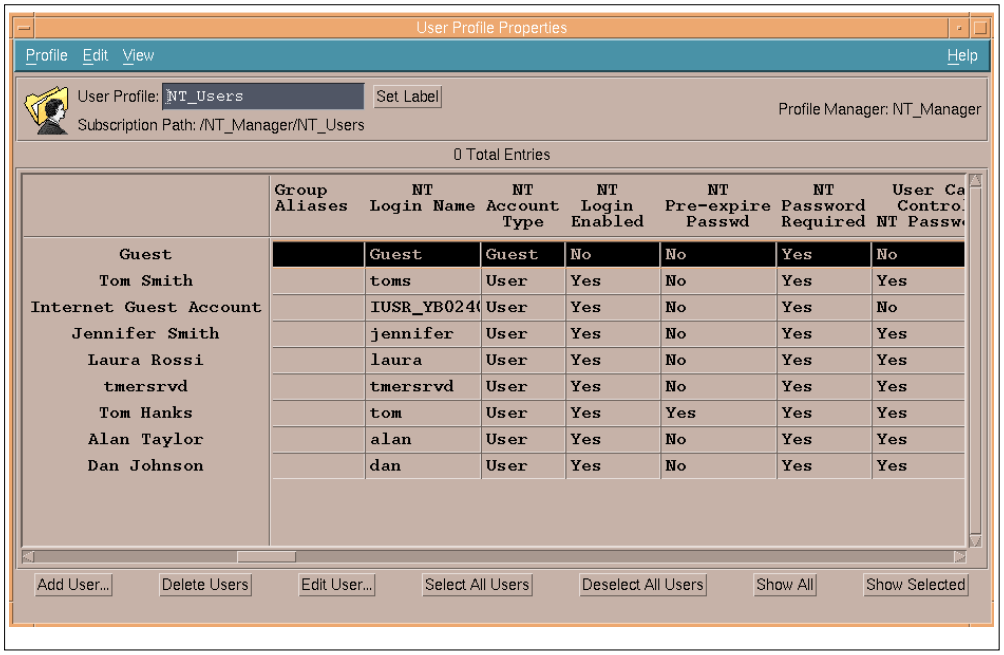


Figure 159. User Profile Properties Dialog

We can check the consistency of this user profile with the Windows NT machine's system files, as shown in the following figures:

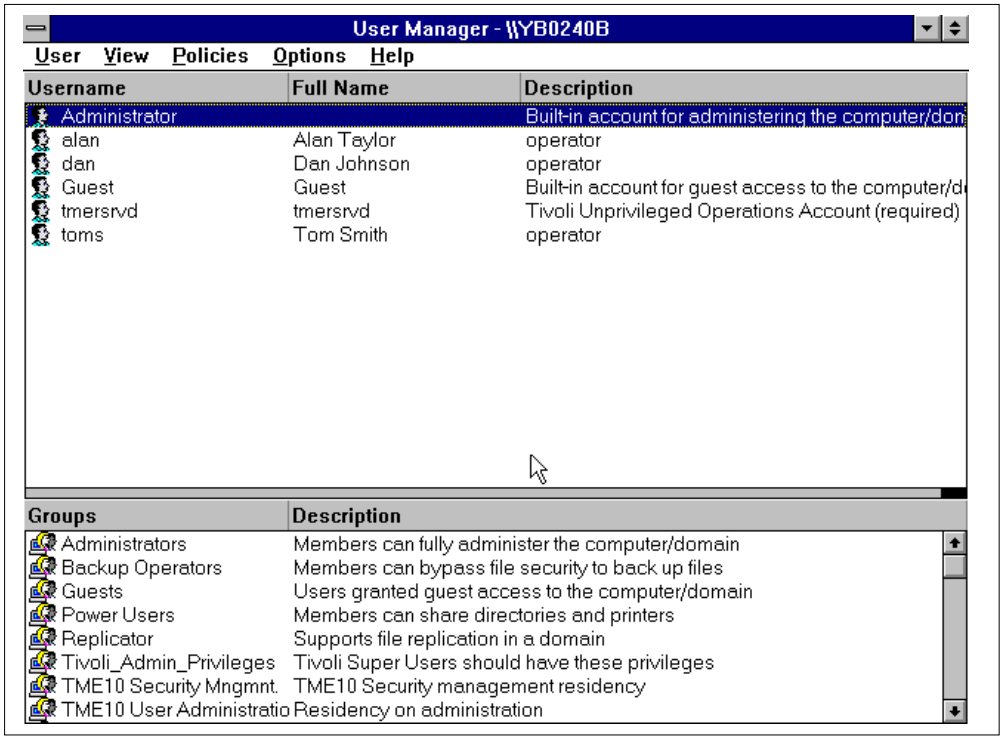


Figure 160. Users Defined on the Workgroup System yb0240b

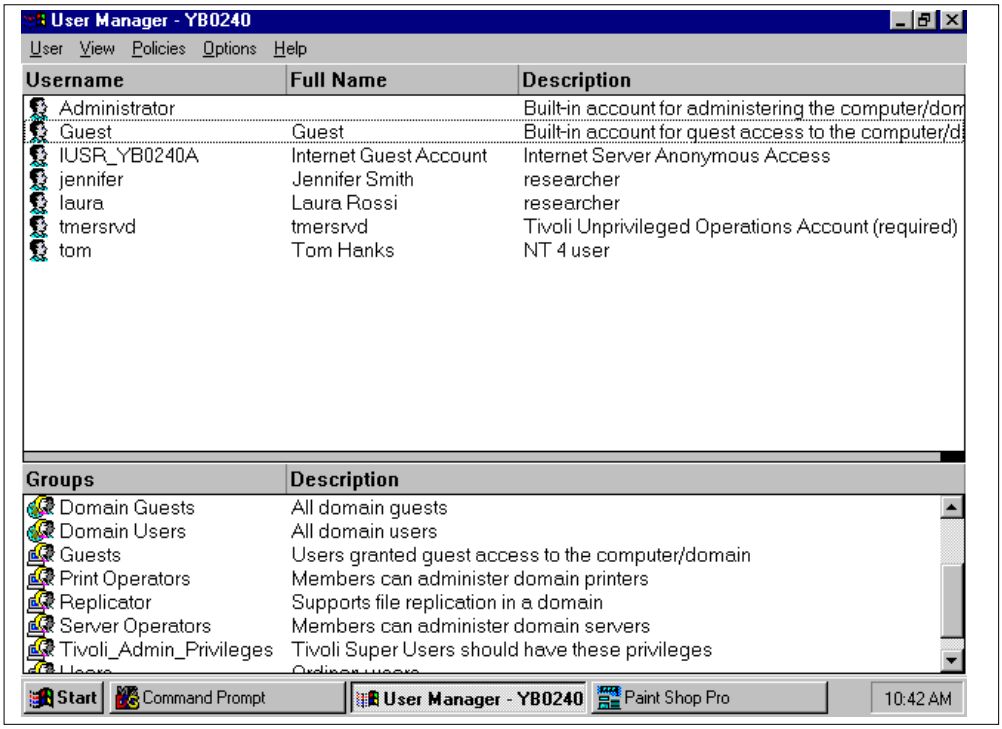


Figure 161. Domain Users Defined on the Primary Domain Controller yb0240a

6.4.2 Merging User Records

TME 10 User Administration allows you to merge two user records. This is useful when two different login names belong to a same user (the same person). The user information stored in the first record is treated as the master record. The second record is treated as the source record and is selectively merged into the master record (the terms first and second refers to the order in which the records appear in the command line operation `wmrgusrs`).

About Merging

This task is executable only from the command line. It is not available on the desktop.

Once two records are merged the source record is deleted from the profile.

Let us consider the following example. We created two accounts for Jack Smith on the yb0240a and yb0240b Windows NT machines: jack on yb0240a and jackie on yb0240b. We want to merge these user accounts in one account that will represent the user Jack Smith on both machines.

From the User Profile Properties window select **Profile**, then **Populate**. Choose the **Append to existing record list** populate option, and select the two Windows NT machines as endpoints from which to populate. Then click **Populate and Close.**

The User Profile Properties window will show two new accounts, jack and jackie, belonging to the same user Jack Smith:

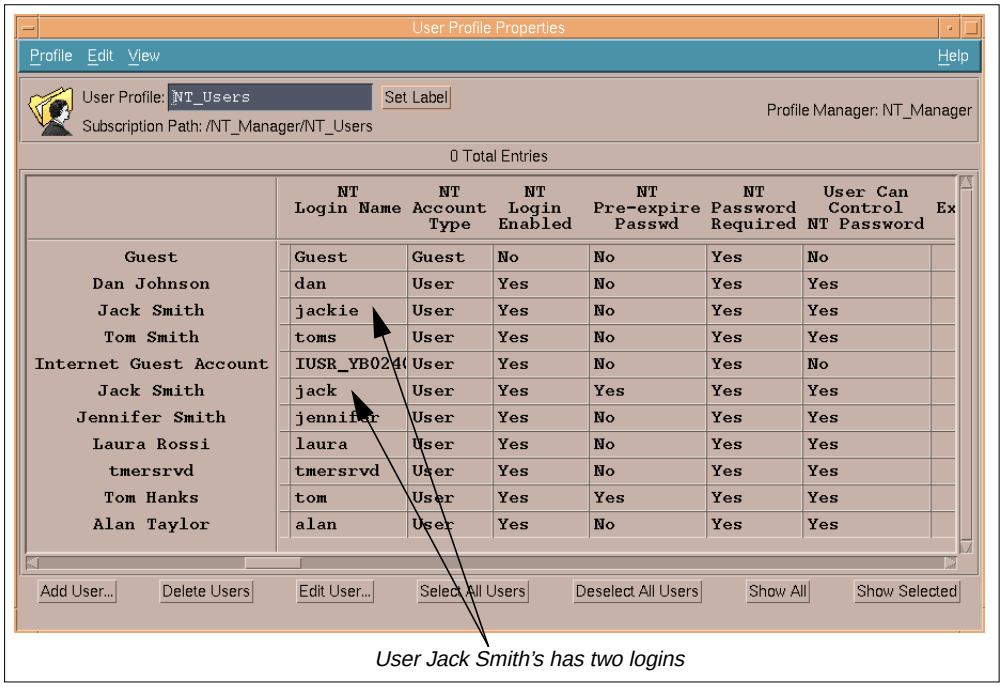


Figure 162. User Profile Properties Dialog

What we need to do now is to establish a master and a source record. Remember that when the merging operation occurs, the Windows NT account information of the master record overrides the NT account information of the source record. If the master record has only NT attributes and the source record has for example both UNIX and NT attributes, the NT account information will not be changed in the master record and the UNIX account information from the source record is added to the master record.

To merge the records, you have to use the `wmrgusrs` command, specifying the name and the location of the users you want to merge. We select the user account jackie as the master record and the user jack as the source record:

```
wmrgusrs @UserProfile:NT_Users jackie @UserProfile:NT_Users jack
```

The following figure shows the result of the operation:

```
# wmrgusrs @UserProfile:NT_Users jackie @UserProfile:NT_Users jack
User 'jack' has successfully been merged into the user 'jackie' in profile
@UserProfile:NT_Users
```

Figure 163. Merge Operation Output

Note

The option `-d` (to delete the home directory of the source record) and `-l` (to keep the home directory of the source record) are specific to UNIX accounts. They do not apply to Windows NT accounts.

Now you can check the effect of the operation on the user profile. Open the User Profile Properties window to get the following window:

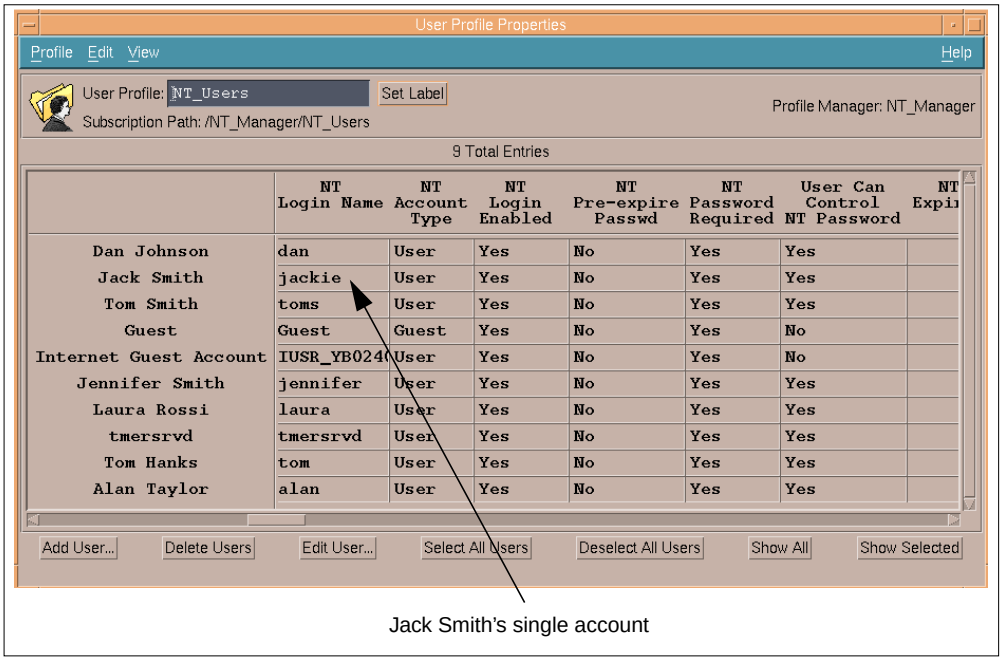


Figure 164. NT_Users User Profile after the Merge Operation

Attention

The two login names jack and jackie have been merged in the user profile. However, the account jack still exists on yb0240b and the account jackie does not exist on yb0240a. If you want the user Jack Smith to be able to login to both systems using the login name jackie, you then need to distribute the profile to both systems in order to have exactly the same user definitions for jackie on both systems.

You will then need to move all the files and directories that belonged to jack on yb02040b, to user jack. Also, rights and permissions on these files and directories will need to be changed so they belong to user jackie.

6.4.3 Adding, Deleting and Editing Users

This chapter explains the steps necessary to add Windows NT users to the user profile. After adding a user, you will be able to distribute the new user profile to the subscribers with the options that better match your requirements. From the User Profile Properties window, click on the **Add User..** button to get the following window:

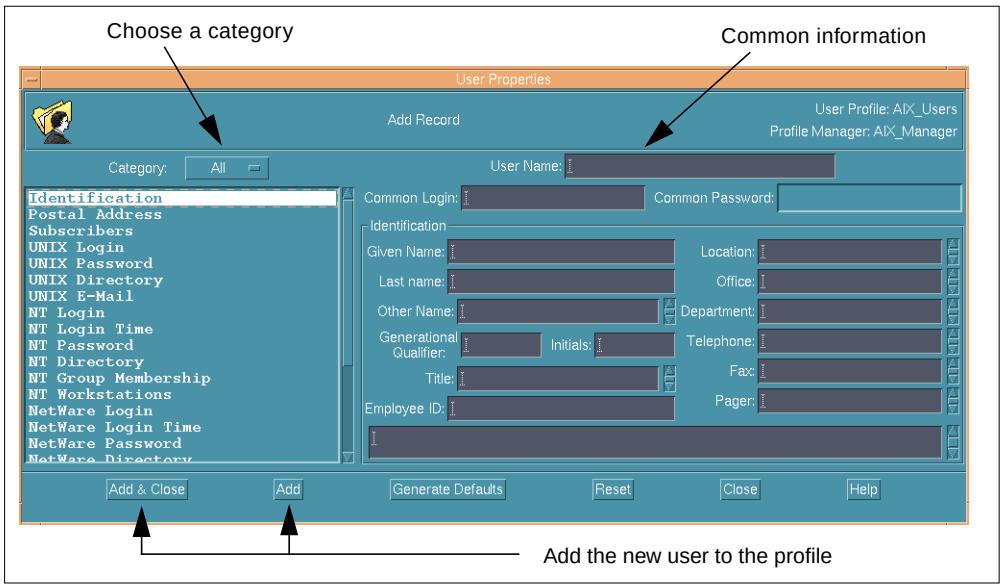


Figure 165. Add Record Window

This is the main window that allows you to add a user for a specific operating system or for all operating systems the defaults are defined for. By choosing a category from the Category list, you can narrow the number of choices to the operating system's specific attributes.

Common Information

Remember that you can simply enter the user name and click on **Generate Defaults** to have a common user login defined on UNIX, Windows NT and Netware systems. This new user will have the attributes set according to the default policies. Simply by editing the default policies, the administrator is allowed to set common conventions for every new user he/she will add to the user profile. It is possible, for example, to establish a consistent naming convention that avoids login name duplications.

In general, when you create a new record to a profile, you can:

- Manually add attribute information
- Use default policies to fill in the attribute information
- Do both

Note

If you just want to create a Windows NT user account and not fill out all the default attributes for UNIX or NetWare, you can disable default policies for UNIX and NetWare with the `wsetdefpol` command:

```
wsetdelpol DISABLED Unix NT_Users

wsetdelpol DISABLED NW NT_Users
```

Let us consider the specific case of an NT user creation, we assume it will be named Henry Taylor, with login name henry.

NT Login

Choose **NT** from the Category list, you will be prompted with the first NT specific dialog, the **NT Login,** as shown in the following figure:

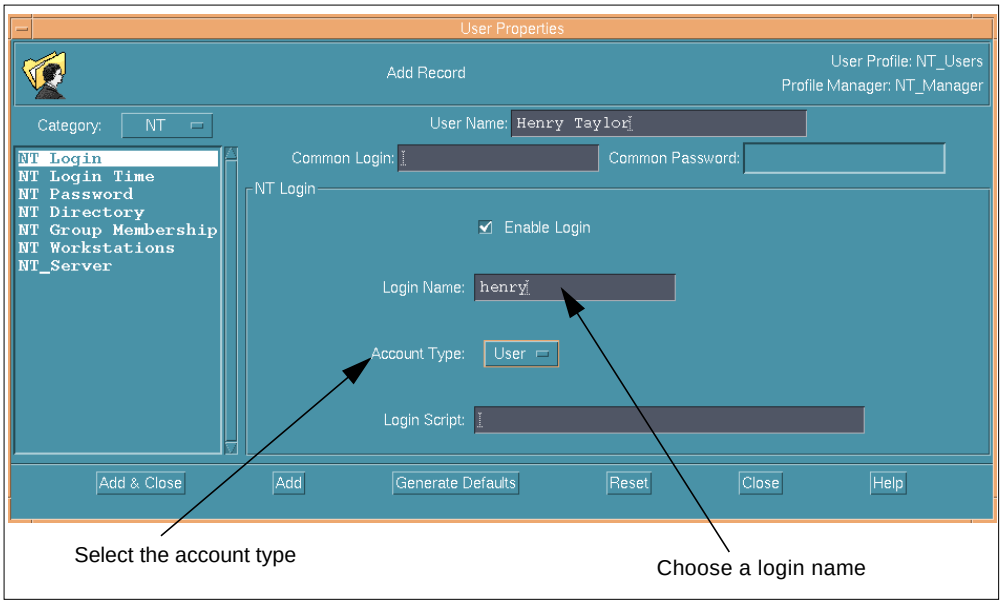


Figure 166. User Properties: NT Login Dialog

Select the **Enable Login** check box to allow this user to log in and select an appropriate account type from the *Account Type* pop-up menu, the available options are:

- None: indicates an invalid account type
- Admin: adds the user to the Domain Administrator group
- User: adds the user to the Domain Users group
- Guest: adds the user to the Domain Guest group

You can also specify a login script for the new created user in the Login Script field. You must specify the name and the path of the script, for example to execute each time the user logs in the batch file CONNECT.BAT, you will put in the Login Script field the following :

```
C:\BATCH\CONNECT.BAT
```

This will execute the `CONNECT.BAT` script located in the `C:\BATCH` directory.

