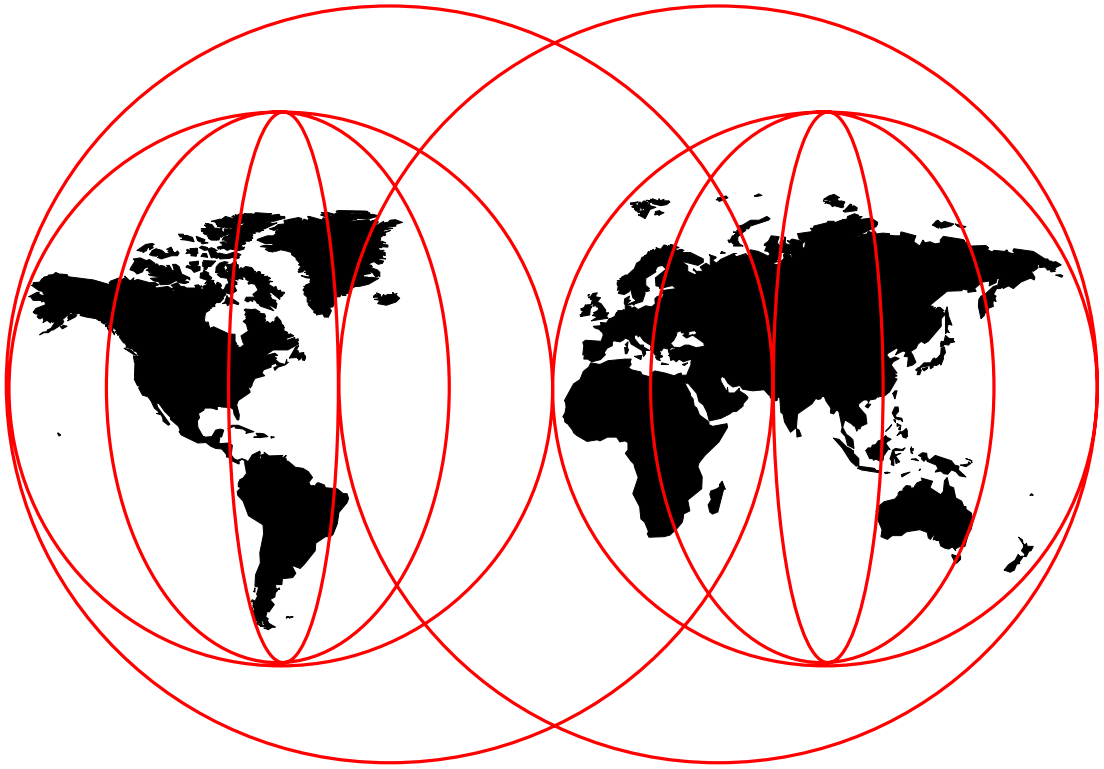
Integrating LAN Management Tools with Tivoli LAN Access

Barry D. Nusbaum, Thomas Ehmann, Monica Guillot Gimeno, Klemen Vidic, Michael Wiser



International Technical Support Organization

http://www.redbooks.ibm.com

SG24-2118-00

International Technical Support Organization

SG24-2118-00

Integrating LAN Management Tools with Tivoli LAN Access

July 1998

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix C, “Special Notices” on page 277.

First Edition (July 1998)

This edition applies to Version 1.1 and Version 1.1.1 of Tivoli LAN Access for use with the Windows NT 4.0 Operating System.

Note

This book is based on a pre-GA version of a product and may not apply when the product becomes generally available. We recommend that you consult the product documentation or follow-on versions of this redbook for more current information.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. HZ8 Building 678
P.O. Box 12195
Research Triangle Park, NC 27709-2195

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 vii

Preface xiii
The Team That Wrote This Redbook xiii
Comments Welcome xiv

Chapter 1. Installation and Configuration 1
1.1 How LAN Access Works 1
1.1.1 LAN Access Objects 1
1.2 Prerequisites for Installing LAN Access 1.1 on Framework 3.2 3
1.2.1 Installation of Tivoli LAN Access 1.1 3
1.2.2 Installation of the Tivoli LAN Access Component 5
1.2.3 Installation of LAN Access Components on the NT Managed Node . . 7
1.3 Administering LAN Access Objects in TME 11
1.4 Upgrade to Tivoli LAN Access 1.1.1 11
1.5 Configuration of the Tivoli Environment 15
1.5.1 Configuring the Desktop 15
1.6 Creating LAN Access Objects in TME 24
1.6.1 Creating a LAN Access Site 25
1.6.2 Creating a LAN Access Collection 33
1.6.3 Deleting a LAN Access Site Object 39
1.6.4 Viewing and Changing LAN Access Collection Properties 40
1.6.5 Deleting a LAN Access Collection Object 42
1.6.6 Viewing the Properties of a LAN Access Object Node 43
1.7 Scheduler 60
1.8 Configuring Support for LAN Alerts 62
1.9 Importing LAN Access Event Classes 64
1.10 Editing the Configuration File 70

Chapter 2. Intel LANDesk with Tivoli LAN Access V1.1 71
2.1 TMR Server 71
2.2 Managed Node 71
2.2.1 Sybase Server 72
2.2.2 LANDesk Management Workstation 72
2.2.3 LANDesk Management Server 72
2.3 Prerequisites for Installing LANDesk 73
2.3.1 Management Server 73
2.3.2 Management Workstation 73
2.3.3 NetWare 73
2.3.4 Windows NT 74
2.3.5 Software Probe Stations 74
2.3.6 Client Workstations 74
2.4 Installation and Configuration of Btrieve 74
2.4.1 Indicating Installation Targets 74
2.4.2 Installation 75
2.4.3 Change Btrieve Files from Read-Only to Normal 76
2.4.4 Btrieve Configuration to Accommodate LANDesk Management Suite 79
2.4.5 Applying the Btrieve 615.440 Update 81
2.5 Installation and Configuration of LANDesk 84
2.5.1 Indicating an Installation Target 85

2.5.2 Management Suite Tools . . . 89
2.5.3 System File Changes . . . 94
2.5.4 Things We Had to Do from the To Do List . . . 97
2.5.5 Check File Changes . . . 102
2.5.6 Client Configuration Utility . . . 104
2.6 Client Installation . . . 104
2.6.1 Windows 95 and Windows 3.x Clients . . . 104
2.6.2 NetWare Clients . . . 104
2.6.3 Windows NT Clients . . . 105
2.6.4 OS/2 Client Install . . . 106
2.6.5 Starting the LANDesk Management Suite . . . 107
2.7 MPM Provider Installation on the Management Workstation . . . 112
2.7.1 Driver Configuration . . . 115
2.8 LAN Access Provider Installation on the Managed Node . . . 117
2.9 Uninstall the Tivoli LAN Access Providers . . . 119
2.10 Alert Management . . . 121

Chapter 3. Netfinity 5.0 . . . 131
3.1 Netfinity . . . 131
3.2 Installing on Windows NT . . . 132
3.2.1 Installing on Windows 95 . . . 135
3.3 Installing on OS/2 . . . 135
3.3.1 Configuring the Netfinity Provider . . . 135
3.4 Installing the LAN Access Transport and Event Adapters . . . 139

Chapter 4. SMS 1.2 . . . 141
4.1 Installation of the SMS Environment . . . 142
4.1.1 Installation of Microsoft SQL Server . . . 143
4.2 Configuration of SQL Server . . . 145
4.3 Setting Directory Replication . . . 148
4.4 Installation of Microsoft Systems Manager Server V1.2 . . . 150
4.5 Configuring SMS for LAN Access Integration . . . 152
4.5.1 Enabling Software Distribution . . . 152
4.5.2 Enabling Inventory . . . 153
4.5.3 Enabling SMS Alerts . . . 164
4.6 Software Distribution . . . 169
4.7 Installation of LAN Access Components on the SMS Site . . . 171
4.8 Working with SMS Clients from Tivoli's Desktop . . . 175
4.8.1 Distributing Software . . . 175
4.8.2 Viewing Inventory Data . . . 190
4.8.3 Retrieving Inventory Data . . . 191
4.8.4 Receiving Alerts . . . 197

Chapter 5. Integration with the Framework . . . 199
5.1 Tivoli Application Support . . . 199
5.1.1 Using Tivoli Software Distribution . . . 199
5.1.2 Using Tivoli Inventory . . . 199
5.1.3 Using the Tivoli Enterprise Console . . . 200
5.2 Installing TME Software Distribution 3.1 . . . 207
5.2.1 Configuring Software Distribution . . . 209
5.2.2 Using LAN Access Together with Software Distribution . . . 221
5.2.3 Distribution to a LAN Access Client . . . 225
5.3 Example for Remote Command Execution . . . 229
5.3.1 Restrictions on Using Tivoli Software Distribution . . . 233

5.4 Preparing for Inventory 233
5.4.1 Configure Inventory 238
5.4.2 Setting the Inventory Profile Subscribers in Tivoli LAN Access . . . 240
5.4.3 Restrictions on Using Tivoli Inventory 248
5.4.4 Configuring the TEC Event Server 249

Appendix A. Configuration Files 259
A.1 LA_LDMS.BAROC 259
A.2 LA_NETF.BAROC 262
A.3 LA_SMS 266
A.4 LANACC.BAROC 266
A.4.1 readme File 268

Appendix B. Microsoft Information 275

Appendix C. Special Notices 277

Appendix D. Related Publications 279
D.1 International Technical Support Organization Publications 279
D.2 Redbooks on CD-ROMs 279

How to Get ITSO Redbooks 281
How IBM Employees Can Get ITSO Redbooks 281
How Customers Can Get ITSO Redbooks 282
IBM Redbook Order Form 283

Index 285

ITSO Redbook Evaluation 287

Figures

1. Tivoli LAN Access - SMS Environment . . . 4
2. Tivoli LAN Access - Netfinity and Intel LANDesk Environment . . . 5
3. Installation of LAN Access . . . 6
4. Installation of LAN Access . . . 7
5. Destination Location Window for LAN Access . . . 8
6. Authentication Window . . . 8
7. Administrators Window in the Tivoli Desktop . . . 9
8. Set Login Names Window . . . 9
9. Network Driver Configuration Window . . . 10
10. Completion Window . . . 10
11. Add Role Install Client . . . 11
12. Installing Upgrade . . . 12
13. Installing Upgrade . . . 13
14. Installing Upgrade . . . 14
15. Installing Upgrade . . . 14
16. Installing Upgrade . . . 15
17. Editing Notice Group Subscriptions . . . 16
18. Set Notice Groups Window . . . 16
19. Set Notice Group Window . . . 17
20. Read Notices Window . . . 17
21. Adding LANAccessSite Object to the Policy Region . . . 18
22. Setting LANAccessSite As a Managed Resource for the Region . . . 19
23. Setting LANAccessSite As a Managed Resource for the Region . . . 19
24. Tivoli Desktop . . . 20
25. Editing LANAccessSite Policies . . . 21
26. Managed Resource Policies Window . . . 22
27. Tivoli Desktop . . . 23
28. Editing Resource Roles for the Root Administrator . . . 23
29. Setting Resource Roles . . . 24
30. Creating a LAN Access Site Object . . . 26
31. LAN Access Site Creation Window . . . 26
32. LANAccess Log File . . . 27
33. LAN Access Site Creation Window . . . 28
34. Searching for MPM Systems . . . 29
35. LAN Access Site Creation Window . . . 30
36. LAN Access Site Creation Window . . . 31
37. Discovering Systems . . . 32
38. Enter User ID and Password . . . 32
39. Inside the Policy Region . . . 33
40. Creating a LAN Access Collection Object . . . 33
41. Creation of LAN Access Collection . . . 34
42. Choose LAN Management Tool . . . 35
43. Choose System Type . . . 35
44. Choose Operating System . . . 36
45. Choose NT/LAN Server Domain . . . 37
46. Selecting Systems . . . 38
47. Inside a LAN Access Site . . . 38
48. Inside a LAN Access Collection . . . 39
49. Delete Selected Objects . . . 39
50. Confirm Deletion of Selected Objects . . . 40

51. Changing LAN Access Collection Object . . . 40
52. Changing Properties of a LAN Access Collection . . . 41
53. Select Objects to Delete . . . 42
54. Confirming Deletion of Object . . . 42
55. LAN Access Object Node - Properties . . . 43
56. Create LAN Access Site - Delete Unwanted MPM Providers . . . 45
57. Newly Created LAN Access Site - winnt100_ip . . . 46
58. Setting Filter Criteria . . . 46
59. Selecting the Client Systems . . . 47
60. LAN Access Collection Test Created . . . 47
61. Discovered Client Systems . . . 48
62. Properties of a Selected Client System - Online . . . 49
63. Create LAN Access Site . . . 50
64. Entering the Netfinity UID and PW . . . 51
65. Creating LAN Access Collection in the LAN Access Site . . . 51
66. Set MS-Windows 95 As a Filter Criteria . . . 52
67. New LAN Access Collection Windows . . . 52
68. 11 Windows 95 Systems Found . . . 53
69. Properties of Machine - WINDOW95/NetBIOS . . . 54
70. Properties of Machine - OS2DSM7 . . . 55
71. Creating a LAN Access Collection with Windows NT Clients . . . 56
72. Netfinity Provider - Install Panel . . . 56
73. List View of the Clients . . . 57
74. Selecting OS/2 and Domain Name . . . 58
75. Name View of Clients Found . . . 59
76. Adding System Type Workstation . . . 59
77. All OS/2 Clients Plus the New Setting . . . 60
78. Tivoli Desktop . . . 61
79. Browse Scheduled Jobs . . . 61
80. Information about a Scheduled Job . . . 62
81. Provider UID-to-TEC Example . . . 63
82. Event Adapter Log File Example . . . 63
83. Compiling the Rule Base - Done . . . 67
84. Event Adapter Log File Example . . . 68
85. Event Adapter Log File Example . . . 69
86. Event Adapter Log File Example . . . 69
87. tecad_msb.cfg . . . 70
88. Server Component Installation Target Directory . . . 74
89. Requesters and Utilities Installation Target Directory . . . 75
90. Requesters and Utilities Installation Target Confirmation . . . 75
91. Backup Overwrite Option . . . 76
92. Find File Panel . . . 76
93. File Properties . . . 77
94. Things to Consider When Adjusting Btrieve's Parameters . . . 80
95. Defining Btrieve Parameter to Work with LANDesk Management Suite . 80
96. Configuration Panel on the NetWare Server . . . 81
97. Btrieve Update Utility . . . 83
98. Successful Update Panel . . . 83
99. Installation Reminder . . . 84
100. Btrieve Information . . . 85
101. Indicate an Installation Target . . . 85
102. NDS Information . . . 86
103. Verifying the Installation Paths . . . 87
104. Updating . . . 88

105. Adding a Tool . . . 89
106. Category Selection . . . 90
107. Workstation Management . . . 90
108. Server Management . . . 91
109. Wire Management . . . 92
110. Network Services . . . 93
111. DLL Metering Confirmation . . . 94
112. System File Changes . . . 95
113. LANDesk Management Suite Program Group . . . 95
114. Intel DMI Utilities Program Group . . . 96
115. NLM Upgrade . . . 96
116. Tool Addition . . . 96
117. LANDesk Installation Completion . . . 97
118. Network Configuration . . . 98
119. IPX/SPX-Compatible Protocol Properties . . . 99
120. Advanced Maximum Connections Settings . . . 100
121. Advanced Maximum Sockets Settings . . . 101
122. LANDesk Management Console . . . 107
123. Distribute Console's Tool Bar Icon . . . 108
124. Configuration Panel for Distribute . . . 108
125. Distribute Console . . . 109
126. Desktop Manager . . . 110
127. Management Console/WUser Icon . . . 111
128. WUser Window . . . 111
129. LAN Access Installation Location . . . 113
130. LAN Access Directory Targets . . . 114
131. LAN Access Transport Target Directory . . . 115
132. LAN Access Network Driver Configuration . . . 116
133. LAN Access Setup Complete . . . 116
134. LAN Access Installation Target Directory . . . 117
135. LAN Access Transport Target Directory . . . 118
136. LAN Access Network Driver Configuration . . . 118
137. LAN Access Setup Complete . . . 119
138. Uninstall Confirmation . . . 120
139. MPM Provider List . . . 120
140. LAN Access Server Manager Tool Bar Icon . . . 121
141. Server Status . . . 122
142. CPU Utilization Graph . . . 122
143. Setting a CPU Threshold . . . 123
144. Event Configuration . . . 123
145. Event Selection . . . 124
146. Event Creation . . . 124
147. Event Selection and Configuration . . . 125
148. Tool (Action) Selection . . . 125
149. Message Box Tool (Action) Configuration . . . 126
150. Alert Message Box . . . 127
151. Advanced Tool Configuration . . . 128
152. MPM Tool (Action) Configuration . . . 129
153. Event Selection . . . 129
154. Event Selection Completed . . . 130
155. Install Fix for Netfinity 4.0 . . . 131
156. Netfinity Provider - Choose Destination Location . . . 133
157. Netfinity Provider - Select Components (Part 1 of 2) . . . 134
158. Netfinity Provider - Select Components (Part 2 of 2) . . . 134

159. Netfinity Provider - Install Panel . . . 135
160. Configuring Netfinity Provider . . . 136
161. Database Directory . . . 136
162. Part of Software Inventory . . . 137
163. Part of Hardware Inventory . . . 138
164. Configuring Netfinity Provider Finished . . . 138
165. Servers Used As Logon Servers . . . 142
166. SMS Environment . . . 142
167. NT 4.0 User Manager Options or SQL User ID . . . 143
168. SQL 6.5 Sort Order . . . 144
169. SQL Installation Path . . . 144
170. SQL Installation Complete . . . 145
171. Security for the System Administrator User ID . . . 146
172. Configure the SQL Server . . . 147
173. SQL Server Configuration . . . 148
174. Configure Directory Replication . . . 149
175. Directory Replication . . . 149
176. Install the SMS Primary Site . . . 150
177. Setup Install Options . . . 150
178. To Connect to the SQL Database . . . 151
179. Site Information . . . 152
180. Creation of a Shared Folder . . . 153
181. Compilation of audit.rul . . . 154
182. audit.PDF Contents . . . 154
183. Open SMS Window . . . 155
184. Package Properties . . . 155
185. Importing a Package Definition File . . . 156
186. Specifying Source Folder . . . 156
187. Directory Browser . . . 157
188. Specifying Source Folder . . . 158
189. Creating a New Job . . . 158
190. Job Properties . . . 159
191. Job Details . . . 160
192. Jobs Window . . . 160
193. Package Command Manager - Audit Software . . . 161
194. Modifying the Polling Interval . . . 161
195. Package Command Manager Options . . . 162
196. Audit Status . . . 162
197. Site Properties . . . 163
198. Inventory Window . . . 163
199. Sites Window - Systems in Domain SMSDOM . . . 164
200. Results of Software Auditing . . . 164
201. Open SMS Window . . . 165
202. Queries . . . 165
203. Query Properties . . . 166
204. Alert's Properties . . . 166
205. Queries . . . 167
206. Value Required . . . 167
207. Value to Enter . . . 168
208. Defining the Actions . . . 168
209. Alert Action . . . 169
210. Welcome Window . . . 171
211. Destination Location Window for SMS Provider . . . 172
212. SMS Provider Configuration . . . 172