NT Login Time

Now you can select **NT Login Time** from the Category list, to get the following window:

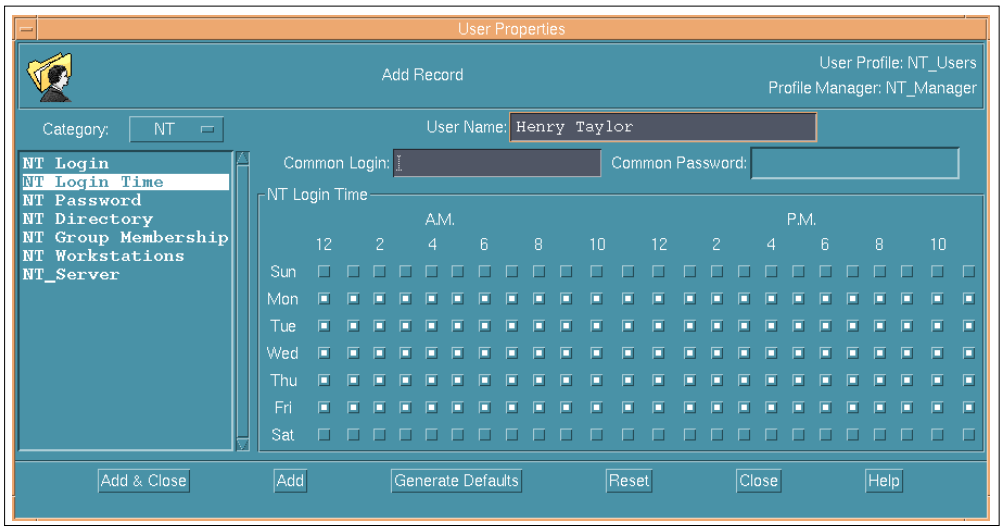


Figure 167. User Properties: NT Login Time

This window allows you to select the periods of time the new user can login with this account. By default, all check boxes are selected and the users can connect at any time. In Figure 167, we allow the user to log in at any time during the week except Saturday and Sunday.

NT Password

Select **NT Password** from the Category list, to get the following window:

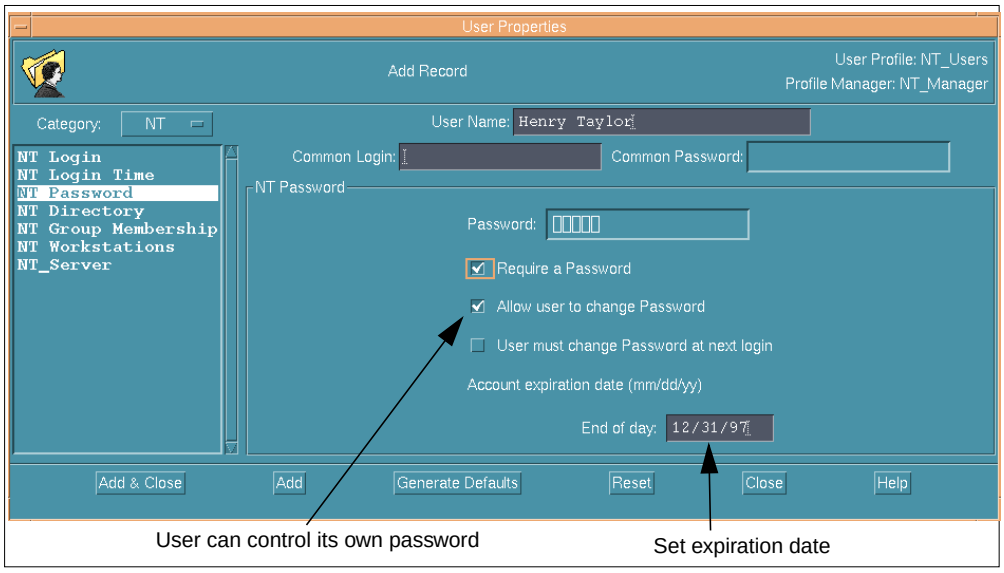


Figure 168. User Properties: NT Password

We set the user password and allowed the user to control it. If this check box is not selected the user password is controlled by the administrator. The user cannot change his/her own password. It is the same with UNIX users. You can also force the user to change the password when the user logs in for the first time after the profile has been distributed. We also selected an expiration date for the password, just by entering the expiration date in the month/day/year format. The user password will expire at the end of the day specified in the End of Day field.

Attention

Windows NT passwords are not populated. When populating, the login name is used as the password. However, when disbributing the profile, the user pssword will not be changed except if the administrator changed the password in the user profile.

If the user is allowed to change his password, he can change it by using the Change Password utility obtained by entering Ctrl-Alt-Del or by using the TME 10 command `wpasswd`.

The `wpasswd` command is available on a Windows NT Managed Node. It is usually installed on the Managed Node under the C:\usr\local\tivoli\bin\w32-ix86\bin directory.

This command allows the user to change his password in the user profile. If the `-l` option is used with the `wpasswd` command, the password is changed in both the Windows NT system and in the user profile.

NT Directory

In the Category list, select **NT Directory** to get the following window:

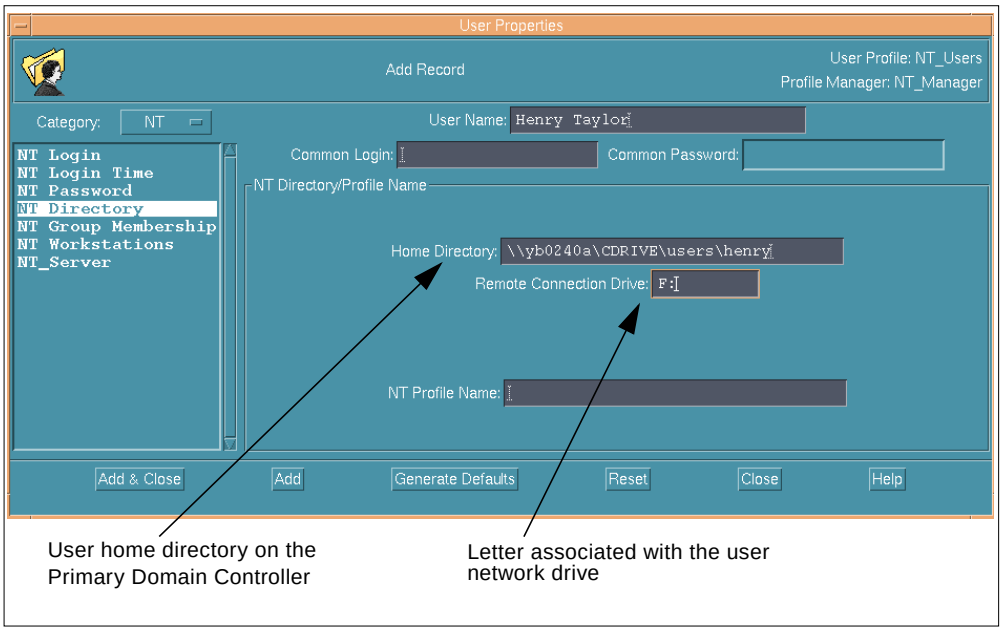


Figure 169. User Properties: NT Directory

Note

The NT_Server subcategory that shows up in the Category scroll list is not a default option. This entry has been added using Application Extension Facility (AEF) in order to be able to automatically create a home directory on a specific Windows NT server for the user when the profile is distributed.

In this window you can specify the user home directory. This directory is the one that will be used by default by the users to store personal files. The home directory can be a local directory or a shared directory defined on a specific Windows NT server. The Windows NT server can be the Primary Domain Controller itself, or a Windows Server (member server). If the home directory is a shared directory, you must specify the Universal Naming Convention (UNC) name for that directory:

```
\\<server_name>\<shared_directory_name>\<directory_name>
```

Figure 169 shows an example where the home directory for the user henry will be F:\users\henry and where F: is a network drive connected to the yb0240a machine (PDC). The C: drive on yb0240a has been shared as CDRIVE. Therefore after login, the user henry will work by default in F:\USERS\HENRY corresponding to C:\USERS\HENRY on the server.

Attention

If the directory C:\USERS\HENRY does not already exist on the server, that directory will not be created automatically by TME 10 User Administration. This is not a standard product feature. However, you will find in “Creating NT Home Directories” on page 223 a way to automatically create a Windows NT home directory. This is done by using Application Extension Facilities (AEF) to customize the User Administration interface for Windows NT and by adding an action that will create that home directory once the user profile is distributed.

NT Group Membership

TME 10 User Administration does not allow you to manage Windows NT groups. However, you can specify a group or several groups the user belongs to. These groups must be directly created on Windows NT.

The NT Group Membership option allows you to specify to which groups the user belongs. Select **NT Group Membership** in the Category list to get the following window:

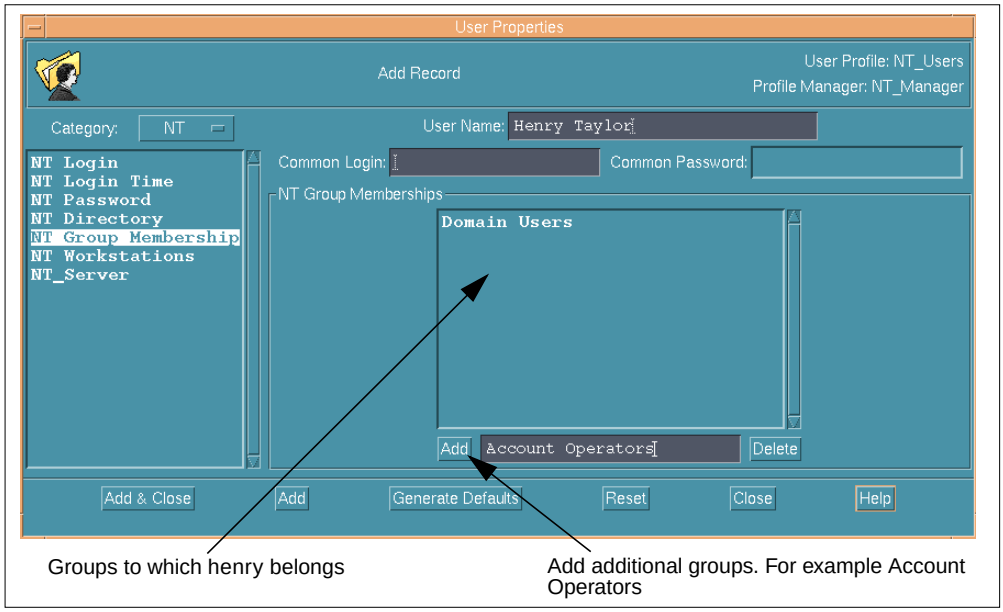


Figure 170. User Properties: NT Group Membership

This dialog box allows you to define the NT group membership for user henry. You simply need to enter the name of the group to which this user belongs and press the **Add** button. This way the group is added to the NT Group Membership scrolling list.

NT Workstations

It is possible to define a list of workstations from which the user is allowed to log in to the Windows NT domain. By default, the user can login from any workstation in the domain.

Select **NT Workstations** in the Category scrolling list to display the following panel:

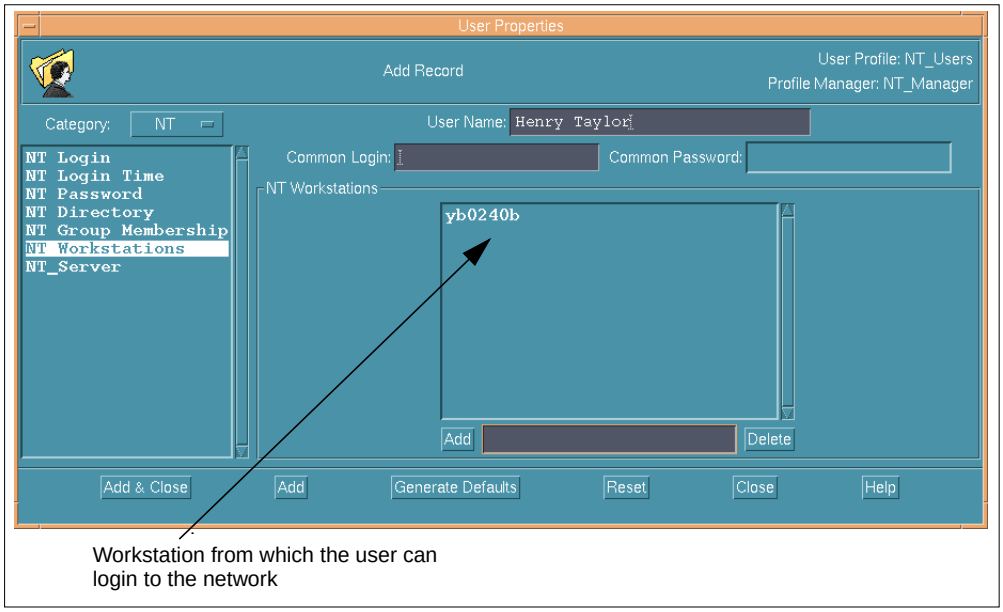


Figure 171. User Properties: NT Workstations

You can specify exactly from which workstation(s) the user can login to the network simply by entering the workstation name and by clicking the **Add** button. If you leave the scrolling list empty, this means that you allow the user to login from any workstations. In our example, we allow the user henry to login only from the yb0240b Windows NT machine.

NT_Server

In order to automatically create the home directory for a user on the Windows NT server, TME 10 User Administration must know the name of the server on which you want to create that home directory. A new attribute is necessary to perform that.

TME 10 User Administration has been customized to provide a new entry in the Category scrolling list. By selecting this option, you get the following window:

Y

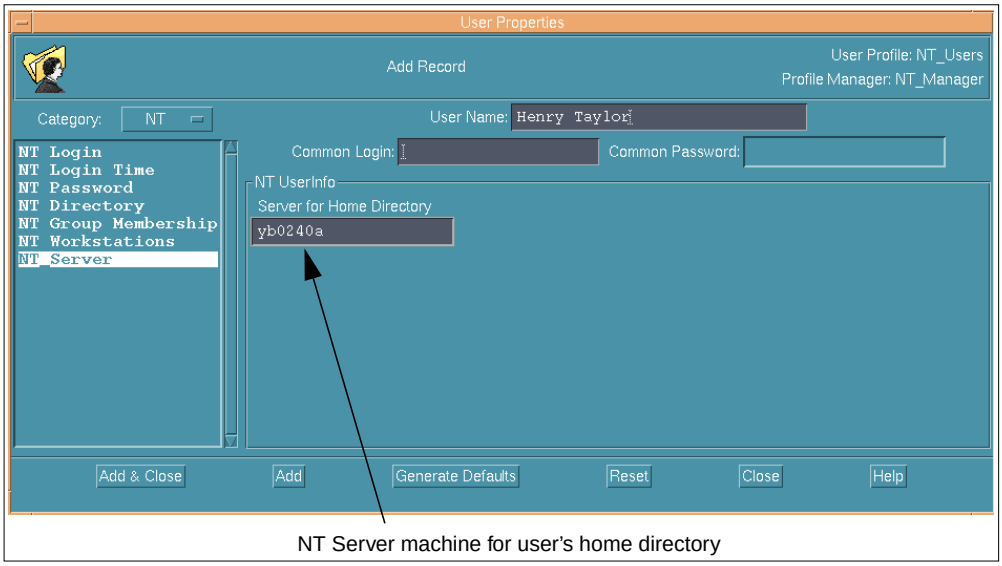


Figure 172. User Properties: NT_Server

This dialog box allows you to specify the name of the Windows NT server on which you want to create the home directory for the user. You just need to fill out the Server for Home Directory field and put the server name in it. In our example, we chose the PDC as the server. The NT_Server attribute is not a user profile standard attribute, it has been added by an AEF procedure that is documented in the following section.

6.4.4 Creating NT Home Directories

TME 10 User Administration does not create home directories for Windows NT users when the profile is distributed unless you customize the application to do it. In this section, we show an AEF customization example that allows you to automatically create the corresponding user home directory on a specific server.

AEF, provided with the TME 10 Framework, allows you to customize your desktop. AEF might not be installed on your TMR server. Installing AEF is easy. As with any other TME 10 application, you just need to go to the Tivoli desktop and select **Install**.

AEF is used in this example to add to the GUI a subcategory that we called NT_Server in the NT Category scrolling list. This subcategory allows us to specify the name of the Windows NT server on which we want to create the home directory for a user.

Then, we will add an action to the user profile. This action will be executed right after the profile distribution and will actually create the home directory.

You will find below all the steps necessary to create that subcategory and add the home directory creation action:

1. Add a new property to the user profile:

   ```
   waddprop @UserProfile:<profile_name> "NT_Server" ""
   ```

   In our case, we entered the following:

   ```
   waddprop @UserProfile:NT_Users "NT_Server" ""
   ```

This new property is then added as a column into the User Profile Properties window, as shown in the following figure:

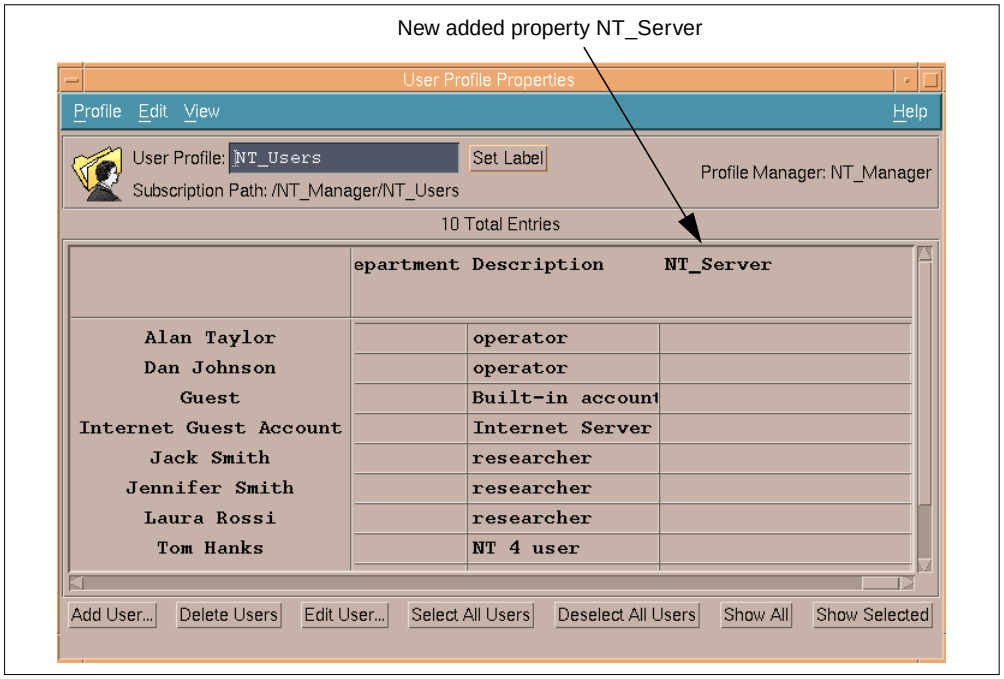


Figure 173. User Profile with New Property NT_Server

The NT_Server attribute indicates the Windows NT machine on which the user home directory will be created.

You can check that the new attribute has been properly added in the User Profile Properties by clicking **Edit** -> **Default Policies** to get the following window:

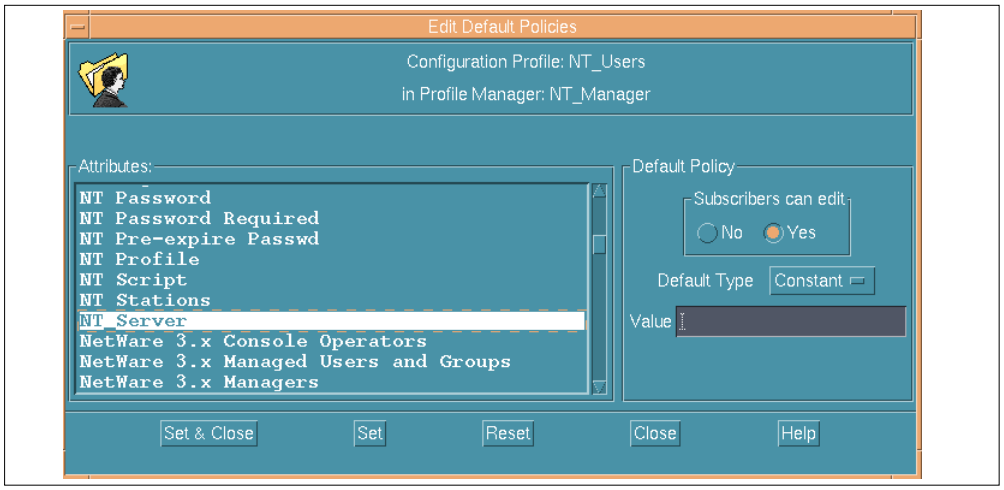


Figure 174. NT_Server Default Policy

You will find that the waddprop operation has also defined a default policy Constant for the NT_Server attribute.