213. SMS Provider Configuration . . . 173
214. SMS Provider Configuration . . . 173
215. Destination Location Window for LAN Access Transport Component . 173
216. Authentication Window . . . 174
217. Network Driver Configuration Window . . . 175
218. Creating Profile . . . 176
219. Profile Manager Window . . . 177
220. File Package Properties . . . 178
221. Selecting Platform Specific Options . . . 179
222. Windows NT Options Window . . . 180
223. Selecting Subscribers for the Profile . . . 181
224. Setting Subscriptions . . . 181
225. Distributing Profile . . . 182
226. File Package Distribution Window . . . 183
227. Packages . . . 184
228. Jobs . . . 184
229. Queries . . . 185
230. Package Properties . . . 185
231. Job Properties . . . 186
232. Job Details . . . 186
233. Package Command Manager at the SMS Client . . . 187
234. Task Manager Window of the SMS Client . . . 188
235. Windows NT Explorer . . . 189
236. create_os_detail_view.sql for Sybase . . . 190
237. Create Profile Window . . . 191
238. Customizing an Inventory Profile . . . 192
239. Customize Inventory Profile Window . . . 193
240. Selecting Targets for Discovery . . . 194
241. Running the Hardware Query . . . 195
242. Results of Query . . . 196
243. Create Profile Window . . . 197
244. Desktop Logon Panel . . . 200
245. TME Desktop . . . 201
246. TME Desktop with TEC Server and Enterprise Console Started . . . 202
247. TME Event Source . . . 203
248. TME Event Groups . . . 203
249. TME All Group's Display . . . 204
250. TEC-MPM CPU Utilization Alert 1 of 2 . . . 205
251. TEC-MPM CPU Utilization Alert 2 of 2 . . . 206
252. Adjusting a CPU Threshold . . . 207
253. Install Product . . . 208
254. Product Install . . . 209
255. Create Profile Manager in Policy Region . . . 210
256. Create Profile Manager . . . 210
257. New Profile Manager in Policy Region . . . 211
258. Create Profile . . . 212
259. Profile Manager . . . 213
260. File Package Properties . . . 214
261. Select Source Host . . . 215
262. Select Directories & Files . . . 216
263. File Package Properties . . . 217
264. Select Platform-Specific Options . . . 218
265. Build File Package Windows NT Options . . . 219
266. New Profile in Profile Manager . . . 220

267. Subscribers Added . . . 221
268. Profile Manager - Add Subscriber . . . 222
269. Available Subscribers . . . 223
270. Select the Subscribers . . . 224
271. Profile Manager with New Subscribers Added . . . 225
272. File Package Properties . . . 226
273. Setting Platform-Specific Options . . . 227
274. Distribute File Package . . . 228
275. Log File after Successful Distribution . . . 229
276. Target Machine . . . 229
277. Create Profile . . . 230
278. Create Commit Script . . . 231
279. Start Program Using the Commit Only Option . . . 232
280. clock.exe Started . . . 233
281. Start Sybase . . . 234
282. Sybase Ping Utility . . . 235
283. Sybping . . . 235
284. tivoli_syb_admin.sql . . . 236
285. Creating Inventory Database . . . 236
286. Create Database Schema . . . 237
287. Check Database Connection . . . 237
288. Start Customize Inventory Profile . . . 238
289. Customize Inventory Retrieval . . . 239
290. Start Add Subscribers to Profile Manager . . . 240
291. Available Subscribers . . . 241
292. Adding Clients to the Current Subscribers Field . . . 242
293. Subscribers . . . 242
294. Profile Manager with New Subscribers . . . 243
295. Inventory Profile Dialog . . . 244
296. Build Inventory Profile - Start Scan . . . 245
297. Create Query Library . . . 245
298. Policy Region with New Query Library . . . 246
299. Create Query . . . 246
300. Create Query Dialog . . . 247
301. Start Query . . . 247
302. Execute a Query . . . 248
303. Edit Rule Bases . . . 249
304. Event Server Rules Bases Window . . . 250
305. Creation of Rule Base . . . 250
306. Copying Default Rule Base . . . 251
307. Copying Default Rule Base . . . 252
308. Importing LAN Access Event Class Files . . . 253
309. Importing lanacc.baroc File . . . 254
310. Importing la_sms.baroc File . . . 255
311. Compiling Rule Base . . . 256
312. Compile Rule Base Window . . . 256
313. Loading the Rule Base . . . 257
314. Load Rule Base Window . . . 257
315. Event Server Rules Bases Window . . . 258
316. Event Class for LANDesk Management Suite V2.51 MPM Provider . . . 259
317. Event Class for Netfinity MPM Provider . . . 263
318. Tivoli Event Classes for Management Services Broker . . . 267
319. readme . . . 268
320. Knowledgebase Article Q166244 . . . 275

Preface

This redbook will help you install, tailor, and configure Tivoli LAN Access. In addition, it will show you how to use the supported LAN Management Suites from IBM, Microsoft and Intel to provide an integrated management solution.

After showing how to install each of the products (Tivoli LAN Access, LANDesk, SMS and Netfinity), the book provides several examples of how to use the tools and functions that are provided with all these products.

This book will be especially useful for professionals who are involved with both systems management and LAN management on the Intel-related platforms. While some basic knowledge of the Tivoli Framework is assumed, the book helps guide you through the usage of the products as well as explains how the pieces fit together.

The Team That Wrote This Redbook

This redbook was produced by a team of specialists from around the world working at the Systems Management and Networking ITSO Center, Raleigh.

Barry D. Nusbaum is a Senior International Technical support representative at the Systems Management and Networking ITSO Center, Raleigh. He writes extensively and teaches IBM classes worldwide on all areas of Tivoli systems management on the NT and AIX platform. He is also currently working on projects related to the Network Computing Framework. Before joining the ITSO five years ago, he worked in Professional Services in the United States as a National Communications Specialist. You can reach him by e-mail at bnusbaum@us.ibm.com.

Michael Wiser is a Systems Management specialist at the Personal Solutions Systems Center in Roanoke, Texas, USA. He has spent his entire career in the systems management field. His areas of expertise include Netfinity on all platforms.

Thomas Ehmann is a software and Tivoli specialist in Germany. He has seven years of experience in network and systems management. He has worked at IBM for 12 years.

Monica Guillot Gimeno is a Systems Management specialist in Spain. She is currently focusing on Tivoli products on the NT and UNIX platforms.

Klemen Vidic is a Microsoft Certified Systems Engineer and Trainer in Slovenia. He works at IBM in the Systems Management department of the Software Group.

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

David Watts and Rufus Credle
Systems Management and Networking ITSO Center, Raleigh

Chris Gaskins, Susan Holahan, Mark Ross, Joe Lambertus,Wayne Schildhauer
Tivoli Corporation, RTP

Roy Ritthaler, Simon Lew
Tivoli Corporation, Austin

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 “ITSO Redbook Evaluation” on page 287 to the fax number shown on the form.
- Use the electronic evaluation form found on the Redbooks Web sites:

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

- Send us a note at the following address:

  `redbook@us.ibm.com`

Chapter 1. Installation and Configuration

This chapter explains the different pieces that are part of Tivoli LAN Access as well as describes the installation and customization of the products in our environment. This project was done in two phases, so we had two different sets of equipment.

1.1 How LAN Access Works

Tivoli LAN Access consists of the following components:

- A LAN Access component that allows you to create a set of new LAN Access objects that plug into Tivoli Framework and interface with existing Tivoli applications.
- A Tivoli event adapter that enables LAN Access to receive network events from supported LAN management applications.
- A multiprotocol transport that enables communication between LAN Access and supported LAN management applications.
- LAN Access API code called Multi-Platform Manager (MPM) providers. MPM providers enable Tivoli applications to use existing transport protocols (TCP/IP, NetBIOS and SNA/APPC) to manage other workgroup managers (Netfinity, SMS and Intel LANDesk).

Figure 1 on page 4 shows where all the pieces fit in. While that figure is for the SMS environment, it also applies to Netfinity and Intel LANDesk.

1.1.1 LAN Access Objects

Tivoli LAN Access objects are used to represent LAN clients on the Tivoli Desktop. Once defined, LAN Access objects can be used by Tivoli Inventory and Software Distribution applications. The GUI for these new objects are consistent with the Tivoli desktop interface. See Figure 61 on page 48 for a sample of what the clients look like.

LAN Access objects created in the TME are:

- LAN Access Site Object

  The LAN Access site object resides on an NT managed node, displays as a managed resource, and allows you to select the network locations where MPM providers have been installed.

- LAN Access Collection Object

  The LAN Access collection object is created inside a LAN Access site object and represents a filtered grouping of LAN tool clients.

- LAN Access Node Object

  The LAN Access node object represents a single LAN client. A LAN Access node object must exist in at least one LAN Access collection object, but can also exist in multiple LAN Access collection objects.

All three types of objects can subscribe to one or more profile managers. Distributing a profile to a Tivoli LAN Access object performs the action upon all LAN clients that are members of that particular LAN Access object. You may need to

distribute a profile to an entire LAN, to a filtered group of LAN clients, or to a single LAN client. LAN Access objects give you the flexibility to perform network operations for all of these scenarios, according to the needs and requirements of your organization.

There are four types of systems that are used in the Tivoli LAN Access environment:

1. TMR Server
2. LAN Access managed node
3. LAN managing station
4. LAN managed stations

The platforms that LAN Access supports for each of these systems are:

- UNIX or Windows NT for the TMR Server
- Windows NT for the LAN Access managed node
- Windows NT for the LAN managing station which is actually the Netfinity Manager, Intel LANDesk Manager or SMS Site server system
- OS/2 for Netfinity

Refer to the *Tivoli LAN Access User's Guide* for more information on the prerequisites of the operating system and software needed on the machines for installing LAN Access.

1.1.1.1 TME Event Adapter

Tivoli LAN Access provides a dedicated event adapter to process LAN-generated alerts. When you create a LAN Access site object, the event adapter is initialized to begin monitoring for alerts. When an alert is received, the LAN Access event adapter sends an event to the event server so that the event can be viewed from and processed by the Tivoli Enterprise Console.

1.1.1.2 Multiprotocol Transport

LAN Access provides transport components to enable communication between the NT managed node where LAN Access is installed and the LAN stations where MPM providers are installed. The LAN Access transport supports TCP/IP, NetBIOS, IPX, and SNA to ensure integration with existing LANs.

1.1.1.3 MPM Providers

MPM providers use the Multi-Platform Management application programming interface (MPM API). The MPM API allows one management application to communicate with another management application by presenting a common API. The MPM API is an open specification and is available for use without royalties.