2. Create the NT_UserInfo subcategory in the NT category by issuing the following command:

   ```
   wcrtusrsubcat -m "NT_Server" -c NT NT_UserInfo
   ```

   NT_UserInfo is the name of the dialog that will be displayed when selecting NT_Server in the NT Category scrolling list. Figure 175 shows the new NT_Server entry in the NT Category scrolling list.

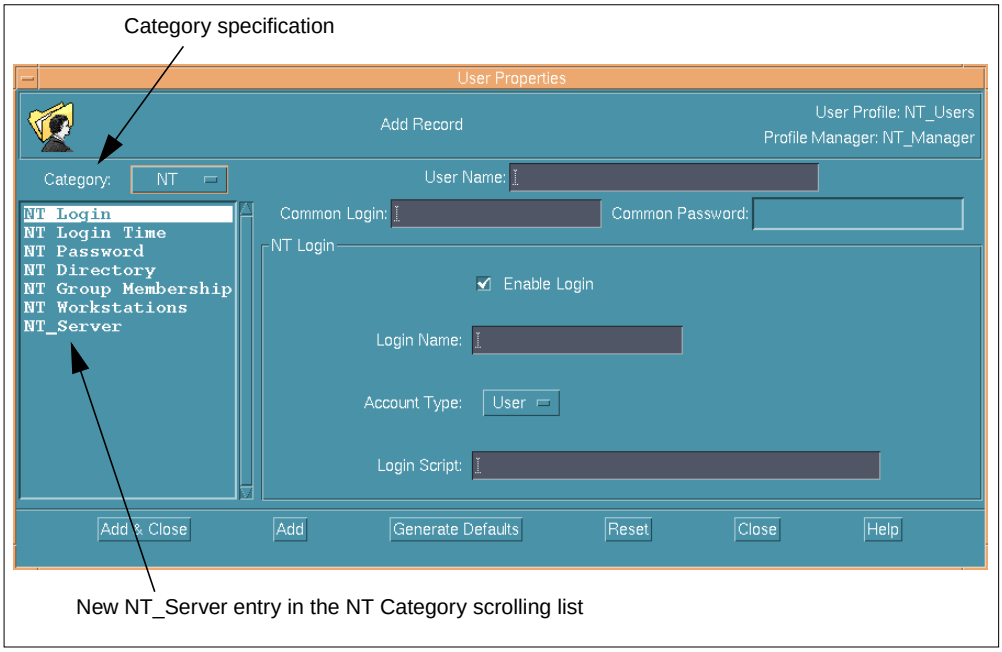


Figure 175. NT_Server New Option

3. Create the dsl (Dialog Specification Language) source file /tmp/nt_server.dsl. This file should look like the following:

```
Partial Dialog
{
        Gadgets
        {
            Group
            {
                Attributes
                {
                    Border = YES;
                    Name = NT_UserInfo;
                    Title = "NT UserInfo";
                    TitlePos = TOP;
                    Visible = NO;
                    GridHorizontal = 0;
                    GridVertical = 0;
                    ChildColumnAlignment = STRETCH;
                    ChildRowAlignment = STRETCH;
                }

                Gadgets
                {
                    Group
                    {
                        Attributes
                        {
                            Layout = VERTICAL;
                            Name = NT_UserInfoContainer;
                            ChildColumnAlignment = LEFT;
                            ChildRowAlignment = STRETCH;
                        }

                        Gadgets
                        {
                            Text
                            {
                                Name = NT_Server;
                                Title = "Server for Home Directory";
                                TitlePos = TOP;
                                ChildColumnAlignment = LEFT;
                                ChildRowAlignment = LEFT;
                            }

                        }
                    }

                }
            }
```

4. Put the dialog in for all user profiles by entering the following command:

   ```
   dsl /tmp/nt.server.dsl | wputdialog -r UserGui NT_UserInfo
   ```

5. Create a shell script called mk_nt_home_dir.sh. This shell script will be executed when the profile is distributed. The shell script should look like the following:

```
#!/bin/sh

if [ $# != "2" ]
then
        echo "Usage: mk_nt_home_dir < hostname > < User > ">>/tmp/debug
        exit 1
fi

DIRMODE=0777
DIROWNER=Administrator
DIRGROUP=Administrators
HOST=$1
DIRPATH="c:/users/"$2
MNO=`wlookup -r ManagedNode $HOST`

idlcall -T top $MNO \
"TMF_ManagedNode::Managed_Node::make_directory" \
"\"$DIRPATH\" { $DIRMODE -1 \"$DIROWNER\" -1 \"$DIRGROUP\" -1 } 1" >> /tmp/debug
2> &1
```

Note that in this script, we create the home directory under C:\users. And the home directory will be C:\users\<login_name>. You can of course customize this shell script for your own needs.

6. Add an action to the user profile when the profile is distributed. That action will be executed on the TMR server itself. Enter the following command:

   ```
   waddaction -c -a @UserProfile:<profile_name> mk_nt_home_dir \
   args='$NT_Server','$nt_logon' < mk_nt_home_dir.sh
   ```

   In our example, enter:

   ```
   waddaction -c -a @UserProfile:NT_Users mk_nt_home_dir \
   args='$NT_Server','$nt_logon' < mk_nt_home_dir.sh
   ```

   `$nt_logon` corresponds to the login name of the user. `$NT_Server` is the name of the Windows NT server where the home directory will be created.

If you want to retrieve the code corresponding to the NT_Server panel, you need to perform the following steps:

1. List all the dialogs associated with the user interface by issuing:

   ```
   wlsdialog -r UserGui
   ```

   You will get the following output:

```
dialog name (customization status)

AddEditUser
DelUserConfirm
EmptyPage
IdentificationGroup
NDSBrowser
NTDirectoryGroup
NTGroupMemGroup
NTLoginGroup
NTLoginTimeGroup
NTPasswordGroup
NTWorkstationsGroup
NW3ManUserGroup
NW3ManagersGroup
NW3MgmtRightsGroup
NWAddrRest
NWDirectoryGroup
NWForEmail
NWForMailGroup
NWGroNWLoginGroup
NWLoginTimeGroup
NWMailGroup
NWNetworkAddrGroup
NWPasswordGroup
NWSecurityGroup
PostalAddressGroup
SubscribersGroup
UDirectoryGroup
UEmailGroup
ULoginGroup
UPasswordGroup
UserProps
UserPropsIcon
NT_UserInfo (resource-wide customization)
upMemGroup
```

Figure 176. Dialog List

You can find the NT_UserInfo subcategory.

2. Retrieve this dialog by issuing the following command:

   ```
   wgetdialog -r UserGui NT_UserInfo > /tmp/nt_server.d
   ```

3. Reverse compile the file that has been retrieved:

   ```
   rdsl /tmp/nt_server.d > /tmp/nt_server.dsl
   ```

4. You are then able to view the code used for the dialog by issuing the following command:

   ```
   vi /tmp/nt_server.dsl
   ```

   You will get the output shown below:

```
Partial Dialog
{
        Gadgets
        {
            Group
            {
                Attributes
                {
                    Border = YES;
                    Name = NT_UserInfo;
                    Title = "NT UserInfo";
                    TitlePos = TOP;
                    Visible = NO;
                    GridHorizontal = 0;
                    GridVertical = 0;
                    ChildColumnAlignment = STRETCH;
                    ChildRowAlignment = STRETCH;
                }

                Gadgets
                {
                    Group
                    {
                        Attributes
                        {
                            Layout = VERTICAL;
                            Name = NT_UserInfoContainer;
                            ChildColumnAlignment = LEFT;
                            ChildRowAlignment = STRETCH;
                        }

                        Gadgets
                        {
                            Text
                            {
                                Name = NT_Server;
                                Title = "Server for Home Directory";
                                TitlePos = TOP;
                                ChildColumnAlignment = LEFT;
                                ChildRowAlignment = LEFT;
                            }

                        }
                    }

                }
            }
```

Figure 177. nt_server.dsl

6.4.5 Synchronizing System Files with User Profiles

If a Windows NT system administrator directly adds or deletes a user on an Windows NT system, the user profile will not be longer consistent with the system files that it manages. The synchronize function provides a way to keep the user profile and the system files consistent by showing you which records in the profile do not match the system files entries. The synchronize function shows you if a user has been added in the system and not in the profile or if a user has been deleted from the system and not from the profile or if a user definition has been modified (attributes changed). Then, if desired, you can ask to update the profile.

Let us consider the following example:

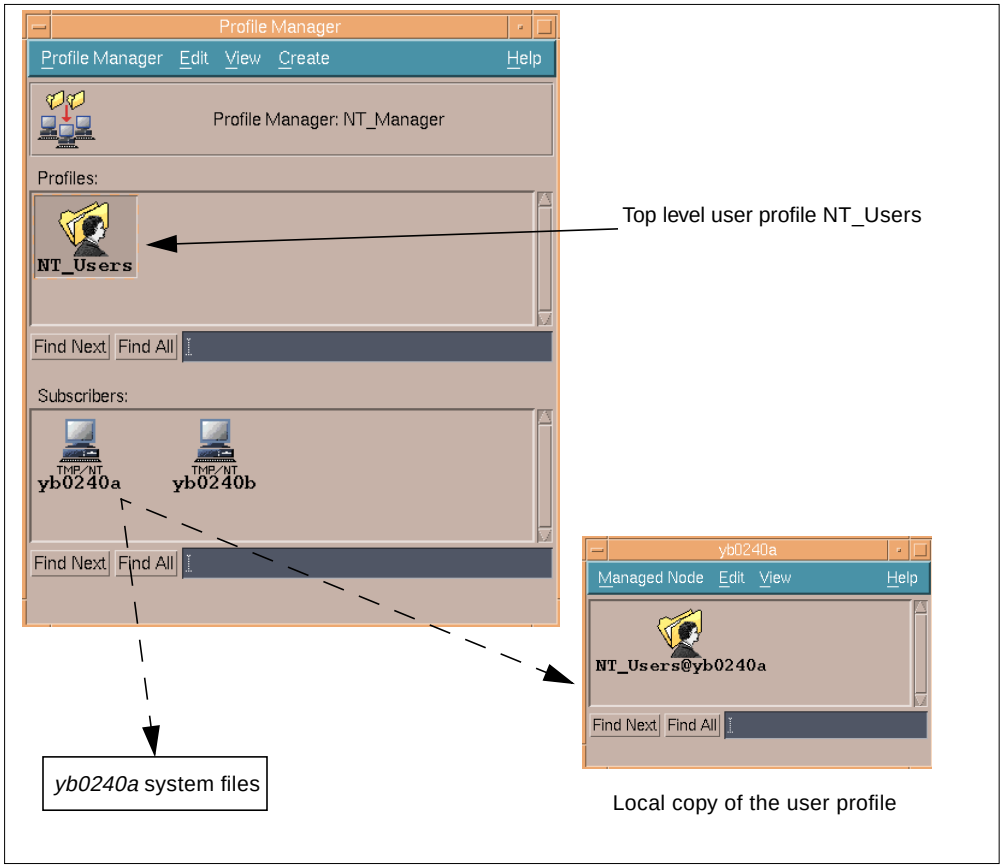


Figure 178. Synchronizing a User Profile

Let's suppose that a system administrator directly adds a new Windows NT user named todd on the machine yb0240a. The system files no longer match the user profiles (neither the local copy at the managed node level or the top level profile).

To update the local copy of the user profile, NT_Users@yb0240a, select **Synchronize** from the Managed Node pop-up menu or from the local user profile pull-down menu. You will get the list of all the profiles available for the Managed Node:

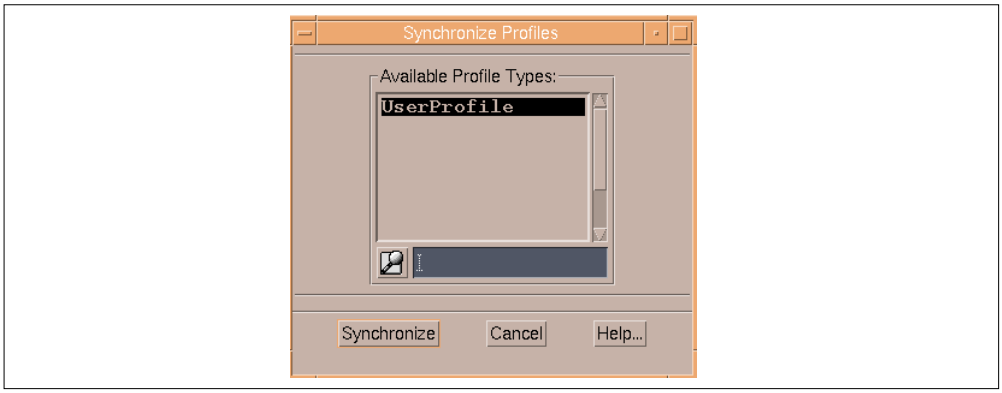


Figure 179. Available Profile for the Managed Node yb0240a

A Managed Node may have several available profile types. It may be a subscriber of User Profiles, Sentry Profiles, Courier Profiles and so on. In our case we have only one available type of profile.

On Figure 179, click on the **Synchronize** button to display the discrepancies between the user profile and system files, as shown in the following figure:

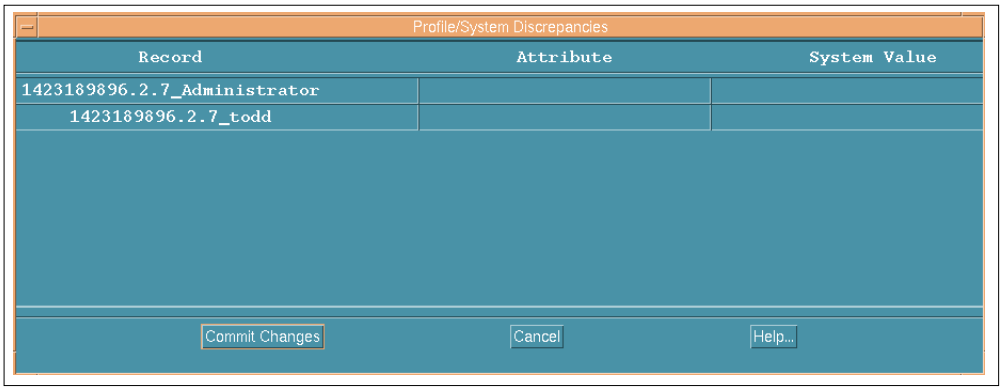


Figure 180. Profile/System Discrepancies Window

We find in this window the user Administrator (that has not been added to the user profile during the populate operation) and the manually added user todd. You can click on the **Close** button and make the changes by manually adding the user to the user profile or click on the **Commit Changes** button to copy the system files information into the user profile. If you click on the **Commit Changes** button, you will get the following window:

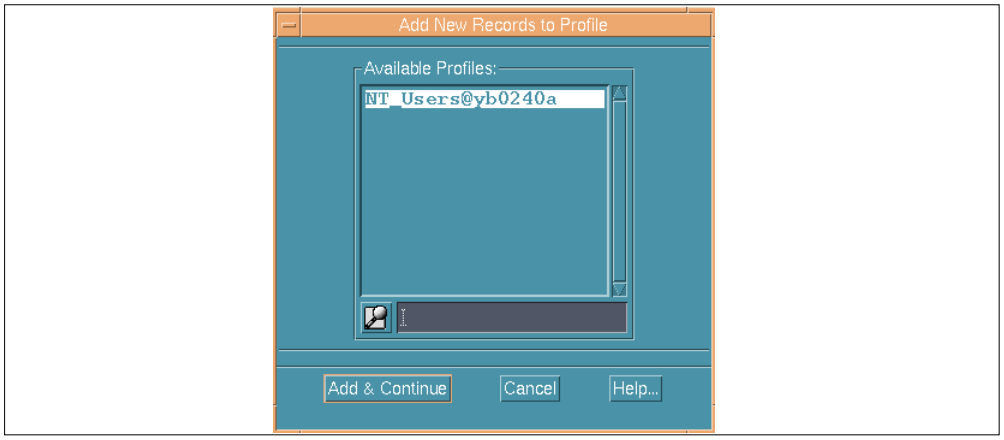


Figure 181. Available Profiles on the NT Managed Node

This window allows you to select the user profile to update. Click on **Add & Continue** to get the following window**:**

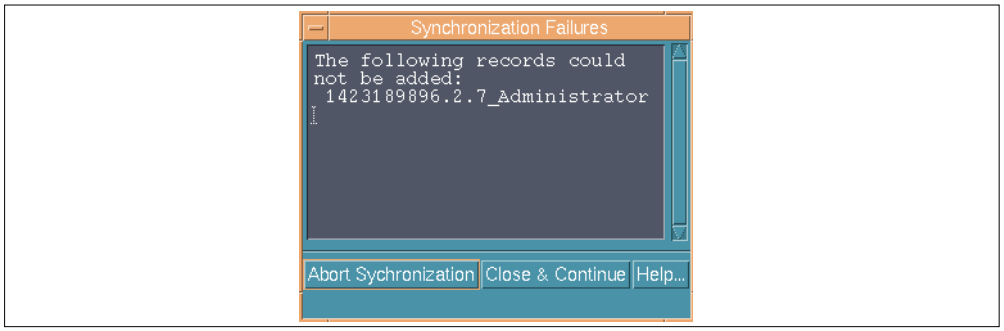


Figure 182. Synchronization Failures

This window warns you that the user Administrator has not been added to the user profile (because the validation policy prevents adding this user). Press **Close & Continue** to finish the operation. NT_Users@yb0240a is now updated with the user todd, as shown in the following figure:

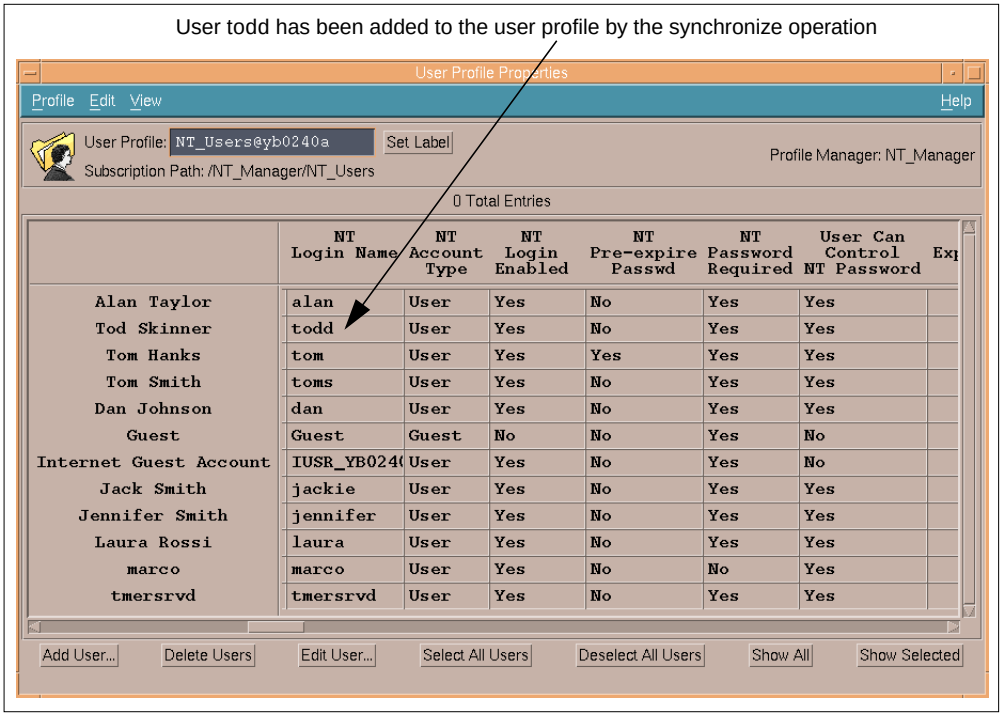


Figure 183. Updated NT_Users@yb0240a User Profile

Note that the synchronize function updates the profile stored at the Managed Node. It does not update the top level profile. To update the top level user profile it is necessary to use the `wchkusrs` command. There are no options on the GUI to perform that. To add the user todd to the top level profile, enter the following:

```
wchkusrs -s @UserProfile:NT_Users -u @UserProfile:NT_Users
@ManagedNode:yb0240a
```

where :

`-s` specifies the source profile (the profile to compare with the system files);

`-u` specifies the profile to update;

`@ManagedNode:<Managed_Node_Name>` specifies the subscriber to synchronize with.

By issuing that command, you will get the following output:

```
Checking endpoint @ManagedNode:yb0240a...
These users were found in the system but not in the database:
    Administrator
    todd
The following records in the profile @UserProfile:NT_Users could not be modified
 or added:
    Administrator

These differences have been updated in the profile.
```

Once again we find that the user Administrator has not been added (which is normal according to the validation policies), the user todd has been successfully added to the top level user profile, as shown in the following figure:

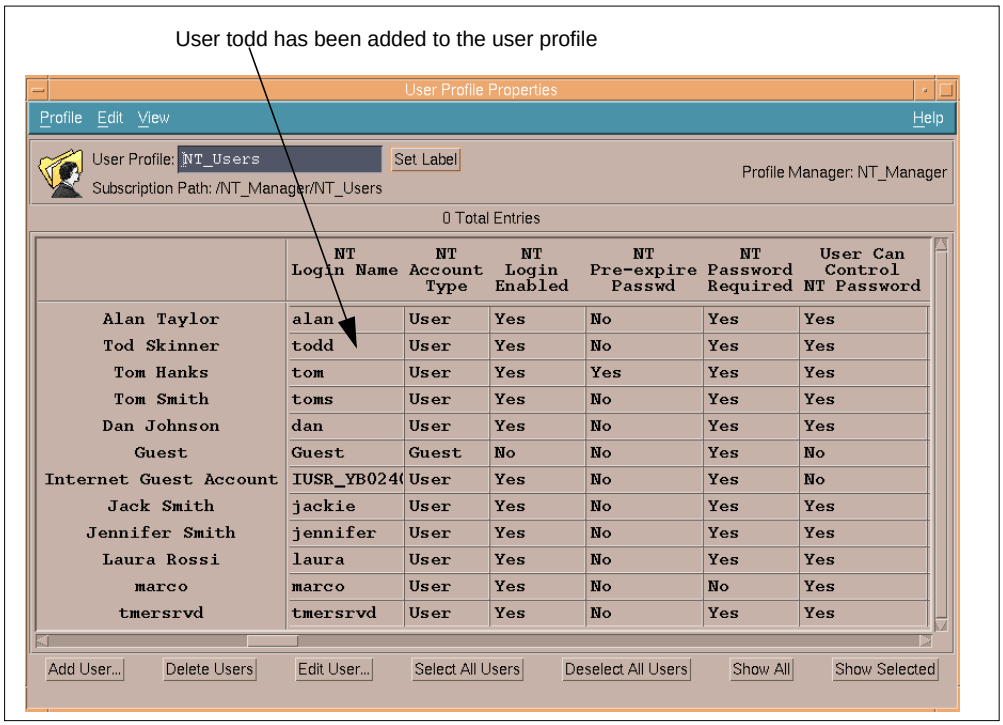


Figure 184. Updated NT_Users User Profile

The synchronize function is working properly for Windows NT users.

6.5 Managing NetWare Users

This section describes how to manage NetWare 4.1 users with TME 10 User Administration. Functions provided by TME 10 User Administration for NetWare are illustrated by simple examples.

6.5.1 Populating a User Profile

Populate is the function of retrieving user definitions from system files and adding them as records to a profile. In this section, we will populate a user profile from a NeWare 4.1 server running NDS.

Reminder

Before you populate a user profile from a NetWare 4.1 PC Managed Node, you must run the `wsetnds` command. This command allows you to access the NetWare NDS tree.

The `wsetnds` command sets the account that is used to log in to the NDS tree when you perform a user profile populate or distribute operation. This account should have Admin level authorization. This information is stored in an encrypted format on the NetWare endpoint.

You should run the `wsetnds` command before you attempt an operation on a NetWare 4.1 endpoint. In addition, any time you change the login name, the password, or the NDS context of the account used to log in to the NDS tree, you need to run the `wsetnds` command again.

The following example sets the account information for the yb0240c NetWare NDS server:

```
wsetnds -l Admin -p password -c ITSO @PcManagedNode:yb0240c
```

where:

`-l Admin` is the login name of the account used to login to the NDS tree

`-p password` specifies the password for the account

`@PcManagedNode:yb0240c` is the name of the NetWare PCManagedNode

To populate a user profile in NetWare, you can use the following steps:

1. From the profile manager, double-click on the user profile icon (in our case NW_Users) to display the User Profile Properties window as shown in Figure 185.

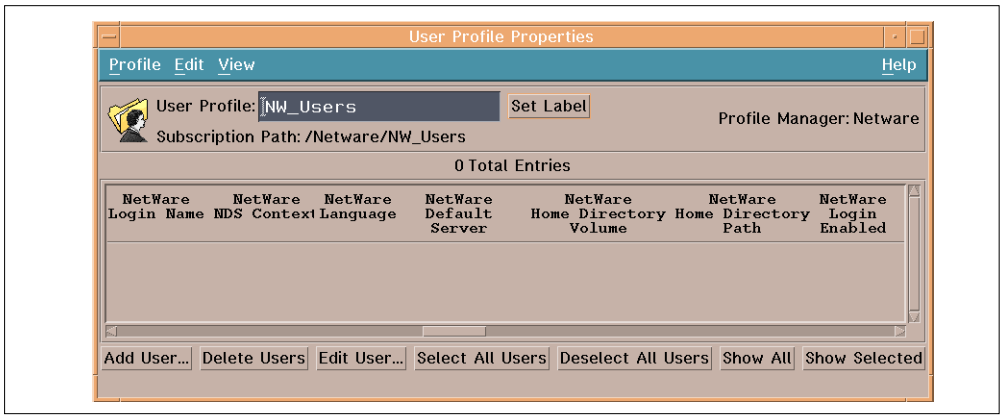


Figure 185. User Profile Properties Dialog

2. Select **Profile**, then **Populate** to display the Populate Profile dialog shown below:

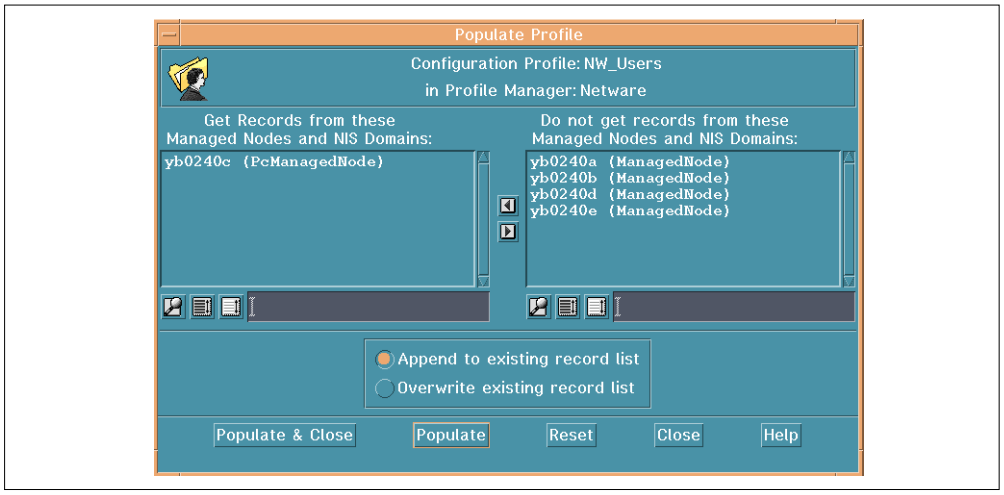


Figure 186. Populate Profile Dialog

3. From the **Do not get records from these Managed Nodes and NIS Domains** scrolling list, select the TME 10 resources from which to populate the profile. In our example, we select *yb0240c* corresponding to the NDS server. Press the left arrow button to move the selected resource into the Get Records from these Managed Nodes and NIS Domains scrolling list.
4. You have two options for populating the profile:
   - Append to existing record list. This option adds the new records to the existing records in this profile. You should use this option when populating an existing profile that contains records you want to keep.
   - Overwrite existing record list. This option replaces the user records in the profile with new records retrieved from the endpoint system files. You should be very careful with this option, because, if you choose this option, all the records in the profile will be lost.

   Since it it the first time we populate the profile, we chose the **Overwrite existing record lis**t option.

5. Press the **Populate & Close** button to add the records to the profile and close the dialog. TME 10 User Administration adds the accounts from the specified system to the profile.

   If you did not change the validation policies, you should get the following error message:

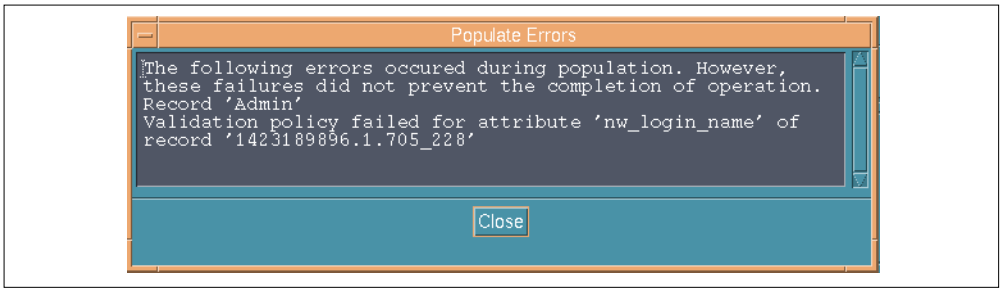


Figure 187. Populate Errors Window

   The window shown in Figure 187 shows that the NetWare user Admin did not pass the validation policies. This is normal. If you want user Admin to be added as a record to the profile, you need to modify the validation policies.

It is also possible to populate the profile by using the command line interface. The following provides an example of how to populate a profile with the `wpopusrs` command:

```
wpopusrs -o -l @PcManagedNode:yb0240c @UserProfile:NW_Users
```

where:

`-o` specifies to overwrite the current contents of the profile,

`-l` leaves the existing home directory as is. This means that the home directory, information is taken from the NetWare server and kept as is

`@PcManagedNode:yb0240c` is the name of the system from which to populate,

`@UserProfile:NW_Users` is the name of the profile to populate.

Note on Passwords

When you populate from a NetWare NDS tree, user passwords are not retrieved by the populate operation and the records that are created use the login name as the password. However, distributing the profile will not overwrite the actual password stored in the system files except if you changed it in the user profile itself.

6.5.2 Merging User Records

TME 10 User Administration allows the administrator to merge two user records. This operation is only supported from the command line interface.

If the records to be merged are in different user profiles, the user profiles must be in the same TME 10 Management Region, or there must be a one or two way connection between these regions.

Note

Two user records from two different user profiles that are in the same Profile Manager or in two different profile managers cannot be merged.

This feature is particularly important if the same user has two different login names on the same server or on two different servers. Once the user profile is populated, you might want to merge these two records. When merging the two records, you must specify a master record and a source record. After the merge, the source record is deleted from the profile.

In the following example, we show how to merge two user records defined in the same user profile.

Lets suppose that Jorge Campos had for historical reasons two accounts on the same NetWare server: campos and jcampos. After populating the profile NW_Users from the NetWare PC Managed Node, we get the two accounts in the profile as shown in Figure 188.

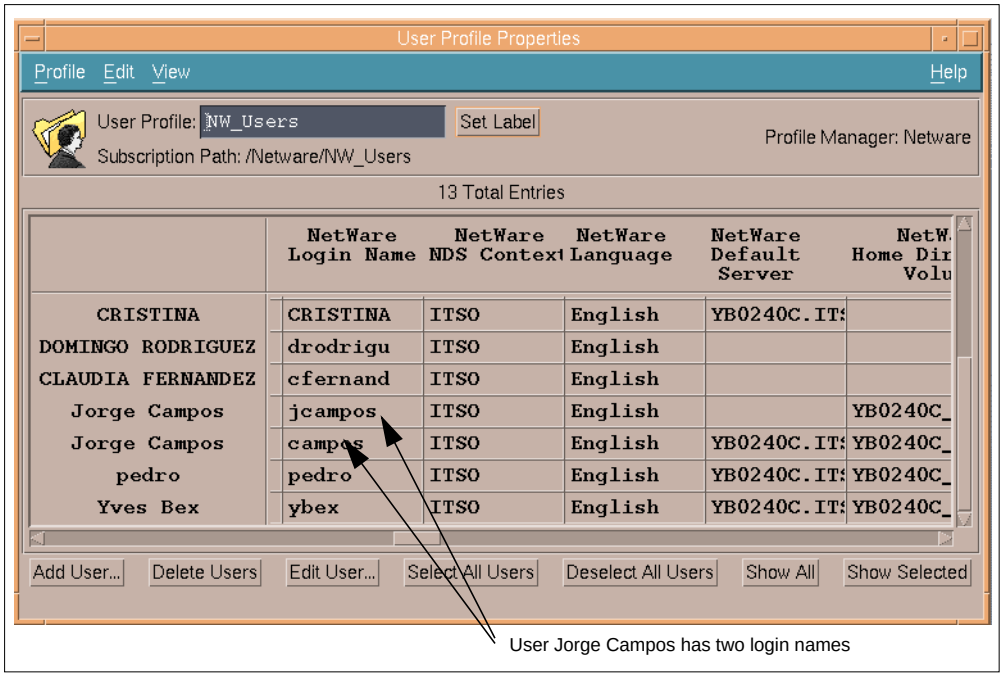


Figure 188. NW_Users User Profile

To simplify our user administration, we want to merge user jcampos into user campos. campos will be the master user record and jcampos the source user record.

To merge the records you need to use the `wmrgusrs` command.

Note: We used the option `-d`. When this option is used, the source record is deleted from the profile. If you use the option `-l`, the source record is not deleted from the profile.

The command is as follow:

```
wmrgusrs -d @UserProfile:NW_Users campos @UserProfile:NW_Users jcampos
```

where:

`@UserProfile: NW_Users` specifies the name of the user profile containing the user records to merge,

`campos` is the master record,

`jcampos` is the source record.

If the command has been successful, you should get the following output:

```
$ wmrgusrs -d @UserProfile:NW_Users campos @UserProfile:NW_Users jcampos
User 'jcampos' has successfully been merged into user 'campos' in profile
@UserProfile:NW_Users
```

You can check the effect of the merge operation in the user profile. Open the NW_Users profile; the window should look like the following:

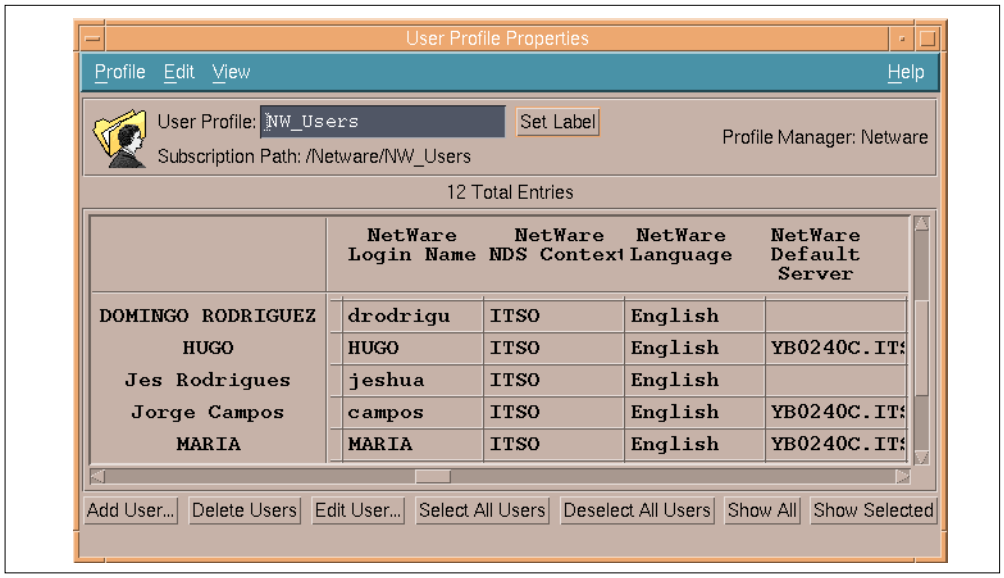


Figure 189. User Profile Properties Window After Merging

Note that now, only one entry exists in the profile for user Jorge Campos.

Attention!

The merge operation merges the two users in the profile. This does not mean that the users are merged on the NetWare server itself. You might need, on the server, to move the files and directories that belonged to jcampos to campos' home directory and check the ownership and permissions of these files so they belong now to user campos.

If you populate the NW_Users profile from two NetWare servers (for example Server_A and Server_B) and have a similar situation; Jorge Campos has two

accounts with two different names, one on Server_A, the other one on Server_B, you would be able to merge the two records in the profile.

However, you will then need to distribute the profile to the two PC Managed Nodes in order to create the campos account on the Server_B. This will allow the user Jorge Campos to use the same login name on both servers. On Server_B, all files and directories belonging to jcampos will need to be copied or moved to the new campos' home directory. The ownership of the files and directories will need to be changed so the user campos will retrieve the environment he had previously on Server_B.

6.5.3 Adding, Editing, Deleting NetWare Users

TME 10 User Administration allows you to manage NetWare user accounts. The information you can add or edit regarding a NetWare user record in a profile includes:

- login
- login time
- password
- home directory
- network address
- group membership
- security
- mail

All that information relates to the NetWare environment.

6.5.3.1 Adding a NetWare User

Adding a NetWare user in the user profile consists of adding a user to the profile as any other type of user. However the information that must be gathered when adding a NetWare user is specific to NetWare. You then must have a sufficient understanding of the NetWare environment and the fields that must be filled out in the user profile.

To add a user, you just need to select **Edit**, then **Add User** in the User Profile Properties dialog. All the attributes related to NetWare can be displayed by selecting **NetWare** from the Category pull-down menu. In the following sections, we describe the different NetWare options that can be filled out for a user.

Common Information

Remember that you can simply enter the user name and click on **Generate Defaults** to have a common user login defined on UNIX, Windows NT and Netware systems. This new user will have the attributes set according to the profile default policies. Simply by editing the default policies, the administrator is allowed to set common conventions for every new user he/she will add to the user profile. It is possible, for example, to establish a consistent naming convention that avoids login name duplications.

In general, when you create a new record to a profile, you can:

- Manually add attribute information

- Use default policies to fill in the attribute information
- Do both

Note: If you just want to create a NetWare user account and not fill out all the default attributes for UNIX or Windows NT, you can disable default policies for UNIX and Windows NT with the `wsetdefpol` command:

```
wsetdefpol DISABLED Unix NW_Users
```

```
wsetdefpol DISABLED NT NW_Users
```

Let us consider the specific case of a NetWare NDS user creation, we assume it will be named Irana Sanches, with login name isanches.

NetWare Login

When selecting the NetWare Login subcategory, you get the following dialog that allows you to enter login information for the user account you want to create.