HTML Pointers

Additional information on the MPM-API can be found at:

- http://www.tivoli.com/o_products/html/body_lan_wp.html

  - *Integrating LAN Management Tools with Tivoli* (White Paper)

- http://www.tivoli.com/o_download/html/mpm_overview.html

  Multi-Platform Manager API Software Developer Kit (Overview and FAQ)

1.2 Prerequisites for Installing LAN Access 1.1 on Framework 3.2

Before beginning the installation of Tivoli LAN Access you should make sure that your LAN tools (SMS, Intel LANDesk or Netfinity) are working correctly. This will be helpful if any problems are discovered during the implementation phase of Tivoli LAN Access.

If you are installing the base release of Tivoli LAN Access V1.1 on the Tivoli V3.2 Framework you will need to make a modification to the IND file. The process you should follow is:

- Copy the contents of LAN Access CD-ROM onto a temporary drive.
- Edit the file LACCESS.IND.
- Delete the last two lines of this file so as to eliminate the dependencies upon Framework 3.1 or Framework 3.1.2.

```
LACCESS:description:Tivoli LAN Access Version 1.1:TIV_MSB
LACCESS:id:CAT:Message Catalogs:both::::
LACCESS:fp:CAT:generic::30:1
LACCESS:id:ALIDB:Server Database:server:@HostName@.db:::
LACCESS:fp:ALIDB:generic::150:2
LACCESS:id:BIN:Binaries:both:@Arch@:::
LACCESS:fp:BIN:w32-ix86::2500:3
LACCESS:fp:BIN:aix3-r2::500:4
LACCESS:fp:BIN:aix4-r1::500:5
LACCESS:fp:BIN:hpux9::500:6
LACCESS:fp:BIN:hpux10::500:7
LACCESS:fp:BIN:solaris2::500:8
LACCESS:fp:BIN:sunos4::500:9
LACCESS:patch_id:LA_1.1
LACCESS:depends:TMP_3.1
LACCESS:depends:TMF_3.1.2
```

Deleting those last two lines removes a dependency check.

1.2.1 Installation of Tivoli LAN Access 1.1

You should have all Tivoli applications and the necessary patches installed as well as the managing application in the appropriate systems before installing Tivoli LAN Access 1.1. For applications on Tivoli Framework 3.2 we used: Tivoli Inventory 3.2, Tivoli Software Distribution 3.1 and Tivoli TEC 3.1. In the following two figures we show our environment and the products needed, depending on the systems role in LAN Access integration. We have also specified the LAN Access components required in each system.

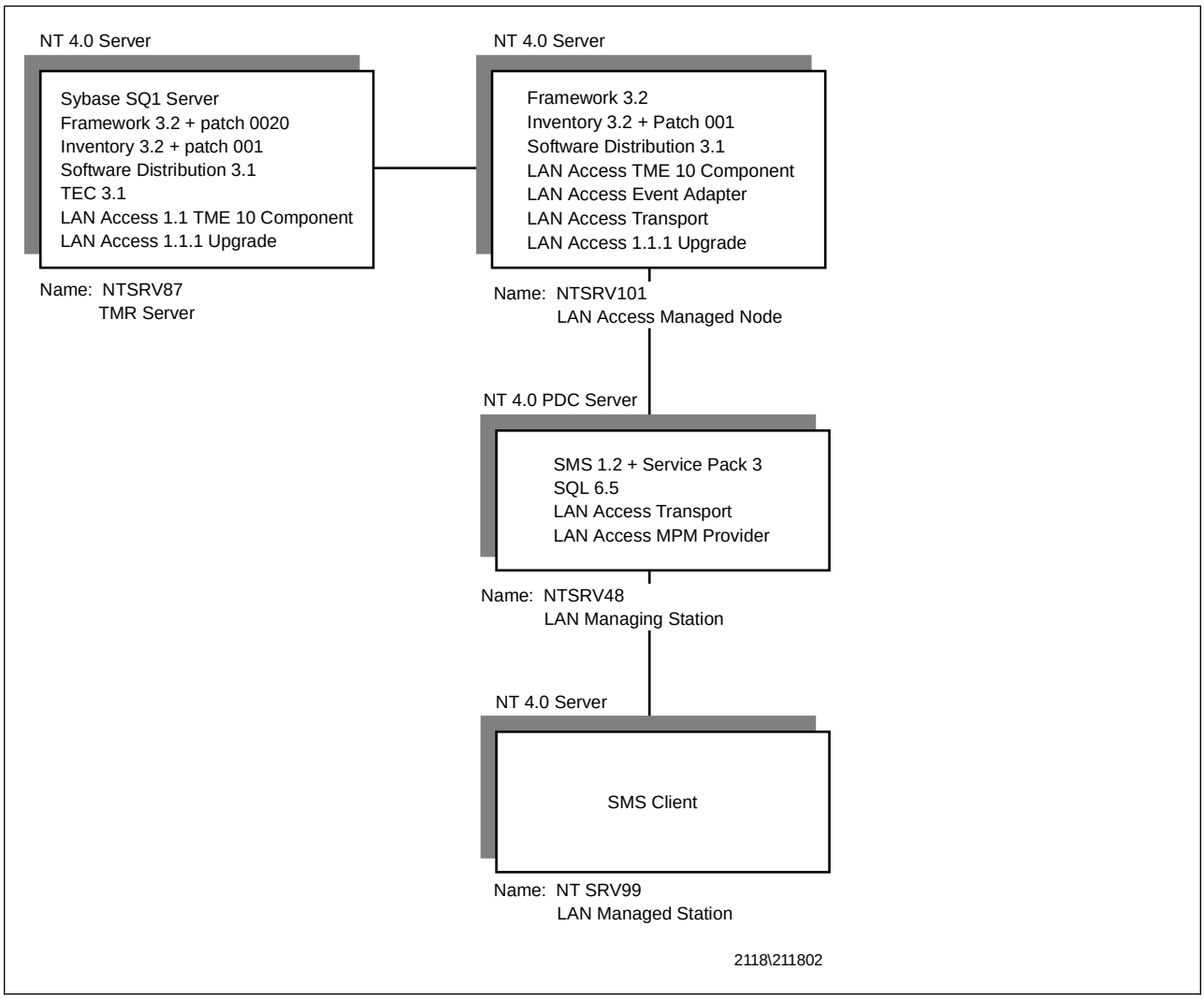


Figure 1. Tivoli LAN Access - SMS Environment

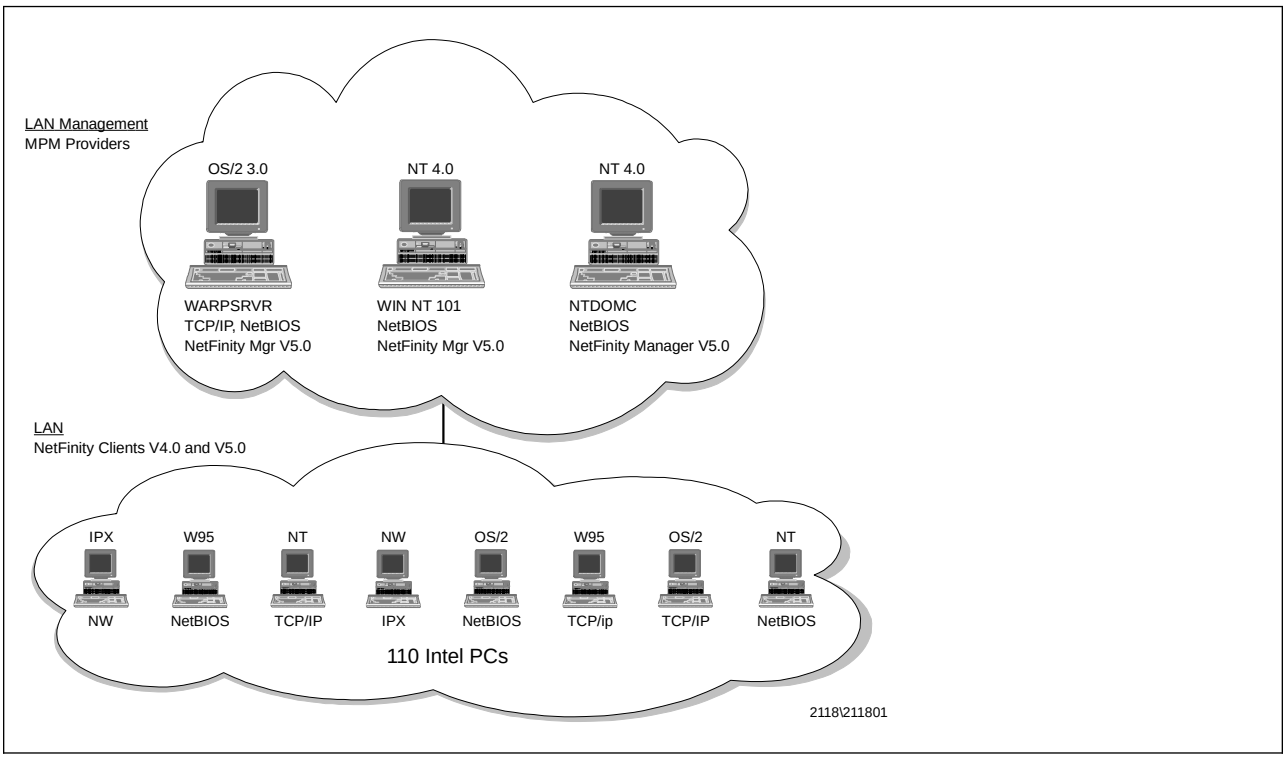


Figure 2. Tivoli LAN Access - Netfinity and Intel LANDesk Environment

1.2.2 Installation of the Tivoli LAN Access Component

The Tivoli LAN Access V1.1 component has to be installed as a base product before you can install V1.1.1. You install this component using the Tivoli desktop on the TMR server, which can be a UNIX or an NT system, and on the NT managed nodes. In our environment we just used NT systems.