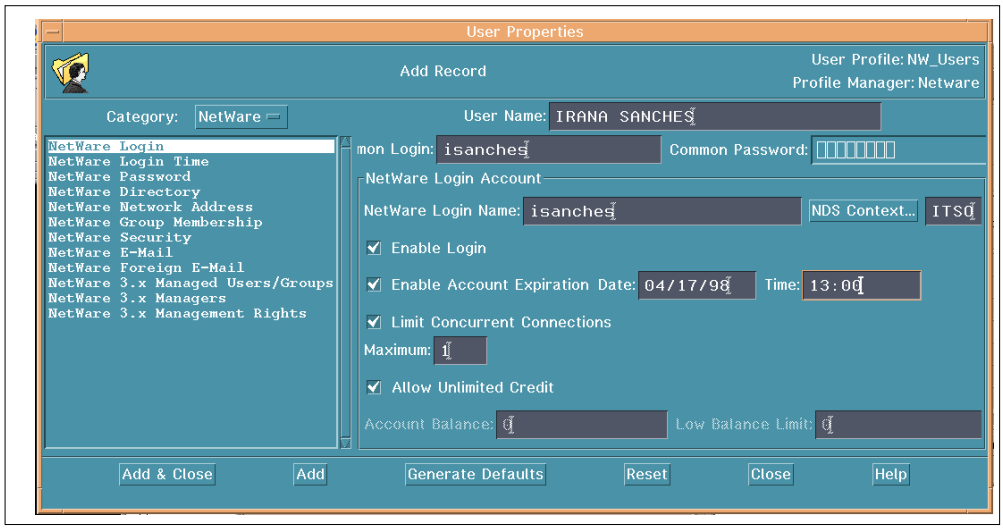


Figure 190. User Properties: NetWare Login

From this panel you can do the following:

1. Enter the NetWare login name for the user in the NetWare Login Name field.

> **Attention!**
>
> Although NetWare supports login names that contain spaces, TME 10 User Administration does not. If in TME 10, you enter a NetWare login name that has a space in it, the user will need to substitute the space with an underscore (_) to successfully log into NDS.

2. For NetWare 4.1 accounts, you must specify the user context in the NDS Context field. The user context is the user container object location in the directory tree. In our case, the context is ITSO.

Attention!

If you do not include an NDS context, the user will not be created when the profile is distributed.

Press the **NDS Context..** button to display the NetWare Directory Services Browser dialog.

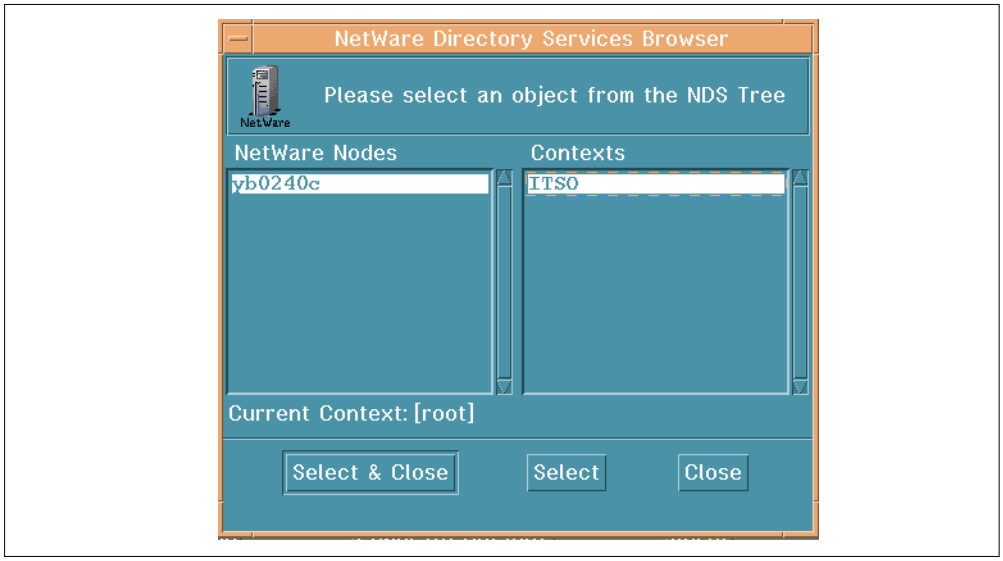


Figure 191. NetWare Directory Services Browser

3. Double-click on a node displayed in the NetWare Nodes scrolling list, yb0240c in our case. The dialog displays the NDS contexts associated with the selected node.
4. Select the context (ITSO in our example) from the Contexts scrolling list. Press the **Select & Close** button to return to the User Properties dialog.
5. Select the **Enable Login** check box to allow this user to log in. When this check box is selected, there is a mark in the check box.
6. Select the **Account Expiration Date** check box to set an expiration date for this user account. When this check box is selected, there is a mark in the check box.
   - Enter the expiration date, in a month/day/year format in the Date field.
   - Enter the expiration time in the Time field. This time must be expressed in a 24-hour format. For example 1300 represents 1:00 PM.
7. Select the **Limit Concurrent Connections** check box to limit the number of concurrent connections for this user. When this check box is selected, there is a checkmark in the check box. Then, enter the number of allowed concurrent connections in the Maximum field. In our case the limit is 1. This option is very useful because it controls the capability of login from more than one PC at a time while using the same login name.
8. Select the **Allow Unlimited Credit** check box if you do not want to track NetWare account balances. When this check box is selected, there is a mark

in the check box. If you want to track the user account balance, enter the amount of credit for that user in the Account Balance field.

Then, enter the user low balance limit in the Low Balance Limit field. Once the user account balance reaches this number, the user can no longer use network resources.

Note

Leaving the Account Balance field blank gives the user an account balance of zero.

NetWare Login Time

NetWare Login Time allows you to control the periods of time the user is allowed to log in to the network with this login name. If the network should not be used during certain hours, you can prevent users from login during those hours. To restrict user login time, do the following:

1. Select **NetWare Login Time** from the subcategory scrolling list to display the following User Properties dialog:

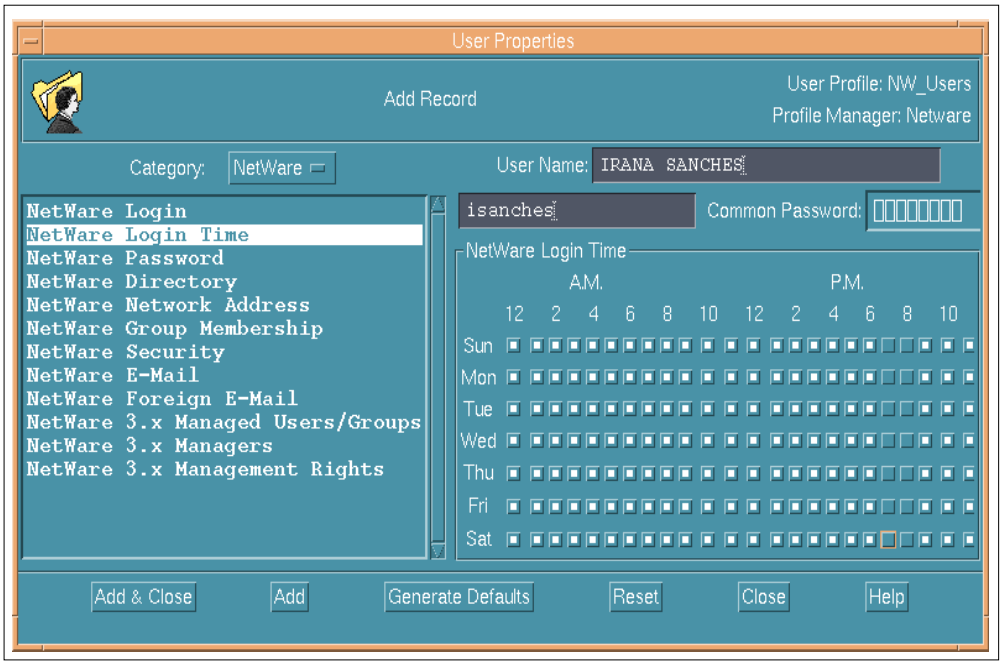


Figure 192. User Properties: NetWare Login Time

2. In our example, we want to prevent the user from accessing the network between 7:00 PM and 8:00 PM and allow her/him to access the network the rest of the time. A selected box has a mark in it. By default all check boxes are selected, this means that the user can log in at any time. So, we just deselected the check boxes corresponding to the period of time between 7:00 PM to 8:00 PM everyday.

NetWare Password

The password information allows you to set the user password and define certain policies concerning that password.

1. Select **NetWare Password** from the user properties list. You will get the following dialog:

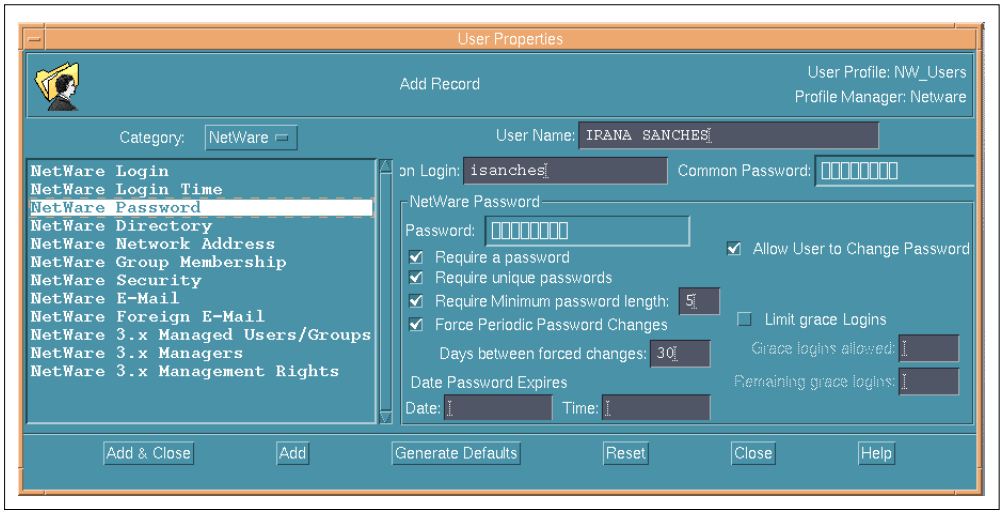


Figure 193. User Properties: NetWare Password

2. Enter the user password in the Password field.
3. Select the **Require a password** check box to ask the user to supply a password upon login. When this check box is selected the user must enter a password every time he tries to log in.
4. Select the **Require unique password** check box to ask the user to use unique passwords.
5. Select the **Require Minimum password length** check box to set the minimum accepted length for passwords. Then enter the minimum length in the text field. In our case the minimum length is 5 characters.
6. Select the **Force Periodic Password Changes** to force the user to change his password periodically. This corresponds to an expiration period. The password will expire after a certain amount of days. When the password is expired, the user will then be prompted to change his password.
   - In our example, we ask the password to be changed every 30 days.
   - Enter the date the current password expires in the Date field. Enter the time at that date the current password expires in the Time field.

     Note: If you leave these fields blank, the password will never expire.
7. Select the **Allow User to Change Password** check box if you want the user to control his own password. This means that the user will be able to change his password with the NetWare `setpass` command. In this case the password will be changed on the NetWare server itself and not in the profile. If you do not select that option, the user will not be able to change his password. The TME 10 administrator will need to change the password in the profile and then distribute the profile.

   Note: We noticed that if you do not allow the user to change his password, selecting the Force Periodic Password Changes check box, has no effects. That attribute is not distributed to the server.

8. Select the **Limit grace Logins** check box to limit the number of grace logins the user is allowed when the password expires. A grace login allows the user to login even if the password has expired. If you do not select this check box, the user is given six grace logins by default. Enter a number in the Grace logins allowed field. The Remaining grace logins field keeps a total of the available grace logins for this user account.

NetWare Directory

The NetWare Directory option allows you to specify a home directory for the user. A home directory is a personal directory that NetWare 4.1 gives the user full access to. Files created by the user will automatically be stored in that directory. If you want to create the home directory when the user is created, NetWare automatically supplies the user object name (or the first eight characters of the user object name if the name is longer than eight characters) in the Home Directory field.

To specify the home directory name, you also must specify the home directory path. The path includes the volume and directory (or directories) beneath which the home directory will be created.

By default NetWare creates a directory called SYS:\USERS, underneath which the personal user directory is created. Placing every home directory beneath a single directory makes it easy to back up these directories as a group and to control the amount of space consumed by disk storage users.

The following steps are necessary to configure the directory information:

1. Select **NetWare Directory** from the subcategory list in the User Properties dialog box to display the following panel:.

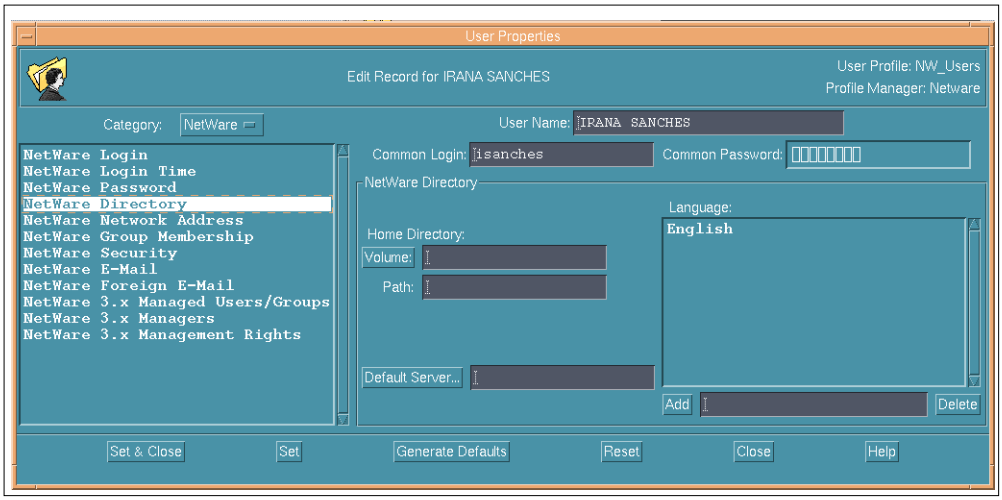


Figure 194. NetWare Directory Dialog

2. If you know the name of the volume where the home directory is created, you can enter the volume name or you can press the **Volume** button to display the **NetWare Directory Services Browser** dialog box.

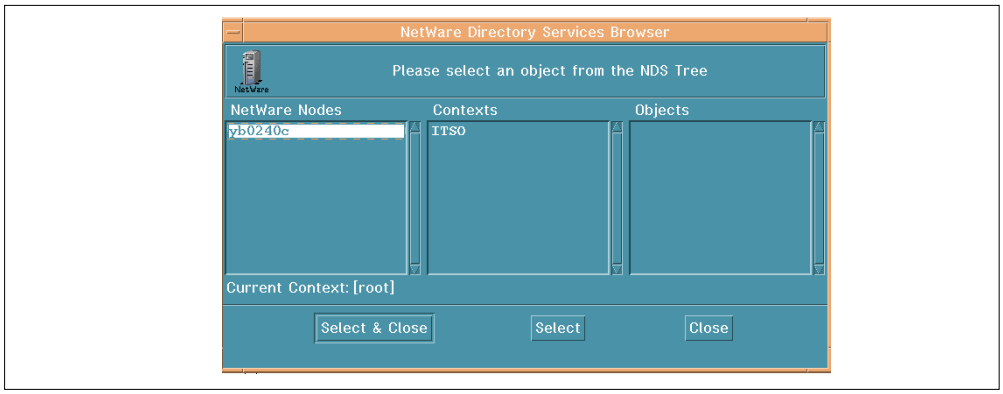


Figure 195. NetWare Directory Services Browser

- Double click on a node displayed in the NetWare Nodes scrolling list. In our case, yb0240c. The dialog box should display the NDS contexts associated with the selected node. In our case, it is ITSO.
- Double click on a context from the Contexts scrolling list. The dialog box displays a list of objects associated with the selected NDS context (ITSO in our case).
- Select an NDS object from the objects scrolling list.
- Click on the **Select & Close** button to return to the User Properties dialog.

3. Enter the path for this user home directory in the **Path** field.

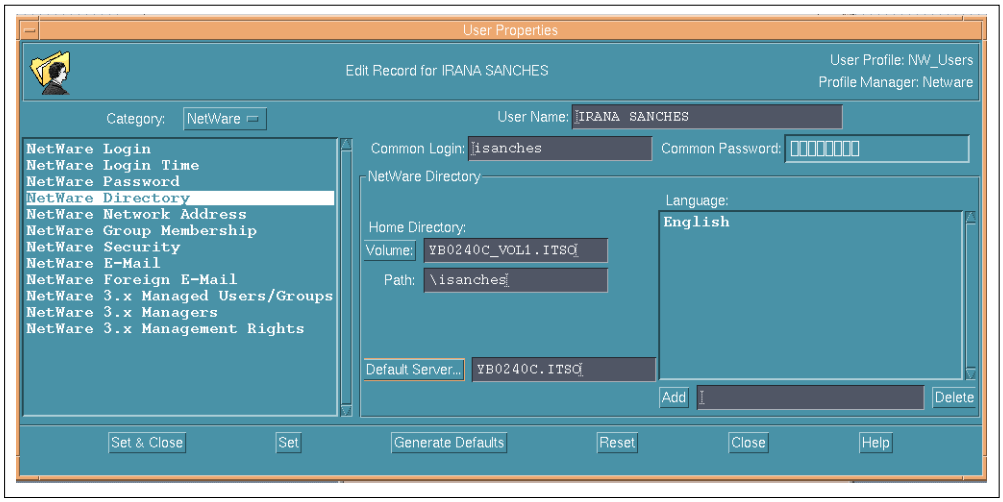


Figure 196. NetWare Directory Dialog

4. Enter the name of the default server. This user will log in to the Default Server field: YB0240C.ITSO in our example. Note that you must enter the complete NDS name for this server.
5. Select the language you want the NetWare messages to appear for this user from the Language scrolling list.

When the profile is distributed the home directory for that user is automatically created on the default server specified above.

NetWare Network Address

It is possible to prevent a user from logging in to the network from a specific workstation. The NetWare Network Address option allows you to define a set of workstations from which the user cannot log in to the network.

1. Select the **NetWare Network Address** subcategory from the User Properties dialog to display the following panel:

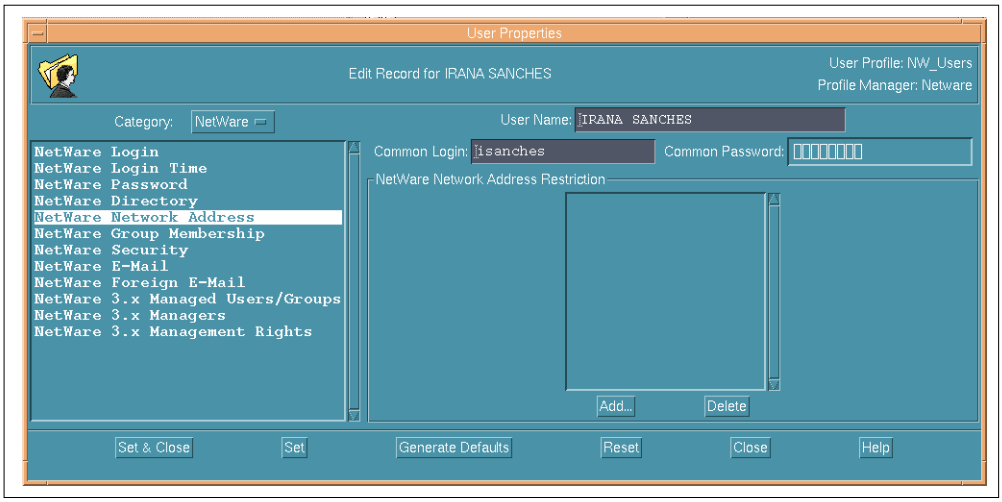


Figure 197. User Properties: NetWare Network Address

2. Click on the **Add** button to display the NetWare Network Address Restrictions dialog shown below:

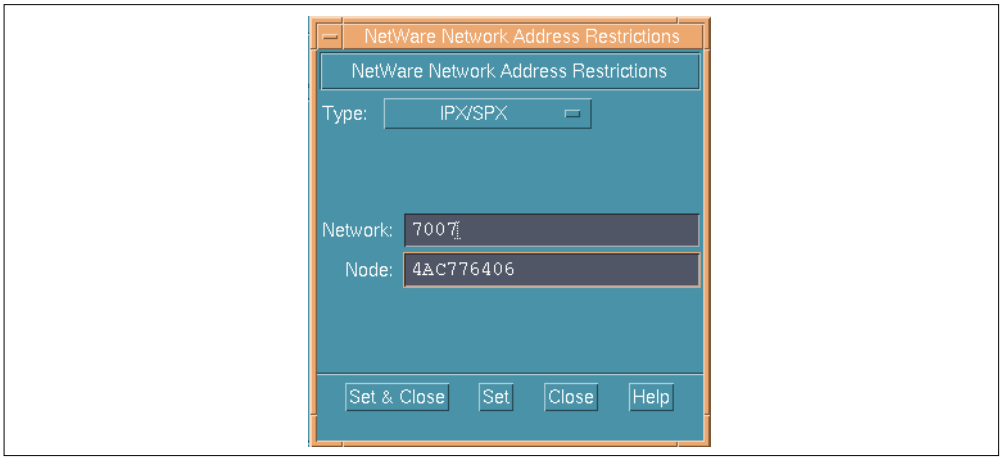


Figure 198. NetWare Network Address Restrictions Dialog

3. Select a network address type from the Type pop-up menu. You can select AppleTalk, Ethernet/TokenRing, IPX/SPX, OSI, SDLC, or TCP/IP address types. Then, enter the network address in the Network field as well as the address of the workstation in the Node field.
4. Click on the **Set & Close** button to set the network address restrictions and return to the User Properties dialog.