Note: As with all product installations, you should back up your Tivoli database before making any changes.

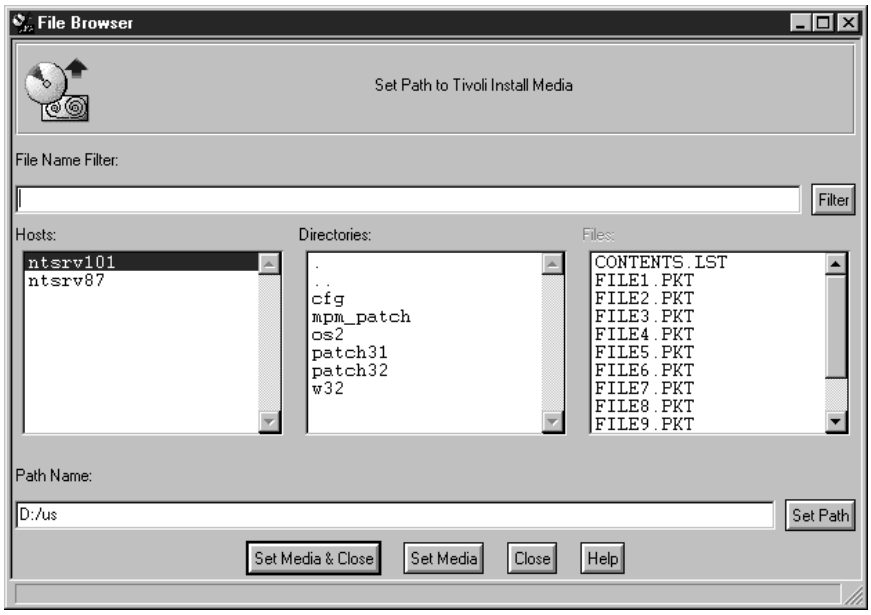


Figure 3. Installation of LAN Access

Note: The media path should point to the temporary drive where you copied the contents of the CD.

Enter the path (absolute path names are required) where your Tivoli LAN Access product files are stored. Click on the **Set Path** button. After that, a window similar to Figure 3 should appear. You should see, at a minimum, a CFG directory and files with extensions of PKT in that directory. If that is what you see, click on **Set Media & Close**. This leads you to the Install Product panel shown in Figure 4 on page 7.

Set the media path to point to the temporary drive where you copied the contents of the CD.

Figure 4. Installation of LAN Access

Include in the Clients to Install On list the TMR server and all other managed nodes that will be used as LAN Access sites. Since Install Options is not available there are no other tailoring options (for example, setting directories) to perform.

The product install for Tivoli LAN Access is no different from any other Tivoli application. You will see a window that shows you what files will be copied and after you click on **Continue Install** it will copy the files to the correct systems. It will then register the application in the Tivoli managed region.

1.2.3 Installation of LAN Access Components on the NT Managed Node

To install the components needed on the NT managed node, you have to run setup.exe found under \us\w32\ on the CD. You run the setup on the managed node itself, not from the TMR. Tivoli LAN Access automatically detects what components are needed and selects and installs them for you, so for the NT managed node, the LAN Access event adapter and LAN Access transport will be installed.

Note: The only thing that is unique across the three providers (Netfinity, SMS and Intel LANDesk), is that for V6.0 and V6.1 of Intel LANDesk you need to run setup.exe tme instead of just setup.exe.

The screens that follow show the steps for the installation:

Click on **Next** since this is just an initial welcome window.

Figure 5. Destination Location Window for LAN Access

Click on **Next** after you set the LAN Access directory.

If you choose destination directories that do not exist, they will be created for you. After you have decided on the directory click on **Next**.

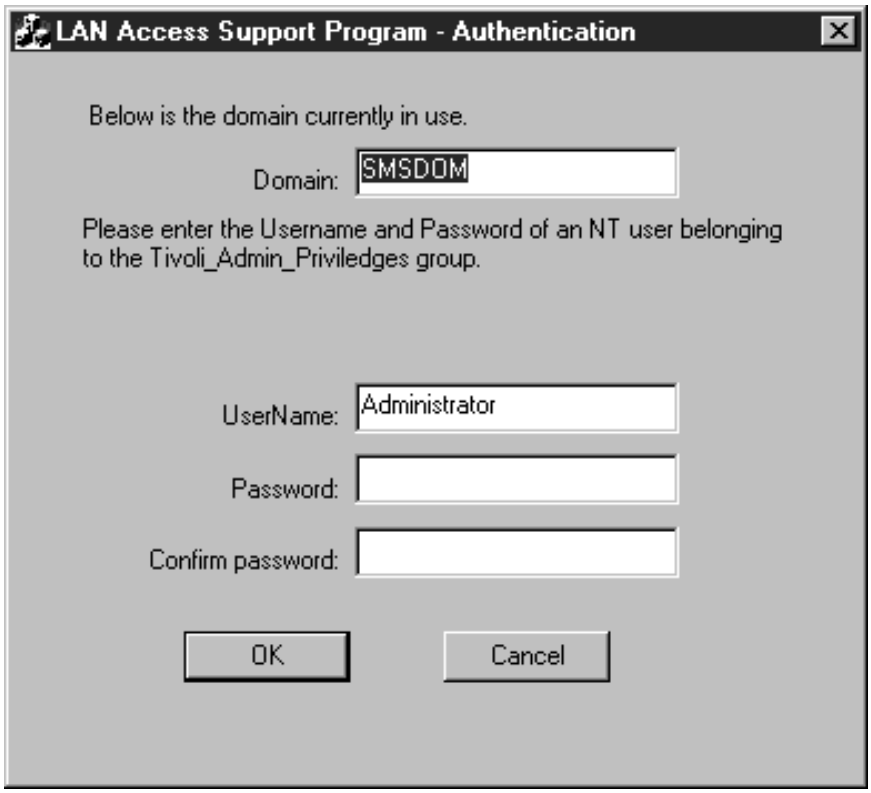


Figure 6. Authentication Window

Tivoli needs to have access authority to start the LAN Access event adapter. The user entered in these fields should be a member of the Tivoli_Admin_Priviledges group in the NT managed node and should also be included in the current login names list for the Tivoli root administrator in the TMR server. In the next two figures we show where you can find the login names for the Tivoli administrator. This can be done once the LAN Access installation is complete.

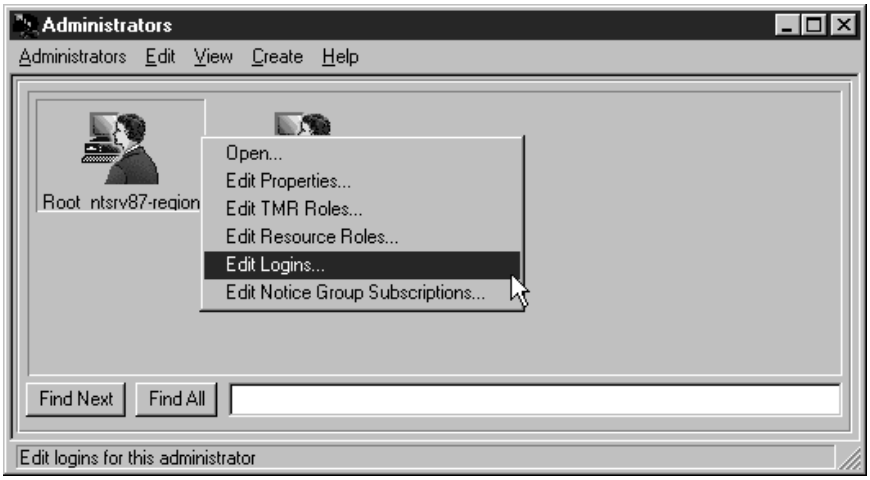


Figure 7. Administrators Window in the Tivoli Desktop

Right-click on the Tivoli administrator and select the **Edit Logins** option to display the Set Login Names window. If the login name is not listed, you can add it by entering the name in the Add Login Name field and clicking on **Change & Close**.

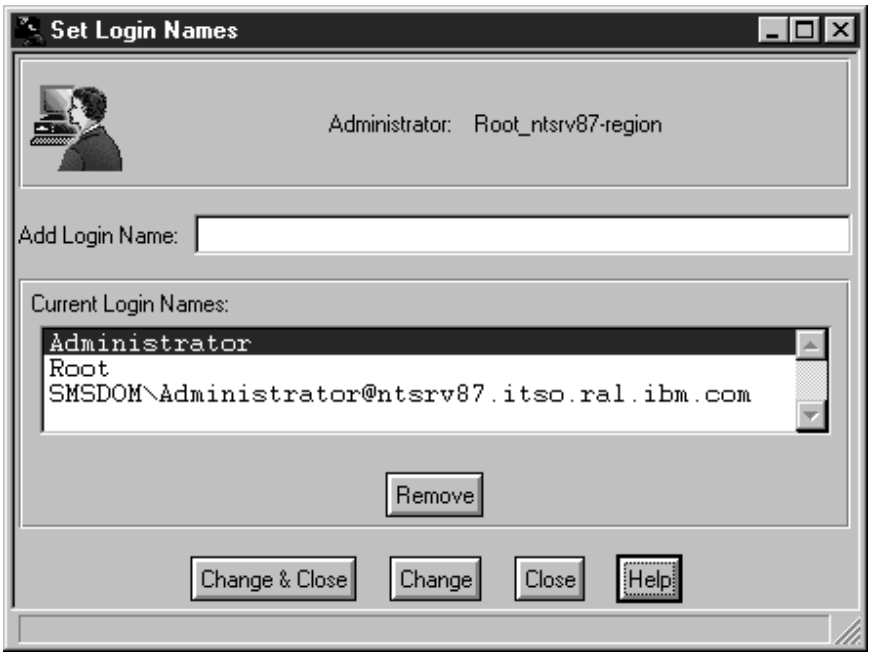


Figure 8. Set Login Names Window

LAN Access automatically detects the network drivers installed in the system. You should enable the driver that the NT managed node is going to use to communicate with the SMS site. In this example we have NetBIOS, IEEE 802.2 (SNA/APPC)

and TCP/IP. In this book we work with TCP/IP and NetBIOS. To start off we only enabled the TCP/IP transport protocol.

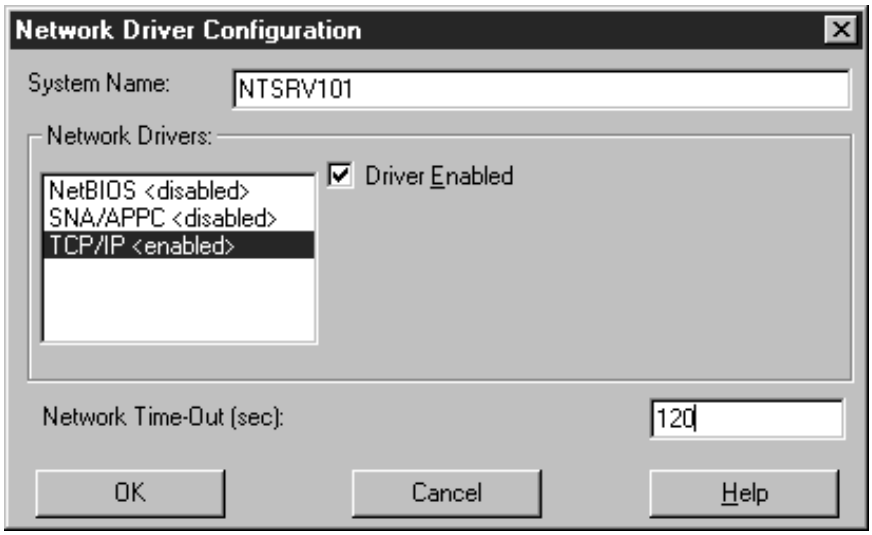


Figure 9. Network Driver Configuration Window

The default network timeout is 15 seconds. You should modify this value taking into consideration the load and speed of your systems and network. If you have many bridges and routers, or slow links that your traffic will be going over, you may need a higher value then 15.

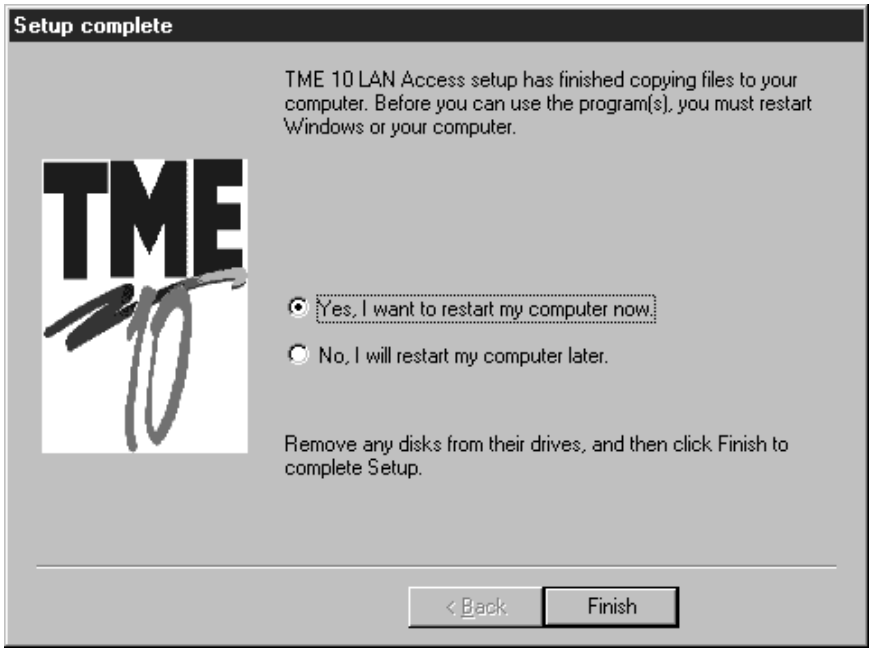


Figure 10. Completion Window

Click on **Finish** to close this window and reboot the system.

The installation of the LAN Access components on the providers is shown in the locations that focus on them: Chapter 2, “Intel LANDesk with Tivoli LAN Access V1.1” on page 71, 3.2, “Installing on Windows NT” on page 132 and Chapter 4, “SMS 1.2” on page 141.

Note: You will have to complete that part of the installation to be able to work with LAN Access.

1.3 Administering LAN Access Objects in TME

Make sure that the following prerequisites are installed or available. To create LAN Access objects it is required that:

- The LAN Access TME component, event adapter, and transport are installed on the managed node if you want events to flow.
- The MPM providers are installed, configured and operational.
- You have TME 10 install_client authority in the policy region in which the objects will be created.

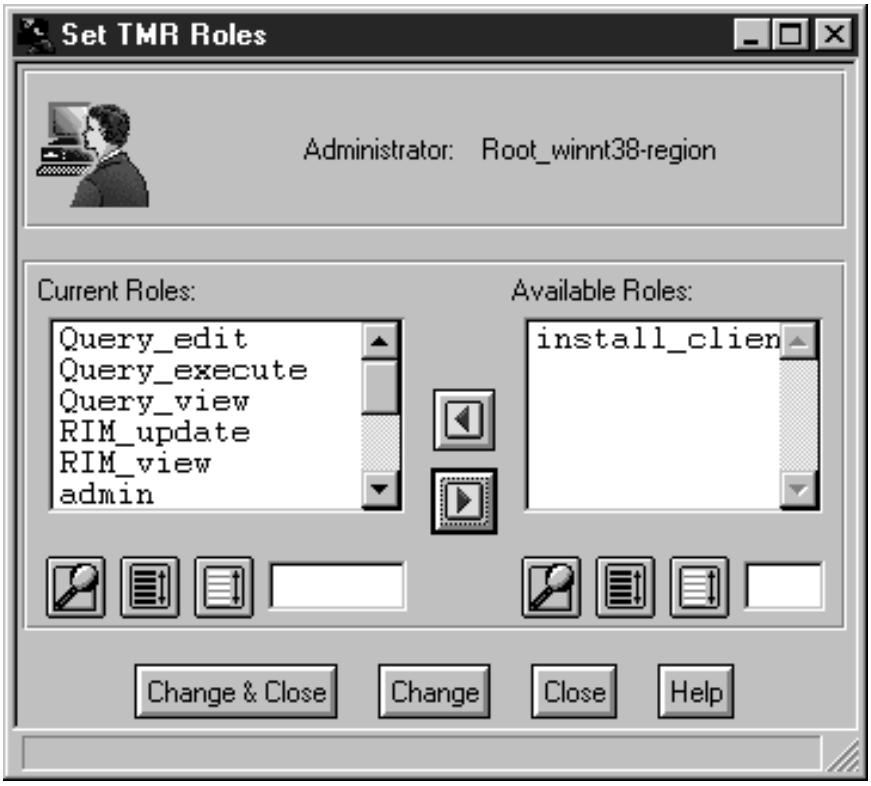


Figure 11. Add Role Install Client

Error messages that occur are recorded in the LAN Access Notices group (see Figure 20 on page 17).

1.4 Upgrade to Tivoli LAN Access 1.1.1

Tivoli LAN Access 1.1.1 is an upgrade to Tivoli LAN Access 1.1. This upgrade also consists of two parts, a TME and a non-TME part.

- The TME part is the Tivoli LAN Access V1.1.1 upgrade for TMF 3.2 and it is installed from the Tivoli desktop with the install patch option on the TMR server and on all LAN Access managed nodes. The path on the CD for this part is \us\patch32\.

- The non-TME part is the Tivoli LAN Access 1.1.1 upgrade for the provider nodes. It must be installed on all sites where we previously installed the provider and on the LAN Access managed nodes. The directory path for the installation of this part is \us\mpm_patch\.

Note: Don't forget to read the Tivoli LAN Access 1.1.1 Release Notes and the README file on the CD, before attempting this installation to make sure you have performed all the prerequisite steps.

1.4.1.1 LAN Access 1.1.1 Upgrade for Tivoli Framework 3.2

Note: You will need to apply a framework patch so that software distribution will work. In addition, you will have to execute an SQL script for inventory to work. These are documented in the 1.1.1 Release Notes.

The upgrade is done using the wpatch command or using the Tivoli desktop. We installed the patch using the desktop Install Patch menu option. Our TMR was located on ntsrv87 and ntsrv101 was our LAN LAN Access managed node. We also installed the patch on ntsrv101.

Note: As with all product upgrades you should first take a backup of your TMR's database.

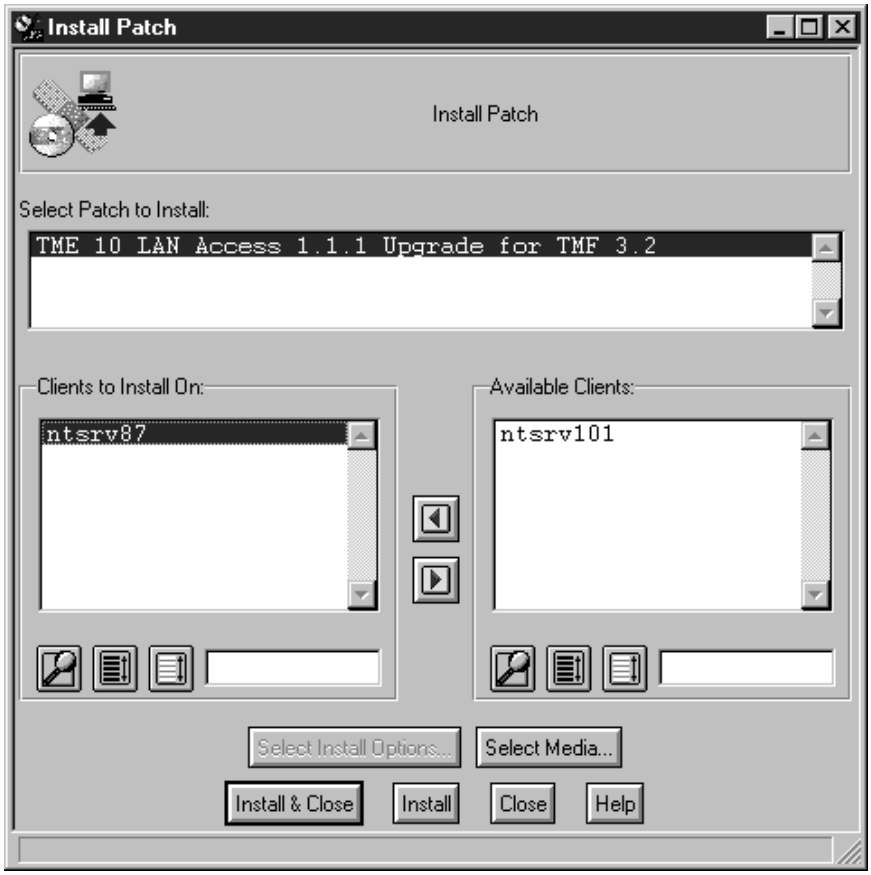


Figure 12. Installing Upgrade

After entering the location we clicked on **Install & Close**.