NetWare Group Membership

The NetWare Group Membership information option allows you to define a group to which the user belongs. TME 10 User Administration does not allow you to create groups, group profiles are not supported. However, it allows you to assign a user to an existing group.

The following steps are necessary to configure the group membership information:

1. Select the **NetWare Group Membership** subcategory from the User Properties dialog box to display the following panel:

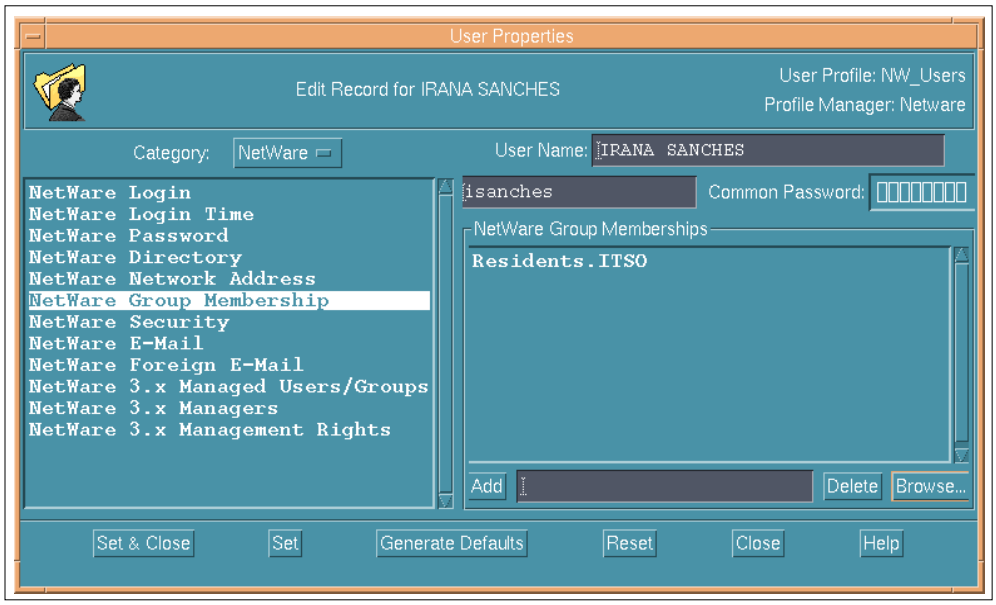


Figure 199. User Properties: NetWare Group Membership

2. Enter the name of the group to which this user belongs and click on the **Add** button. In our case, the group is Residents. The group is added to the scrolling list. You can add several groups if the user belongs to several groups.

NetWare Security

The NetWare Security information option allows you to set the security level for that user at the same level as another specified user. This corresponds to the option Security Equal To in NetWare.

The following steps are necessary to configure the security information:

1. Select the **NetWare Security** subcategory from the User Properties dialog to display the following panel:

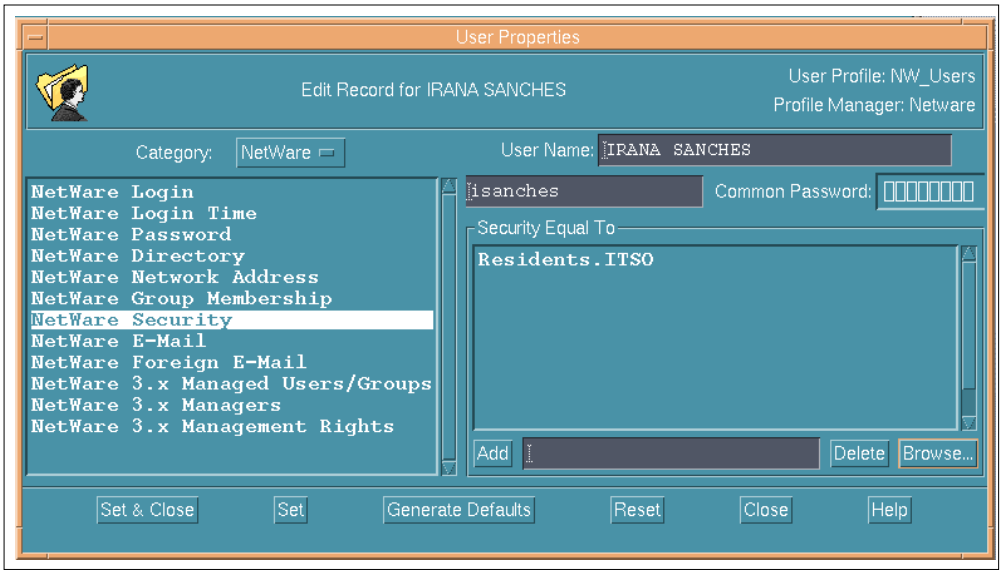


Figure 200. User Properties: NetWare Security

2. Enter the login name of the user with whom you want this user to have equivalent security and click on the **Add** button. Or, click on the **Browse** button to display all the available options.

NetWare E-Mail

The NetWare E-Mail information option allows you to define the user mailbox location and mailbox ID.

The following are the necessary steps to configure the E-Mail information:

1. Select the **NetWare E-Mail** subcategory from the User Properties dialog box to display the following panel:

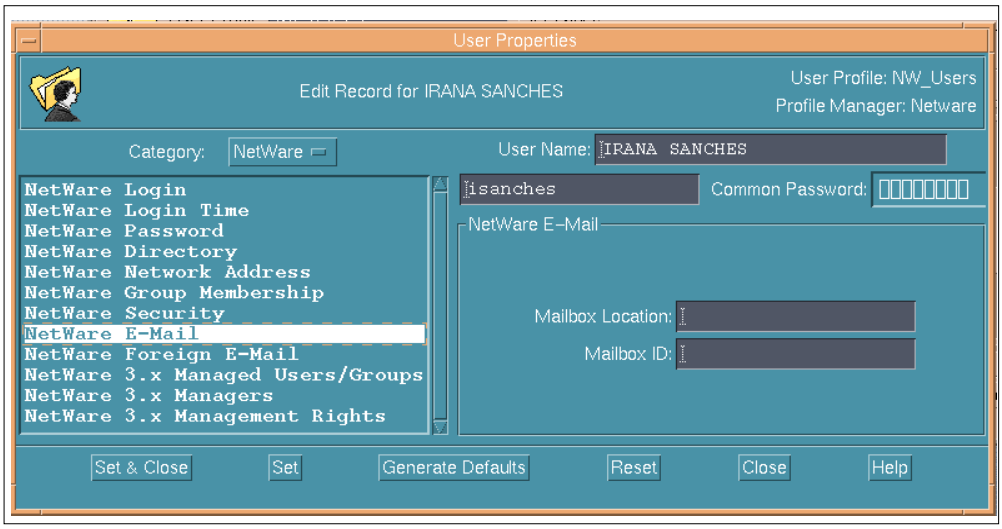


Figure 201. NetWare E-Mail Window

2. Enter in the **Mailbox Location** field the name of the Messaging Server where the user mailbox resides.

3. Enter in the **Mailbox ID** field the user unique mailbox identification. This ID allows the user mailbox to be located in the NetWare Messaging Database.

NetWare Foreign E-Mail

The NetWare Foreign E-Mail option allows you to define external E-Mail addresses for the user.

The following are the necessary steps to configure the E-Mail foreign information:

1. Select the **NetWare Foreign E-Mail** subcategory from the User Properties dialog box to display the following panel:

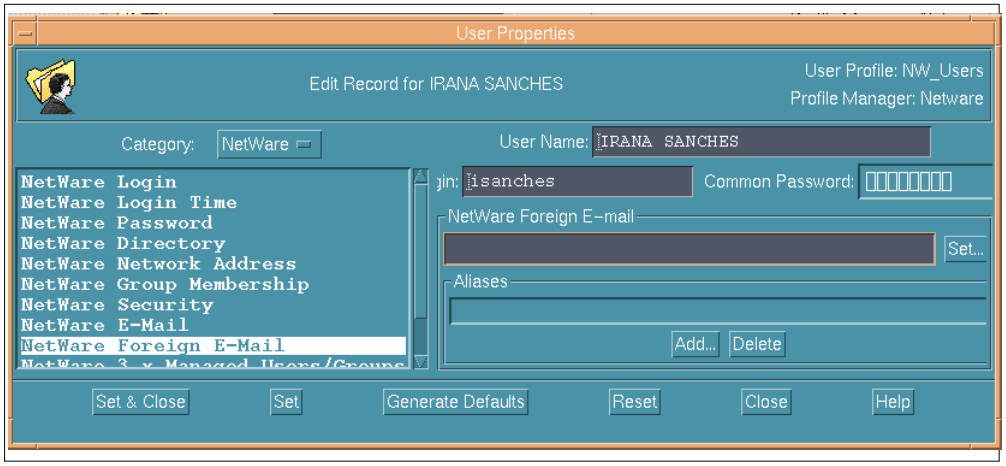


Figure 202. User Properties: NetWare Foreign E-mail

2. To add an address type to the Aliases scrolling list, click on the **Add** button. TME 10 User Administration displays the NetWare Foreign Email dialog box n the following form:

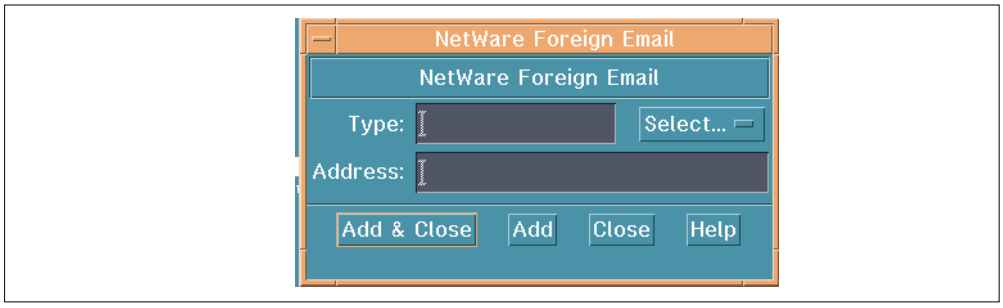


Figure 203. NetWare Foreign Email Dialog

3. Select an option from the **Select** option list. If the option that you want is not in the list, you can enter it in the Type field.
4. Enter an address in the **Address** field.
5. Press the **Add & Close** button to close this dialog and add this address to the Aliases scrolling list.
6. Select an alias from the **Aliases** scrolling list, then press the **Set** button to display the NetWare Foreign Email dialog box. This dialog box allows you to set a Foreign E-mail address.

7. Select an option from the **Select** option list. If the option that you want is not in the list, you can enter it in the **Type** field.
8. Enter an address in the **Address** field.
9. Click on the **Set & Close** button to close this dialog box and add this address to the address field.

Disabling Default Policies for Other Platforms

When we were creating a new NetWare user in a user profile without providing any information for UNIX and Windows NT, we found that the UNIX and Windows NT attributes were automatically filled out in the profile. For example, the home directory specified for NetWare was defined in UNIX and Windows NT with corresponding attributes.

If you do not want to fill out the attributes for other platforms than NetWare, you can disable the default policies for the other platforms by using the `wsetdefpol` command. The command `wsetdefpol` enables or disables the UNIX, NetWare or Windows NT default policies for a specific user profile.

The following command shows how to disable the UNIX and Windows NT default policies for the NW41_Users user profile:

```
wsetdefpol DISABLED Unix NW_Users
wsetdefpol DISABLED NT NW_Users
```

where:

`DISABLED` disables default policies for the specified profile,

`Unix` specifies UNIX default policies,

`NT` speficies Windows NT default policies, and

`NW_Users` specifies the name of the user profile

Notes

The `wsetdefpol` command does not recognize profile names in the format `@UserProfile:<profile_name>`

When default policies for other platforms are disabled, creating a user in a profile is faster since default policies do not need to be checked against all attributes already entered.

6.5.3.2 Deleting User Records

If you no longer need a user account, you can delete it from the profile. When you distribute the profile with the option All levels of subscribers, the record is deleted from all copies of the profile stored at the subscribers level. It is also deleted from the system files. Otherwise, the record is deleted only from the top level profile. Deletion of user records follows the same pattern of subscription and distribution. Use the following steps to delete a user account:

1. Use the User Locator to locate the user you want to delete or if you know in which profile the user is defined, open the corresponding profile.
2. Select the record to be deleted.

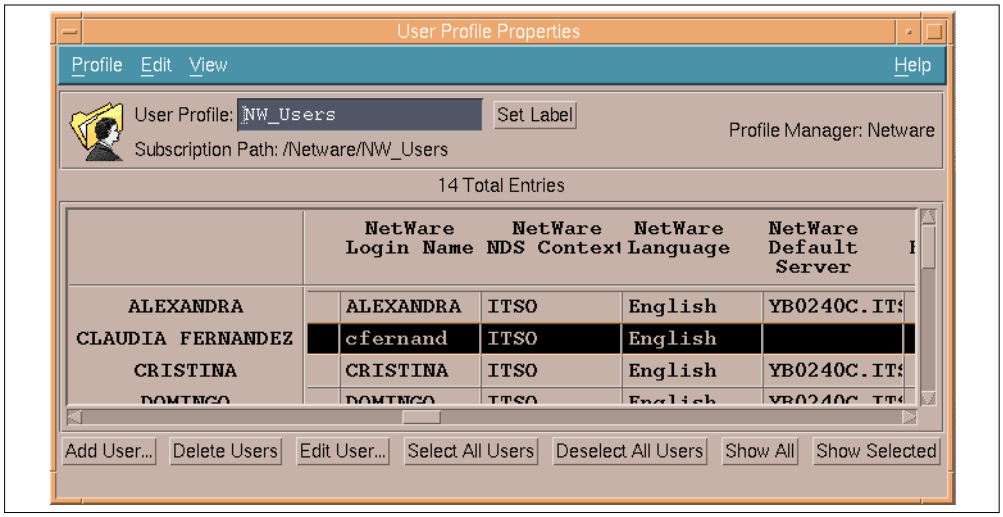


Figure 204. Selecting a User for Deletion

3. Click on the **Delete Users** button to display a warning dialog box.

Figure 205. Warning Window

   At this step, you have two options: Delete Home Directory or Leave Home Directory. Click on the **Delete Home Directory** button if you want to delete the user home directory when the profile is distributed to the endpoint. Click on the **Leave Home Directory** if you want to keep the home directory for that user.

4. Distribute the profile to the PC Managed Node (in our case) in order to delete the user from the system files. We recommend that you distribute the profile to all levels of subscribers and preserve modifications in the subscribers copies of the profile.

   Note that the PC Managed Node itself does not maintain a copy of the profile. The copy is maintained at the TMR server itself. In our example, that copy is called NW_Users@yb0240c.

   If you distribute to the next level of subscribers, the system files will not be modified.

   Be extremely careful with the EXACT COPY distribution option. This option will not preserve any modifications made in the copy of the profile and can delete user accounts that were defined in the system and not in the profile you distribute.

Note on Home Directory

We noticed that even if you choose to delete the user home directory, the home directory is not deleted on the NetWare server when the profile is distributed to all levels.

For more information about distributing user profile, see Section 6.5.4, “Distributing a User Profile” on page 253.

You can also delete user accounts from the command line. The following example deletes a user record:

```
wdelusr -l @UserProfile:NW_Users cfernand
```

where:

`-l` leaves the user home directory as is. The home directory is not deleted when the profile is distributed.

`@UserProfile:NW_Users` is the profile from which to delete the user record.

`cfernand` is the login name of the user record to delete.

Attention!

We noticed that if you use the option `-d` (to ask for deletion of the home directory) with the `wdelusr` command, the user is deleted in the user database but still shows up in the user profile.

For more information on the `wdelusr` command, you can refer to the Appendix D, Commands in the TME 10 User Administration User and Group Management Guide Version 3.1.

6.5.4 Distributing a User Profile

Once a profile has been created and/or records have been added to it, you can distribute copies of the profile to the suscribers. You can also update the system files on the NetWare server. This mechanism is not specific to NetWare. Since a profile can contain UNIX, Windows NT, NetWare as well as RACF user information. Distributing a profile works the same way, no matter what platform you are working on.

For more information on the different distribution options, you can refer to section 6.1.4, “Distributing a Profile” on page 141.

It is also possible to distribute a profile from the command line interface by using the `wdistrib` command. The following example distributes the user profile NW_Users to the PC Managed Node yb0240c:

```
wdistrib -l maintain -m @UserProfile:NW_Users @PcManagedNode:yb0240c
```

where

`-l maintain` retains any local modification in suscribers’ copies of the profile.

`-m` specifies that the profile is distributed to all levels of subscribers, including the actual system files.

For more information about using the command line to distribute user profiles, see the `wdistrib` command in the TME 10 Framework Reference Manual.

6.5.5 Synchronizing a User Profile

If someone modifies the system configuration files directly, the profile will no longer be consistent with the system files. In our case, if someone adds a user account or modifies a user account by using NWADMIN in NetWare, the user profile will no longer be consistent with the system files.

Synchronizing the profile and its associated database with system files shows you which entry in the system files does not match the profile. Then the synchronize function provides a way to reconcile the profile with the system files.

Note

On NetWare, synchronization is only supported by using the command `wchkusrs`. There is no support from the GUI. In other words, the synchronize option does not show up in the PC Managed Node icon pull down menu.

You can synchronize a profile so it accurately reflects the current system configuration of the NetWare NDS server. When you synchronize a profile, a list of differences between the profile and the system files is displayed. There are three types of differences:

- Items that exist in the profile, but not in the system files
- Items that exist in the system files but not in the profile
- Items that differ in the profile and in the system files

As other platforms, there are actually two profiles that you might need to synchronize. The profile at the PC Managed Node level and the top level profile. The trick for a PC Managed Node is that the local copy of the profile is not actually stored on the PC Managed Node itself, but stored on the TMR server. In our example, the copy of the profile for the PC Managed Node is called: NW_Users@yb0240c, while the top level profile is called NW_Users.

Added Records

In the following example, we want to synchronize the user profile NW_Users shown in Figure 206 with the system files. On the system itself, a user allison has been directly added on the NetWare server (yb0240c).

Figure 206 on page 255, shows the content of NW_Users profile.