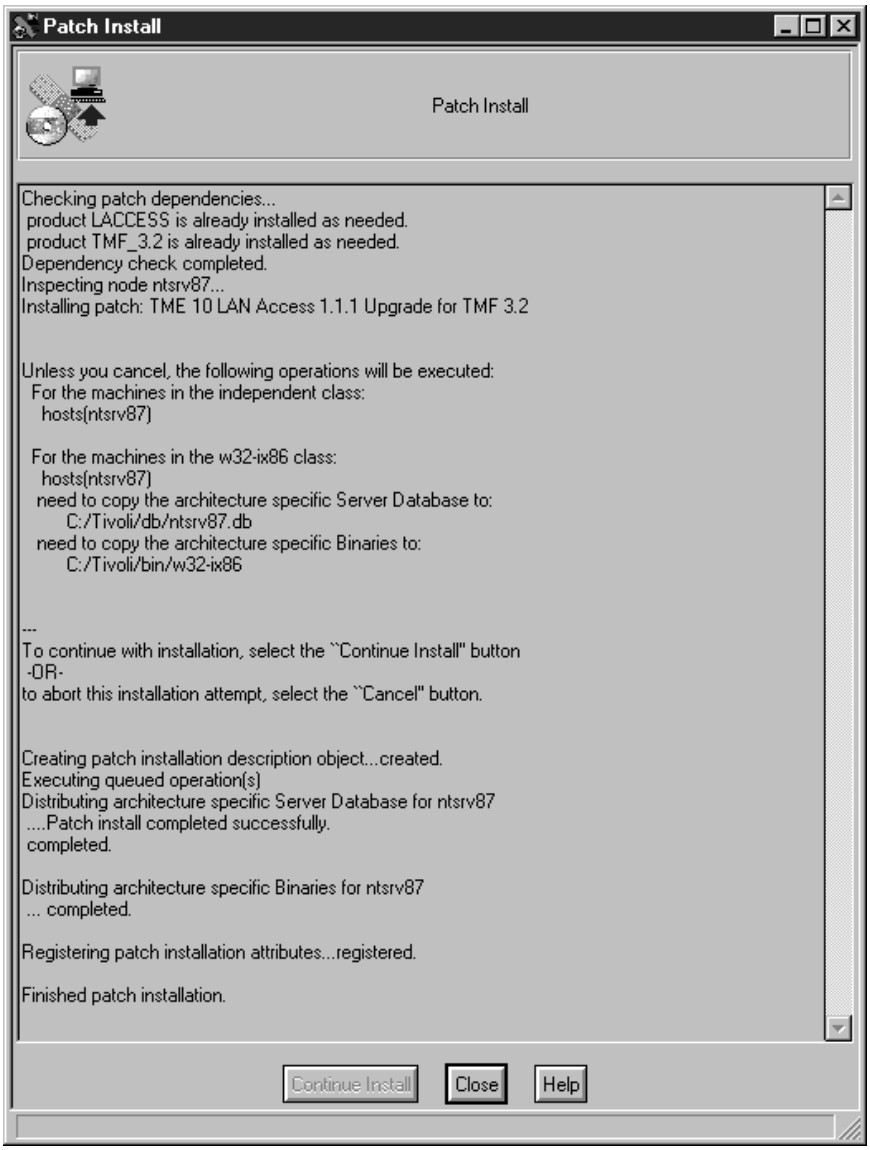


Figure 13. Installing Upgrade

The patch installed successfully and we were upgraded to Tivoli LAN Access V1.1.1. After that we took another backup of our Tivoli database.

1.4.1.2 LAN Access 1.1.1 Upgrade for Provider Nodes

A patch was also required to be installed on the MPM provider sites. There is not a separate patch for each provider. The only exception being that you need to use the following for Intel LANDesk 6.0 and 6.1:

```
setup.exe tme
```

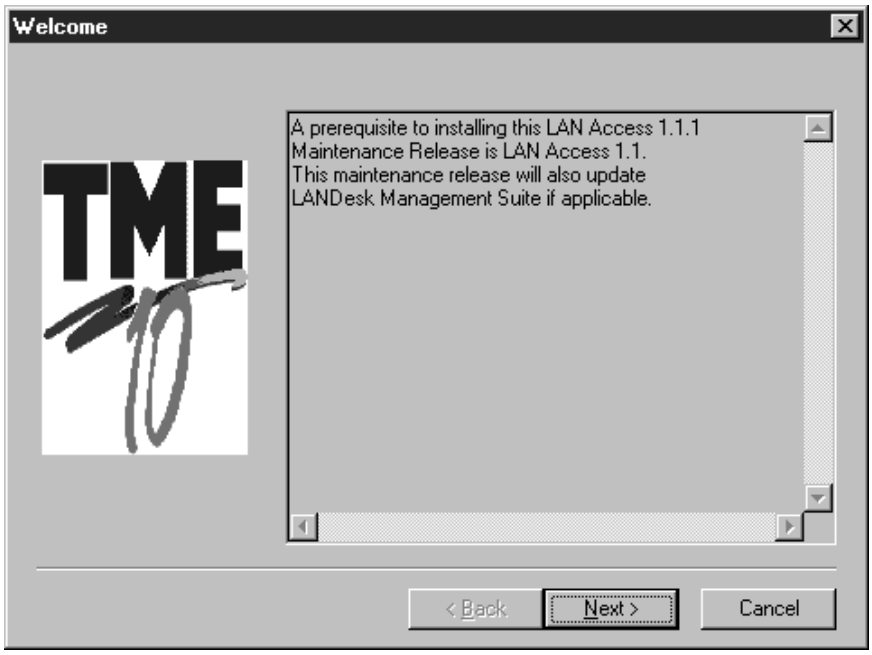


Figure 14. Installing Upgrade

The updated code will be placed in the same directory as the base Tivoli LAN Access V1.1 code.

Figure 15. Installing Upgrade

You will need to reboot your MPM provider after installing the patch.

Figure 16. Installing Upgrade

1.5 Configuration of the Tivoli Environment

The next thing to do, after a complete and successful installation of the environment, is to make several configuration changes to complete the LAN Access integration with the framework and be able to work with the clients as if they were Tivoli objects.

1.5.1 Configuring the Desktop

The Tivoli component of LAN Access adds LAN Access objects to the Tivoli desktop. These objects are a new notice group for LAN Access notification and a managed resource to manage LAN Access nodes. You will have to include these objects in the appropriate administrator or policy region that is going to work with those objects. We are going to show how this is done.

1.5.1.1 LANAccess Notice Group

To add the LANAccess notice group to Tivoli's root administrator, double-click on the administrator's icon on the desktop. This displays the Administrators window.

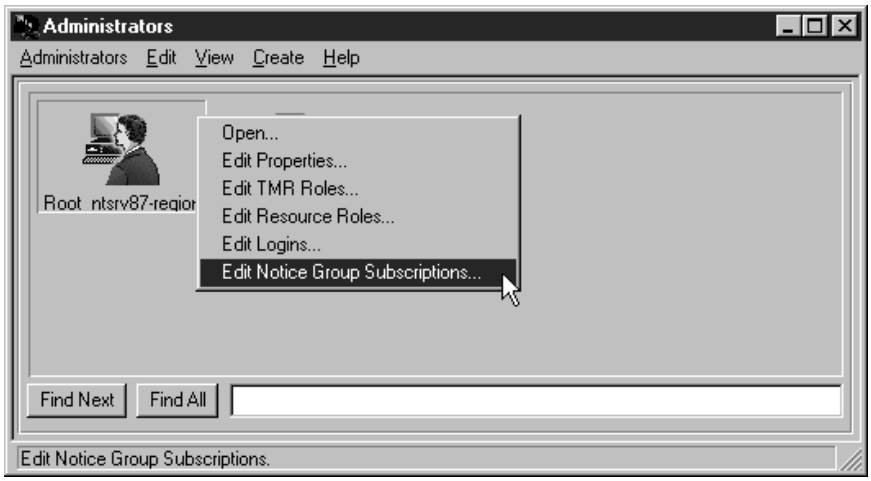


Figure 17. Editing Notice Group Subscriptions

Select **Edit Notice Group Subscriptions...** after right-clicking on the root administrator.