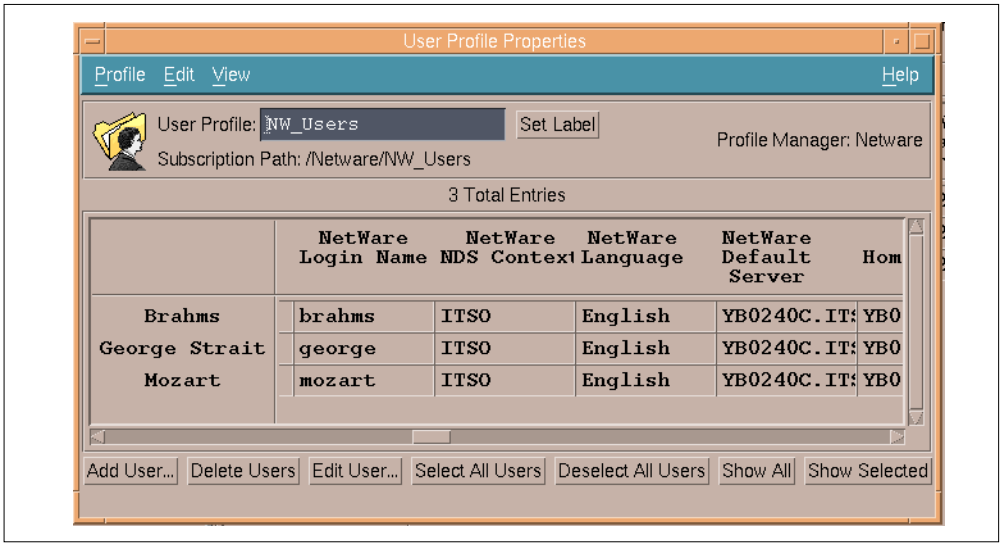


Figure 206. NW_Users User Profile

To look at the content of NW_Users@yb0240c, from the NW_Users User Profile Properties window, you can select **Profile**, **Go To Profile At...** You will then get the following window:

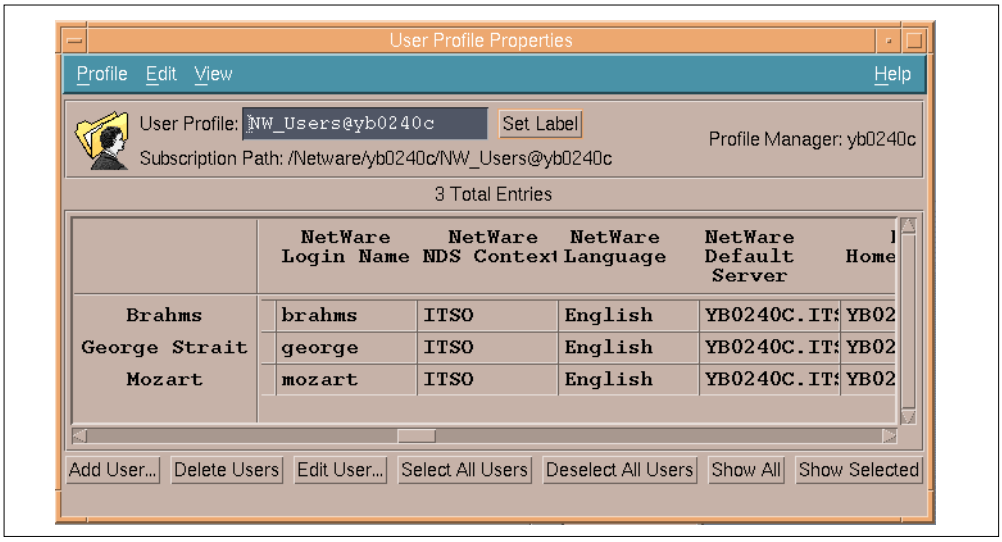


Figure 207. NW_Users@yb0240c User Profile

To check the consistency of NW_Users@yb0240c profile with the system files, you need to run the following command.

```
wchkusrs -s @UserProfile:NW_Users@yb0240c @PcManagedNode:yb0240c
```

where:

`-s @UserProfile:NW_Users@yb0240c` specifies the profile with which you want to check the consistency with the system files

@PcManagedNode is the fully qualified name of the PC Managed Node (NetWare server)

You should get the following output:

```
# wchkusrs -s @UserProfile:NW_Users@yb0240c @PcManagedNode:yb0240c
Checking endpoint @PcManagedNode:yb0240c...
These users were found in the system but not in the database:
    Admin
    allison
These differences have not been updated in the profile.
```

Figure 208. Checking Consistency Between User Profile and System Files

If you want to check the consistency of the profile with the system files and update the profile at the same time, you need to run the following command:

```
wchkusrs -s @UserProfile:NW_Users@yb0240c -u @UserProfile:NW_Users@yb0240c
@PcManagedNode:yb0240c
```

where:

`-s @UserProfile:NW_Users@yb0240c` specifies the profile with which you want to check the consistency with the system files

`-u @UserProfile:NW_Users@yb0240c` specifies the profile you want to update. Users that are discovered in the system files that are not in the source profile, will be added to the source profile.

You should get an output similar to the following:

```
##  wchkusrs -s @UserProfile:NW_Users@yb0240c \
>  -u @UserProfile:NW_Users@yb0240c @PcManagedNode:yb0240c
Checking endpoint @PcManagedNode:yb0240c...
These users were found in the system but not in the database:
    Admin
    allison
The following records in the profile @UserProfile:NW_Users@yb0240c could not be
modified or added:
    Admin
```

Figure 209. Checking Consistency and Updating the User Profile

Note: We noticed that even if the synchronization function has been performed properly, the user allison does not show up in the NW_Users@yb0240c user profile.

You can synchronize the same way the top level profile NW_Users with the system files by entering the following command:

```
wchkusrs -s @UserProfile:NW_Users -u @UserProfile:NW_Users
@PcManagedNode:yb0240c
```

You will get an output similar to the one shown in Figure 209 on page 256. Also, the new user should show up in the NW_Users profile. You might need to refresh

the profile or close it and open it again to see the user allison added to the profile as shown below:

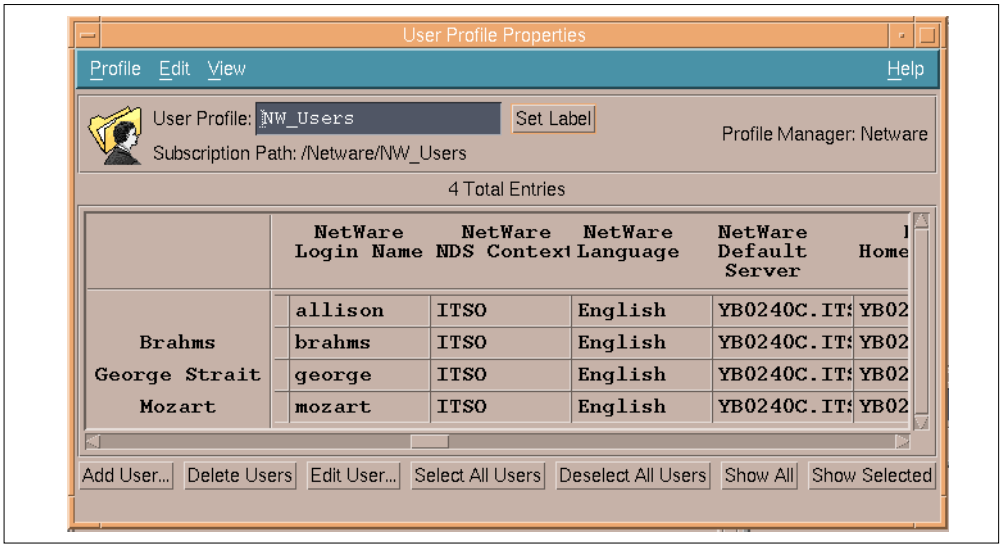


Figure 210. NW_Users Profile After Synchronization

Note: You can notice that the User Name does not show up in the profile. You might want to fill out the User Name and common login information for that user and then distribute the profile to the next level of subscribers so the user allison shoows up in the NW_Users@yb0240c profile.

Changed Records

The `wchkusrs` command can also pick up records that have been modified on the NetWare server itself. For example, we modified the home directory for the user brahms. We created a directory BRAHMS1 under the volume YB0240C_VOL1.ITSO and switched the home directory attribute for user brahms to BRAHMS1.

Then, if you issue the `wchkusrs` command to check the consistency between NW_Users and the system files, you will get the following:

```
# wchkusrs -s @UserProfile:NW_Users @PcManagedNode:yb0240c
Checking endpoint @PcManagedNode:yb0240c...
These users were found in the system but not in the database:
    Admin
These users were found in both the system and the database with different values:

Login          Attribute      System Values            Database Values
brahms         Home Directory Path BRAHMS1                  \brahms
These differences have not been updated in the profile.
```

Figure 211. Checking for Modified Records

You can of course check consistency between the profile and the system files and at the same time update the profile with the `-u` option. Once the profile has been updated, you can check the result by refreshing the profile or closing it and then open it again. You should see the new directory BRAHMS1 for user brahms.

6.6 Managing RACF Users

The typical OS/390 environment is different then other platforms supported by TME 10 User Administration. This is a result of the inherent differences in the security product employed for OS/390, and the scale of administration on a single system.

This section provides some general considerations for implementing TME 10 User Administration in an OS/390-RACF environment. We will examine what effect differences in the OS/390 platform have upon use of the TME 10 User Administration product. We describe some of the basic steps to managing user IDs on the OS/390 platform, briefly discuss default and validation policies, and finally the issuing of RACF commands from the TMR server. This section is based on some early experience with the product.

6.6.1 General Considerations

TME 10 User Administration provides an infrastructure to manage multiple heterogeneous environments using common concepts. This management is achieved by interfacing with the security products and methodologies already existing on the respective platforms. The advantages to this range from protection of existing security infrastructures and investment, to a cleaner installation process with no intrusive software hooks.

The existing products and methodologies were of course not designed in conjunction with each other, and while the broad scope of their functions are similar, there are differences in implementation across platforms. This means that while TME 10 User Administration concepts generally map well across the various platforms, there are differences in some areas. It is important to understand these differences to get the full value from the product.

The inherent nature of each platform will also be a consideration in the implementation of TME 10 User Administration. OS/390 systems have long been known as large scale systems, with large numbers of users, and while the numbers of users in a client/server environment may number in the hundreds and thousands, the numbers of user IDs per system image is generally low. This cannot be said for the OS/390 RACF environment, where it is common to find large numbers of user IDs on a single system image.

6.6.1.1 Differences in Administration

The large numbers of user IDs generally present on an OS/390-RACF systems will dictate how administrators interface with the product. For instance, adding a few user IDs via dialogs is efficient, adding several hundred becomes more difficult. Generally operations are able to be performed through command line interfaces as well as dialogs, so you can choose which interface more effectively meets your particular requirements.

It is likely the large numbers of user IDs will force administration of bulk user IDs to be done through command interfaces, rather than using dialogs. In this instance some investment in scripts can make more efficient use of the command level environment for a given enterprise.

6.6.1.2 Definition of User Profiles and Profile Manager Hierarchies

One of the strengths of the OS/390 Security Server is in the ability to decentralize security administration functions while still having some relationship between various administration groups. For instance you can have central definition of user IDs, but have the access requirements of those user IDs managed by decentralized groups. This is a difference from the client server environment where decentralization would generally indicate different groups managing different systems.

Chapter 4, “What Is TME 10 User Administration?” on page 65 introduced the concept of Profile Managers and User Profiles. TME 10 User Administration’s ability to have profile managers as subscribers to user profiles allows a hierarchy to be established that can allow any combination of centralized and decentralized security administration functions. You should consider carefully what options are available and what hierarchy best meets the needs of your organization. The infrastructure that TME 10 provides is very flexible and should be thoroughly understood before determining what structures should be implemented.

For performance reasons it is recommended that the number of user ID records in a user profile should not exceed 500. Since it is not uncommon for RACF groups to have in excess of 500 users you may not be able to directly map RACF user groups to TME 10 User Profiles. The *TME 10 User Administration User and Group Management Guide* documents this limitation and suggests various scenarios for managing large numbers of users.

Note: This recommendation is purely for performance reasons, if you have a TMR server with ample resources you may consider defining more user IDs in a group. There have been instances where up to 1000 users were able to be created within a single user profile.

6.6.1.3 Relationship to Overall OS/390 Security Management

It is important to position TME 10 User Administration, and the functions it provides within overall management of the OS/390 security environment. TME 10 User Administration is not designed to manage all aspects of security management, as the product name implies the primary objective is the management of user IDs by using user profiles.

Within the area of user administration there are a couple of important details that should be understood before implementing the product, this may mean that there is still some security administration that would be required on individual OS/390-RACF platform:

- TSO user administration - you are unable to administer catalog aliases and manipulate TSO user datasets from the TME desktop environment. Dataset profiles, while not able to be defined directly through the product, are able to be defined through the RACF command interface described later.
- RACF group administration - the TME 10 User Administration product does not cater for the connection of RACF user IDs to multiple groups. Support for this function is provided within the TME 10 Security Management product.

6.6.1.4 TP Server User ID and Administration User IDs

Both the TP Server user ID and user ID associated with TME 10 Administrators are going to be managed by TME 10 User Administration. It is important you do not inadvertently remove authority from these user IDs. If you do remove any

authorities required by the TME 10 administration user IDs then you will be unable to correct the problem using TME 10 User Administration. You would have to use another user ID with appropriate RACF authorities on the system itself.

6.6.1.5 Supported Segments

The current release of TME 10 User Administration contains support for a subset of commonly used segments, these are:

- CICS
- Netview
- OMVS (MVS OpenEdition)
- TSO

The base user segment is fully supported. The next code shipment of TME 10 GEM User Administration for OS/390 Users should provide full support for all user segments.

6.6.1.6 Common Login

When an administrator in RACF sets a password for a user ID, the password is said to be an *expired* password. This means that the first time the password is used, it must be changed. This is applicable if the password is for a new user ID, or a password change for an existing user ID.

At the time of writing RACF does not support the creation of a non-expiring password by an administrator.

As a result of this, RACF does not support the Common Login function of TME 10 User Administration. This function sets the passwords for all the user IDs of a given user to the same value. The password set in this manner is a non-expired password.

6.6.1.7 Supported Operations

The basic operations provided by TME 10 User Administration are population, creation and modification of user records, distribution of user records to appropriate endpoints, and synchronization of endpoint configurations with TME databases. OS/390-RACF implementation supports all these operations with the exception of the synchronize function. This section deals with these operations.

To better understand this section, Figure 212 on page 262 details the TME configuration that was used during the residency that created this book. Commands and examples given will be from this configuration.

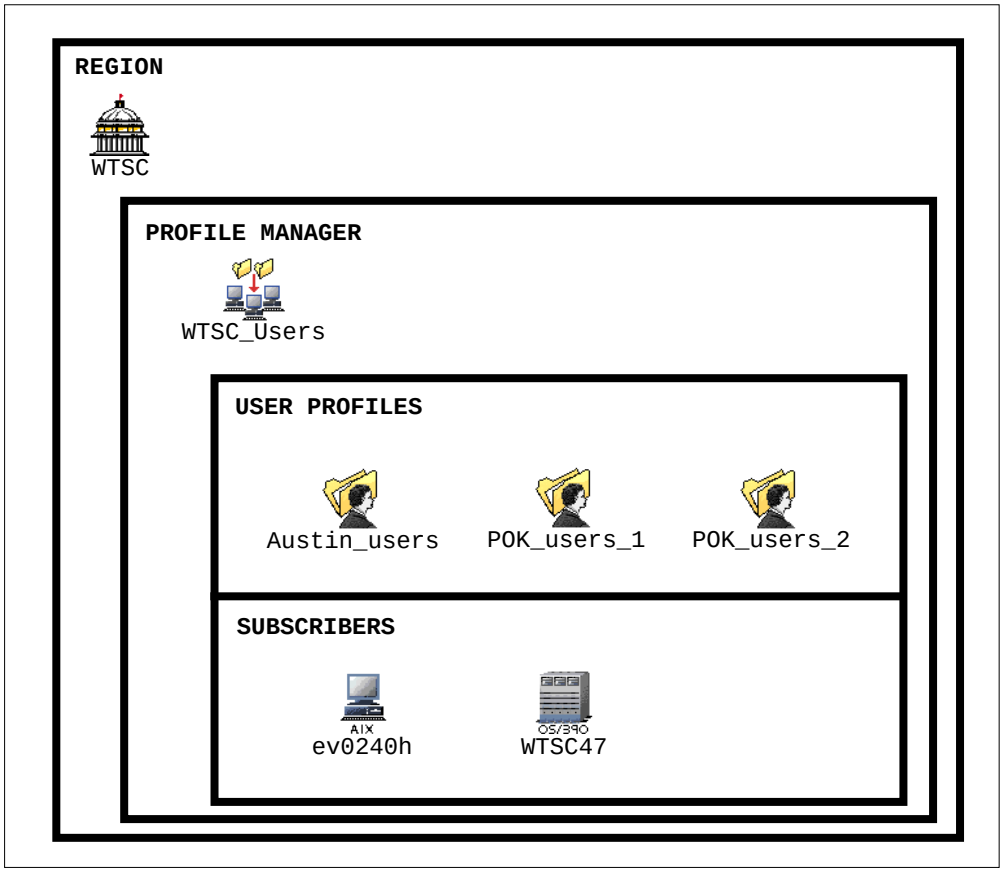


Figure 212. TME 10 Configuration Used During Residency

6.6.2 Populating a User Profile

As discussed before, population is the TME 10 User Administration function to load a user configuration to a TME 10 user profile. To populate in the OS/390-RACF environment TME 10 User Administration requires a list of user IDs to be populated. This list is provided in the form of a flat file, and since the dialogs do not provide for a field for the user ID file, the command line interface must be used to initiate the operation.

There are a number of options for the generation of the user ID file, the *TME 10 GEM User Administration for OS/390 Users' Guide* suggests the approach of manipulating an unloaded copy of the RACF database with a sort product to generate the appropriate user ID files. For large numbers of user IDs, this is an appropriate and efficient way to create the files, for smaller number of user IDs the files might equally be created manually. The user ID file only contains the user IDs to be populated, TME 10 contacts the endpoint (RACF system itself) to extract the data that is imported into the user profile.

The system considered in our scenario contain approximately 500 users, and while we could have placed these users into one user profile, we have created three to provide some guidance on populating to more than one user profile. In our instance we have decided to populate by location, on the systems we are examining this is reasonable. The users are essentially in two locations

Poughkeepsie, New York and Austin, Texas. Further we are going to split the Poughkeepsie users into two different user profiles.

Since we only have a few users in Austin we will not load directly to the Austin_users profile, rather we will load to POK_users_1 and POK_users_2, and then move the required users to the Austin_users profile. This illustrates another technique in populating profiles, you can assemble users into approximate groupings, populate the users, and then fine tune the user IDs into the final user profile configuration.

We used the following JCL to unload the RACF database:

```
//RACFUNLD JOB (999,POK),'Unload Database',NOTIFY=DAVE,
//       MSGCLASS=T,MSGLEVEL=(1,1)
//*
//IRRDBU00 EXEC PGM=IRRDBU00,PARM='NOLOCK'
//SYSPRINT DD   SYSOUT=*
//INDD1    DD   DISP=OLD,DSN=SYS1.RACFESA
//OUTDD    DD   DISP=OLD,DSN=DAVE.IRRDBU00.FLATFILE
```

The following JCL was used to sort users into two different files:

```
//TMESORT  JOB (999,POK),'Sort Users',NOTIFY=DAVE,
//       MSGCLASS=T,MSGLEVEL=(1,1)
//*
//SORT     EXEC PGM=SORT
//SYSOUT   DD   SYSOUT=*
//SYSPRINT DD   SYSOUT=*
//SORTIN   DD   DISP=SHR,DSN=DAVE.IRRDBU00.FLATFILE
//POK1OUT  DD   DISP=(NEW,CATLG,DELETE),DSN=DAVE.POKUSER1.SORTOUT,
//       SPACE=(TRK,(5,3)),LIKE=DAVE.IRRDBU00.FLATFILE
//POK2OUT  DD   DISP=(NEW,CATLG,DELETE),DSN=DAVE.POKUSER2.SORTOUT,
//       SPACE=(TRK,(5,3)),LIKE=DAVE.IRRDBU00.FLATFILE
//SYSIN    DD   *
 SORT FIELD=(10,8,CH,A)
 OUTFIL INCLUDE=(5,4,CH,EQ,C'0200',AND,10,1,CH,LT,C'P'),
 OUTREC=(1,4,10,8),FNAMES=POK1OUT
 OUTFIL INCLUDE=(5,4,CH,EQ,C'0200',AND,10,1,CH,GE,C'P'),
 OUTREC=(1,4,10,8),FNAMES=POK2OUT
 OPTION VLSHRT
/*
```

This job splits all users into the POK1OUT and POK2OUT ddnames. Separation is based on the user ID, with those whose first character is below P going into POK1OUT, and others going into POK2OUT.

These two files were transferred to the ev0240h system as pokusers1.load and pokusers2.load, using TCP/IP FTP.

Once on the ev0240h system, the following commands were used to populate from these two files:

```
wpopusrs -f pokusers1.load -o -l @UserProfile:POK_users_1
wpopusrs -f pokusers2.load -o -l @UserProfile:POK_users_2
```

These commands effectively loaded all pokusers1.load users to the POK_users_1 user profile, and pokusers2.load to POK_users_2 user profile.

There is a further difference in the populate function. The user IDs are loaded to user records where the name equates to the RACF user ID. This is different from the UNIX environment where the name is derived from the GECOS field.

This may present difficulties where user IDs are populated from different platforms, leading to a need for manual intervention to merge records correctly.

6.6.3 Adding, Editing and Deleting User Records

The creation and manipulation of user ID records within user profiles is the same as for other platforms supported by TME 10 User Administration. To continue with our example, we needed to move two users, dave and hilding from the POK_users_1 user profile to the Austin_users profiles. The move operation was performed from the *User Profile Properties* panel shown in Figure 213.

To display this dialog:
-> Policy Region (double-click)
-> Profile Manager (double-click)
-> User Profile (double-click)
-> Select user (single-click)
-> Select Move from Edit menu

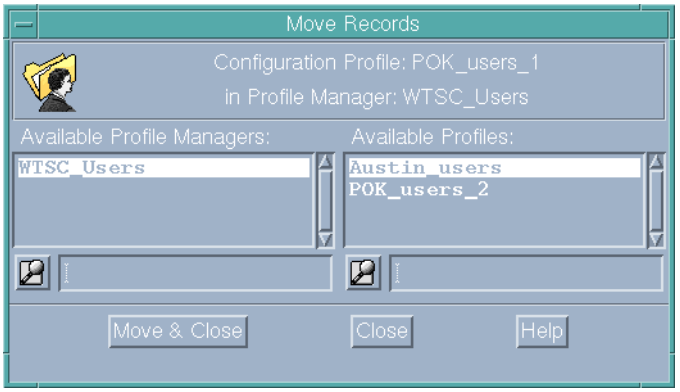


Figure 213. Moving a User

Alternatively, we could have issued the following commands to move the users to their new location:

```
wmvusr @UserProfile:POK_users_1 @UserProfile:Austin_users dave hilding
```

Attention!

Moving a user or copying a user from one profile to another does not work properly if you are running your TME 10 framework on AIX. When trying to move a user, you get a message saying:

```
Table '' has not been created yet. You need to call ttable_init() first
```

Copying by command also gives the following message:

```
The addition of users to profile $UserProfile:Austin_users has failed:
    1152645027.1.616_0
     --> No login name was specified in the attempt to add an user to
profile "Austin_users"
```

This should be fixed with the TME 10 Framework 3.2.

Adding a user is similar to adding a user on other platforms, so this will not be discussed here. There is one difference in the area of default policies, in that there are no default policies provided for the OS/390-RACF environment. This will be discussed later.

6.6.4 Distributing a User Profile

Distribution is the TME 10 mechanism where changes in user profiles are propagated to other Profile Managers and endpoint subscribers.

EXACT COPY

There are a number of options available when performing distribution, with the *EXACT COPY* option not being fully supported for the OS/390-RACF platform. As for other platforms, *EXACT COPY* ensures that the contents of the profile distributed overwrite any definitions made on the endpoint. This means any changes made on the endpoint, for instance a user password change, will be lost. *EXACT COPY* also generally means that any users not in the distributed profile would be deleted from the endpoint. This deletion of user IDs is an extremely powerful operation, and dangerous in the context of the OS/390 platform. As a consequence the deletion of user IDs with *EXACT COPY* does not occur with OS/390-RACF. The copy of distributed records still occurs, but there is no deletion component.

Passwords

Support for the distribution of passwords differs between the OS/390-RACF environment and the other platforms. With the other platforms you are able, through the dialogs, to change passwords both for new user IDs being added, as well as for existing user IDs. OS/390-RACF passwords are only distributed with the creation of a new user ID. You cannot change the password of an existing OS/390 user ID by updating the user record through the dialogs, and then distributing to the endpoint. This does not mean you have to manage RACF passwords from the endpoints themselves, rather you can use the RACF command facility in TME 10 to change passwords.

Other Remarks

Many of the attributes in a RACF user ID profile are elements of other classes in RACF. Since TME 10 does not keep a fully copy of the RACF database within the TME server, it is not able to fully validate the values you might enter. For example,

a user must have a default group specified, since TME 10 does not maintain the group structure in its databases, it cannot validate if you have entered an appropriate group name. Similar issues may arise with the security levels and labels, categories, and class authorities you might assign to a user ID.

In a similar fashion TME 10 is not able to anticipate any function you might have implemented via RACF exits. For example, you might have password content being validated in the password change exit. TME 10 has no way of determining what criteria you have in the exit for password quality, and hence cannot fully validate that you have entered a password that will be acceptable.

In both these instances you have the possibility of entering invalid data, and TME 10 has no way of detecting the problem. There are syntactical checks performed to validate length and character set content. These types of problems will only surface when user profiles are distributed to endpoints. It is vital that you set appropriate data and validation policies to determine appropriate content of the user ID profile you are either creating or modifying, this can greatly minimize the likelihood of these problems occurring.

If content errors do occur these will be reported as distribution errors in the *Notices* icon of the TME desktop, Figure 214 shows a typical message issued when a content problem is detected at the host.

```
Notice-id: 45
Date: Mon May 05 16:48:51 1997
Priority: Error
Administrator: dave@ev0240h.itsc.austin.ibm.com

Endpoint '9.12.14.204' RACF: 'Update to OS/390 for User AFUNG failed
Diagnostic information for the RACF TSO  Segment :
        SAF  Return Code: 8 RACF Return Code: 10 RACF Reason Code: 8

IKJ56702I INVALID USERDATA, 0
IKJ56701I MISSING USER DATA+
IKJ56701I MISSING DEFAULT USERDATA FOR TSO
```

Figure 214. Error Messages from Distributing Incorrect User Definitions

In this example we attempted to propagate incorrect USERDATA from the TSO segment to the OS/390-RACF system. RACF requires four characters for this field, however we only supplied one.

The midpoint system (TCP/IP address 9.12.14.204) is identified, as well as the user record in error.

Distribution of user records on the OS/390-RACF platform is achieved through the R_Admin callable service, also known as the RACF administration API. The SAF and RACF return codes in the figure above are from this service and are documented in the *OS/390 Security Server (RACF) Callable Services* manual.

The R_Admin callable service in some instances may provide textual messages as well as the SAF and RACF return code data, from above these are the IKJ56702I and IKJ56701I messages.

6.6.5 Synchronizing a User Profile

We discussed before that synchronization is not supported for the OS/390-RACF environment. It is relatively simple for a script to be written that would compare the output of a RACF database unload to the contents of a user profile. Commands could then be issued to synchronize the TME user profile contents with the RACF database.

6.6.6 Default and Validation Policies

One of the strengths of TME 10 User Administration is the ability to provide default and validation policies for managed resources. In our instance we are discussing default and validation policies in the context of UserProfile managed resources.

Default policies provide defaults for the creation of users, this can reduce the amount of information entered when creating a new user ID.

Validation policies can be used to ensure user IDs have been defined correctly. We discussed before how TME 10 User Administration is unable to detect some instances of invalid data when entering RACF user ID fields. Good validation policies, reflecting the content of exit code you have implemented, and other local implementation standards, can greatly reduce, if not eliminate, the entering of bad data.

Both types of policies are propagated during a distribution operation. You can lock policies to ensure they cannot be manipulated at lower levels in a subscription hierarchy. This gives you the ability to define policies at a high level, and have them enforced at lower levels in a decentralized security environment, once you have locked the policies, those administrators at lower levels will not be able to modify them.

With most of the environments that TME 10 User Administration supports there are default policies for User Profiles provided as standard with the product. This is not the case with the OS/390-RACF environment, where you must define your own policies.

Given TME 10 User Administration for OS/390 Users does not provide yet default policies, these need to be developed. For our environment, the following commands were used to define default policies in the POK_users_1 user profile:

```
wputpolm -d -F -c ACCNT# @UserProfile:POK_users_1 racf_tso_tacct
wputpolm -d -F -c IKJACCNT @UserProfile:POK_users_1 racf_tso_tlproc
wputpolm -d -F -c 6144 @UserProfile:POK_users_1 racf_tso_tlsize
wputpolm -d -F -c 0 @UserProfile:POK_users_1 racf_tso_tmsize
wputpolm -d -F -c SYSDA @UserProfile:POK_users_1 racf_tso_tunit
```

These defaults might be entered via the panel interface, but we chose to use the command interface since these definitions had to be made for three user profiles. It would be more efficient to add these commands to an executable script file with appropriate arguments to represent the specific user profile. In this fashion it is simple to define consistent defaults between different user profiles.

6.6.7 Issuing RACF Commands

TME 10 User Administration allows RACF commands to be issued from the TME 10 Desktop environment. As for the administration function of distribution, these

commands are processed using the R_admin callable service. Figure 215 illustrates how commands can be issued. The return codes in this figure are the return codes from the R_Admin callable service, and are documented in the *OS/390 Security Server (RACF) Callable Services* manual.

To display this dialog:
-> Policy Region (double-click)
-> OS/390 Connection (right button hold)
-> Select Run RACF Command

or

-> Policy Region (double-click)
-> Profile Manager (double-click)
-> OS/390 Connection (right button hold)
-> Select Run RACF Command

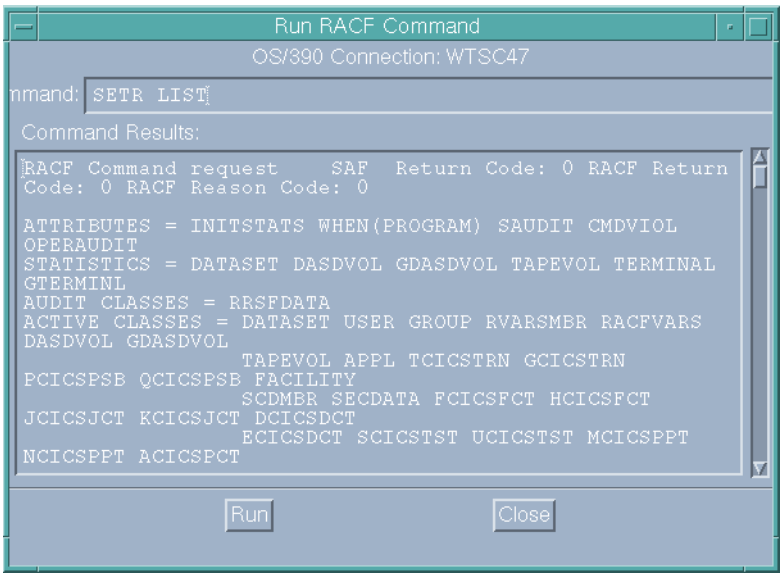


Figure 215. Issuing RACF Commands from the TME 10 Desktop

The same RACF command could have been issued from the command line interface using the following TME 10 User Administration command:

```
wracfruncmd @OS390Connection:WTSC47 "SETR LIST"
```

The full range of RACF commands is supported through this interface with the exception of the following commands:

- BLKUPD
- RVARY
- RACLINK
- DISPLAY
- RESTART
- SET
- SIGNOFF
- STOP
- TARGET

It is unlikely any of the above commands are a serious impediment to managing your security environment from TME 10 since these are not commands that would generally be used to administer resources or users.

There is an additional restriction in that the AT and ONLYAT parameters normally used for directed commands cannot be used through this interface.

This interface provides additional flexibility to managing your OS/390-RACF environment, particularly for those areas not directly addressed by TME 10 User Administration. You also have the flexibility to issue commands on a range of different systems without having to log onto each system. This would be a good interface to use to reset passwords across multiple systems.

Appendix A. Special Notices

This publication is intended to help consultants and systems engineers in understanding, installing and using TME 10 User Administration. The information in this publication is not intended as the specification of any programming interfaces that are provided by TME 10 User Administration. See the PUBLICATIONS section of the IBM Programming Announcement for TME 10 User Administration 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, 500 Columbus Avenue, Thornwood, NY 10594 USA.

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 information about non-IBM ("vendor") products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. 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.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

ADSTAR®
AIX®
AT®
CICS®
IBM®
NetView®
OS/2®
OS/390
Powered by S/390
RACF
RS/600

The following terms are trademarks of other companies:

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Microsoft, Windows, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

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 International Technical Support Organization Publications

For information on ordering these ITSO publications see “How To Get ITSO Redbooks” on page 275.

- *Understanding Tivoli's TME 3.0 and TME 10*, SG24-4948
- *TME 10 Cookbook for AIX*, SG24-4867

B.2 Redbooks on CD-ROMs

Redbooks are also available on CD-ROMs. **Order a subscription** and receive updates 2-4 times a year at significant savings.

CD-ROM Title	Subscription Number	Collection Kit Number
System/390 Redbooks Collection	SBOF-7201	SK2T-2177
Networking and Systems Management Redbooks Collection	SBOF-7370	SK2T-6022
Transaction Processing and Data Management Redbook	SBOF-7240	SK2T-8038
AS/400 Redbooks Collection	SBOF-7270	SK2T-2849
RISC System/6000 Redbooks Collection (HTML, BkMgr)	SBOF-7230	SK2T-8040
RISC System/6000 Redbooks Collection (PostScript)	SBOF-7205	SK2T-8041
Application Development Redbooks Collection (available soon)	SBOF-7290	SK2T-8037
Personal Systems Redbooks Collection (available soon)	SBOF-7250	SK2T-8042

B.3 Other Publications

These publications are also relevant as further information sources:

- *Tivoli/Management Platform Documentation Kit, SK2T-6058*
- *Tivoli/Administration Documentation Kit*, SK2T-6055
- Tivoli/AEF User's Guide, GC31-8345
- *Essential System Administration*, AEleen Frisch, O’Reilly & Associates, Inc., ISBN 1-56592-127-5
- *Managing NFS and NIS,* Hal Stern, O’Reilly & Associates, Inc., ISBN 0-937175-75-*7*
- *Using NetWare 4.1*, Bill Lawrence,QUE, ISBN 1-56529-894-2
- *NetWare Unleashed, Rick Sant’Angelo,* SAMS Publishing, ISBN 0-672-30712-X
- *Mastering Windows NT Server 4*. Mark Minasi, Network Press, ISBN 0-7821-1920-4
- *OS/390 Security Server (RACF) Security Administrator’s Guide,* SC28-1915-02

How To Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, CD-ROMs, workshops, and residencies. A form for ordering books and CD-ROMs is also provided.

This information was current at the time of publication, but is continually subject to change. The latest information may be found at URL `http://www.redbooks.ibm.com`.

How IBM Employees Can Get ITSO Redbooks

Employees may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **PUBORDER** – to order hardcopies in United States
- **GOPHER link to the Internet** – type `GOPHER.WTSCPOK.ITSO.IBM.COM`
- **Tools disks**

  To get LIST3820s of redbooks, type one of the following commands:

  ```
  TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET SG24xxxx PACKAGE
  TOOLS SENDTO CANVM2 TOOLS REDPRINT GET SG24xxxx PACKAGE (Canadian users only)
  ```

  To get lists of redbooks:

  ```
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET LISTSERV PACKAGE
  ```

  To register for information on workshops, residencies, and redbooks:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1996
  ```

  For a list of product area specialists in the ITSO:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ORGCARD PACKAGE
  ```

- **Redbooks Home Page on the World Wide Web**

  `http://w3.itso.ibm.com/redbooks`

- **IBM Direct Publications Catalog on the World Wide Web**

  `http://www.elink.ibmlink.ibm.com/pbl/pbl`

  IBM employees may obtain LIST3820s of redbooks from this page.

- **REDBOOKS category on INEWS**
- **Online** – send orders to: USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL
- **Internet Listserver**

  With an Internet E-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an E-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank). A category form and detailed instructions will be sent to you.

How Customers Can Get ITSO Redbooks

Customers may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **Online Orders** (Do not send credit card information over the Internet) – send orders to:

	IBMMAIL	**Internet**
In United States	usib6fpl at ibmmail	usib6fpl@ibmmail.com
In Canada	caibmbkz at ibmmail	lmannix@vnet.ibm.com
Outside North America	dkibmbsh at ibmmail	bookshop@dk.ibm.com

- **Telephone orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside Notrh America	(long distance charges apply)
(+45) 4810-1320 - Danish	(+45) 4810-1020 - German
(+45) 4810-1420 - Dutch	(+45) 4810-1620 - Italian
(+45) 4810-1540 - English	(+45) 4810-1270 - Norwegian
(+45) 4810-1670 - Finnish	(+45) 4810-1120 - Spanish
(+45) 4810-1220 - French	(+45) 4810-1170 - Swedish

- **Mail Orders** – send orders to:

IBM Publications Publications Customer Support P.O. Box 29570 Raleigh, NC 27626-0570 USA	IBM Publications 144-4th Avenue, S.W. Calgary, Alberta T2P 3N5 Canada	IBM Direct Services Sortemosevej 21 DK-3450 Allerød Denmark

- **Fax** – send orders to:

United States (toll free)	1-800-445-9269
Canada	1-800-267-4455
Outside Notrh America	(+45) 48 14 2207 (long distance charge)

- **1-800-IBM-4FAX (United States)** or **(+1) 408 256 5422 (Outside USA)** – ask for:

  Index # 4421 Abstracts of new redbooks
  Index # 4422 IBM redbooks
  Index # 4420 Redbooks for last six months

- **Direct Services** – send note to `softwareshop@vnet.ibm.com`

- **On the World Wide Web**

Redbooks Home Page	http://www.redbooks.ibm.com
IBM Direct Publications Catalog	http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Internet Listserver**

  With an Internet E-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an E-mail note to `announce@webster.ibmlink.ibm.com` with the keyword `subscribe` in the body of the note (leave the subject line blank).

IBM Redbook 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.

DO NOT SEND CREDIT CARD INFORMATION OVER THE INTERNET.

List of Abbreviations

ACE	Access Control Entries
ACL	Access Control List
ADSTAR	ADSTAR Distributed Storage Manager
APA	All Points Addressable
ARP	Access Resolution Protocol
BCD	Backup Domain Controller
CICS	Customer Information Control System
CORBA	Common Object Request Broker
CSNW	Client Services for NetWare
DAC	Discretionary Access Controls
DCE	Distributed File System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EGID	Effective Group ID
GEM	Global Enterprise Manager
GID	Group ID
GSNW	Gateway Services for NetWare
GUI	Graphical User Interface
IBM	International Business Machines Corporation
IPX/SPX	Internet Packet eXchange/Sequenced Packet eXchange
ITSO	International Technical Support Organization
JCL	Job Control Language
LSA	Local Security Authority
LUID	Login User ID
MVS	Multiple Virtual Storage
NDS	Novell Directory Services
NFS	Network File System
NIS	Network Information Service
NLM	NetWare Loadable Module
NWMS	NetWare Managed Site
OMG	Object Management Group
PDC	Primary Domain Controller
PROFS	Professional Office System
RACF	Resource Access Control Facility
RDBMS	Relational Database Management System
RGID	Real Group ID
RID	Real User ID
SAF	System Authorization Facility
SAM	Security Account Manager
SDSF	Spool Display and Search Facility
SID	Security ID
SRM	Security Reference Monitor
TCP/IP	Transport Control Protocol/Internet Protocol
TME	Tivoli Management Environment
TME 10 AEF	Tivoli 10 Application Extension Facility
TMF	Tivoli Management Framework
TMR	Tivoli 10 Management Region
TSO	Time Sharing Option
TP	Transaction Program
UCT	Universal Coordinated Time
UID	User Identifier

Index

Symbols

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y