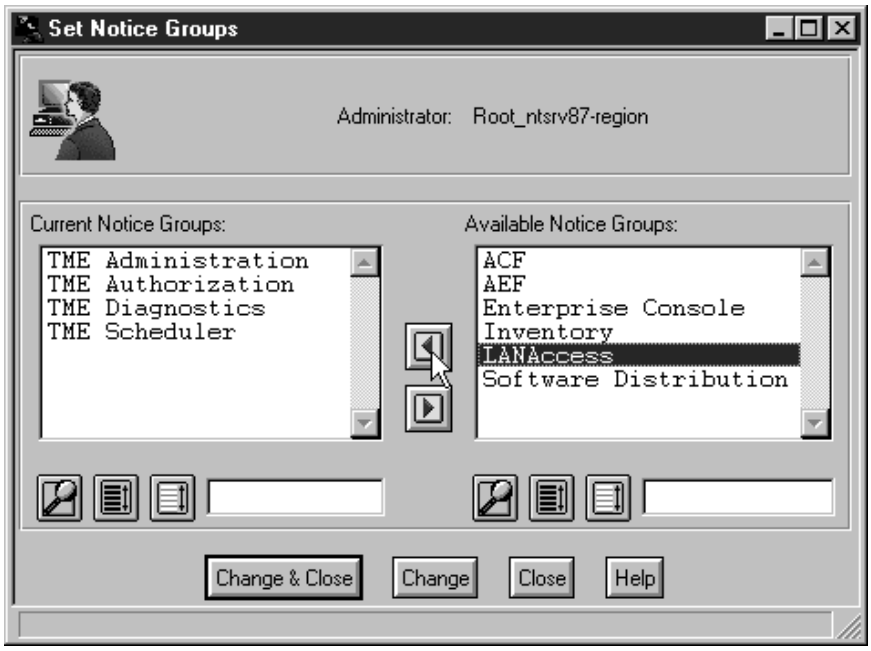


Figure 18. Set Notice Groups Window

Select **LANAccess** from the Available Notice Groups list and move it to the Current Notice Groups list by clicking on the arrow pointing left.

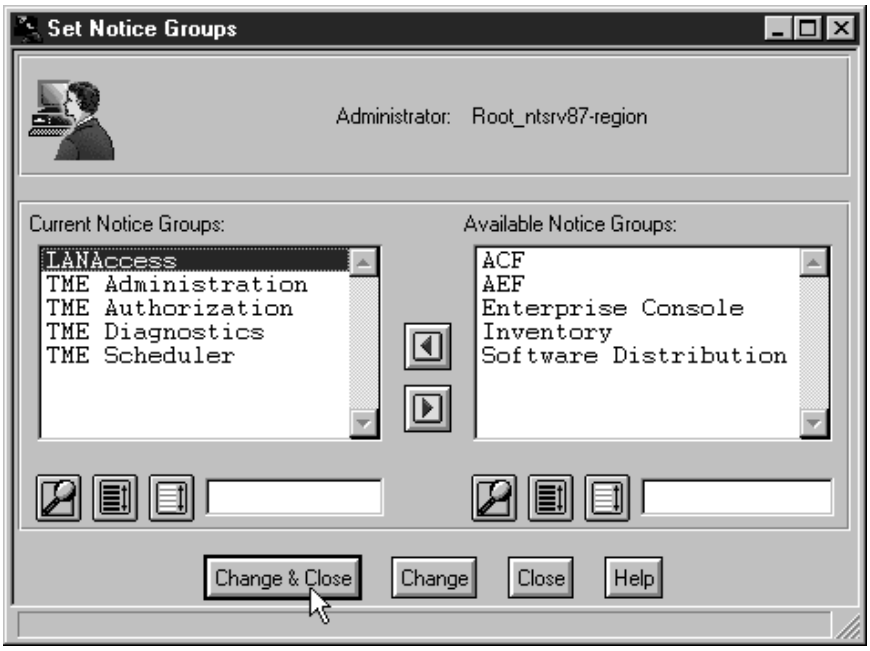


Figure 19. Set Notice Group Window

Click on **Change & Close**. If you open the Notices board now, you should see the LANAccess notice group listed. When we start working with LAN Access, information gets logged in this notice group. We show some examples of LAN Access notices later in the chapter.

Figure 20. Read Notices Window

1.5.1.2 Configuring the Policy Region

LAN Access adds an object called LANAccessSite to the desktop which can be treated as any other Tivoli managed resource. To work with these objects you have to do the following modifications in the policy region where you are planning to create LAN Access objects.

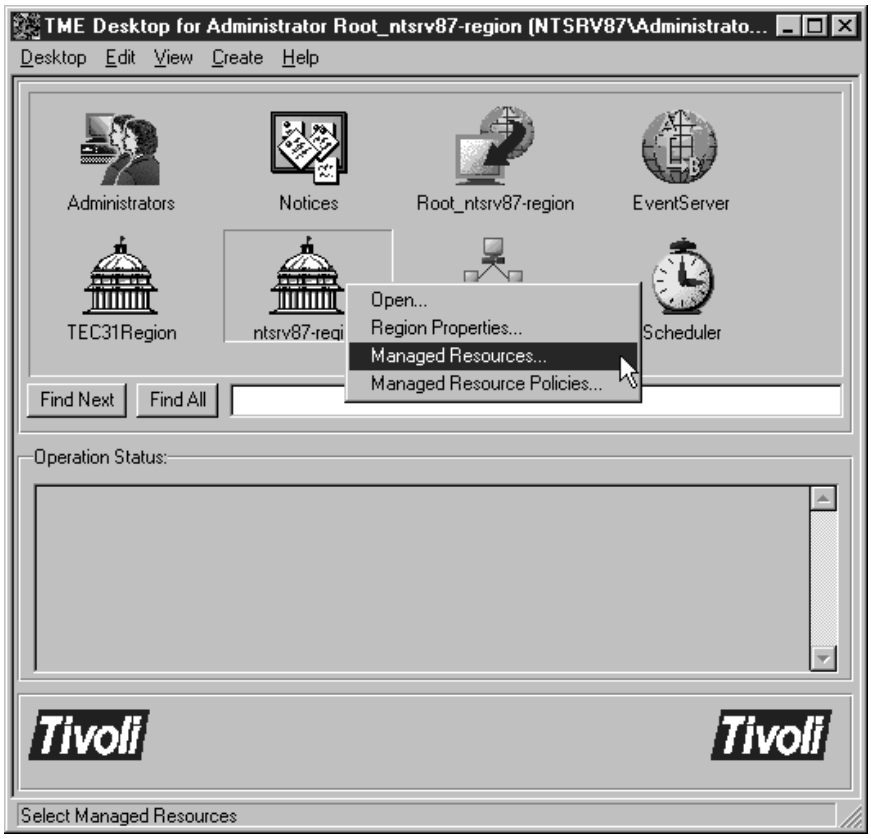


Figure 21. Adding LANAccessSite Object to the Policy Region

To add the LANAccessSite object to the policy region start by selecting **Managed Resources...** from the Context menu of the policy region.

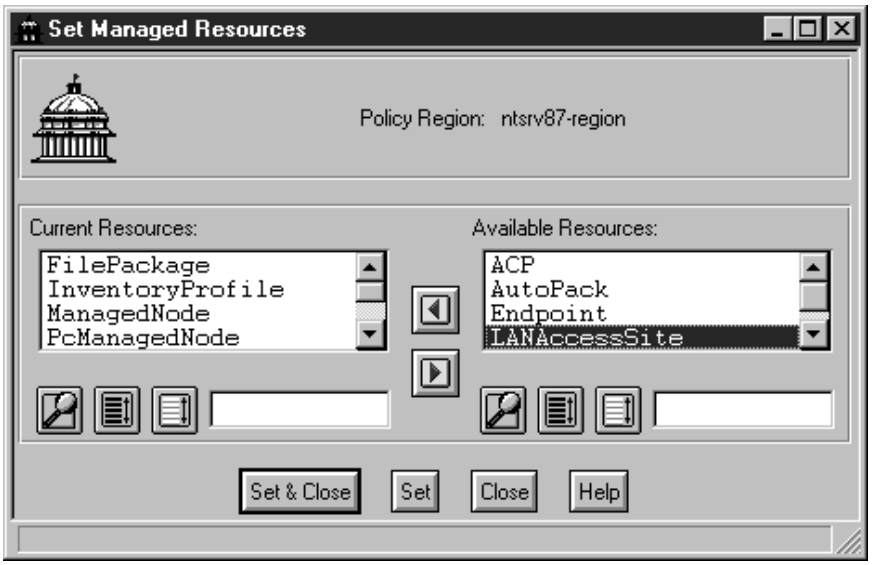


Figure 22. Setting LANAccessSite As a Managed Resource for the Region

Highlight **LANAccessSite** from the Available Resources scroll list and click on the arrow pointing left to move it to the Current Resources scroll list. Make sure the ManagedNode resource is also included in the Current Resources list.

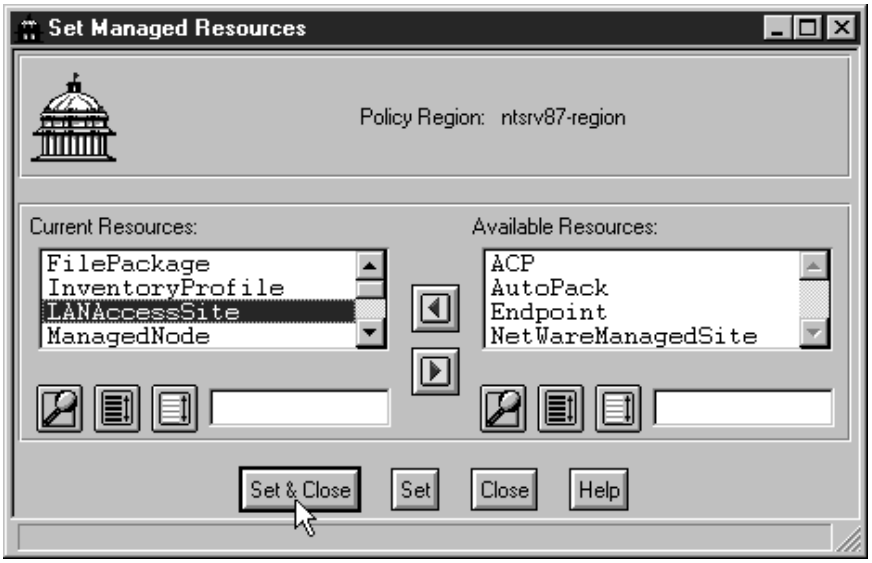


Figure 23. Setting LANAccessSite As a Managed Resource for the Region

Click on **Set & Close**.

You should see the change you have just made described in the Operation Status part of the desktop in the following window:

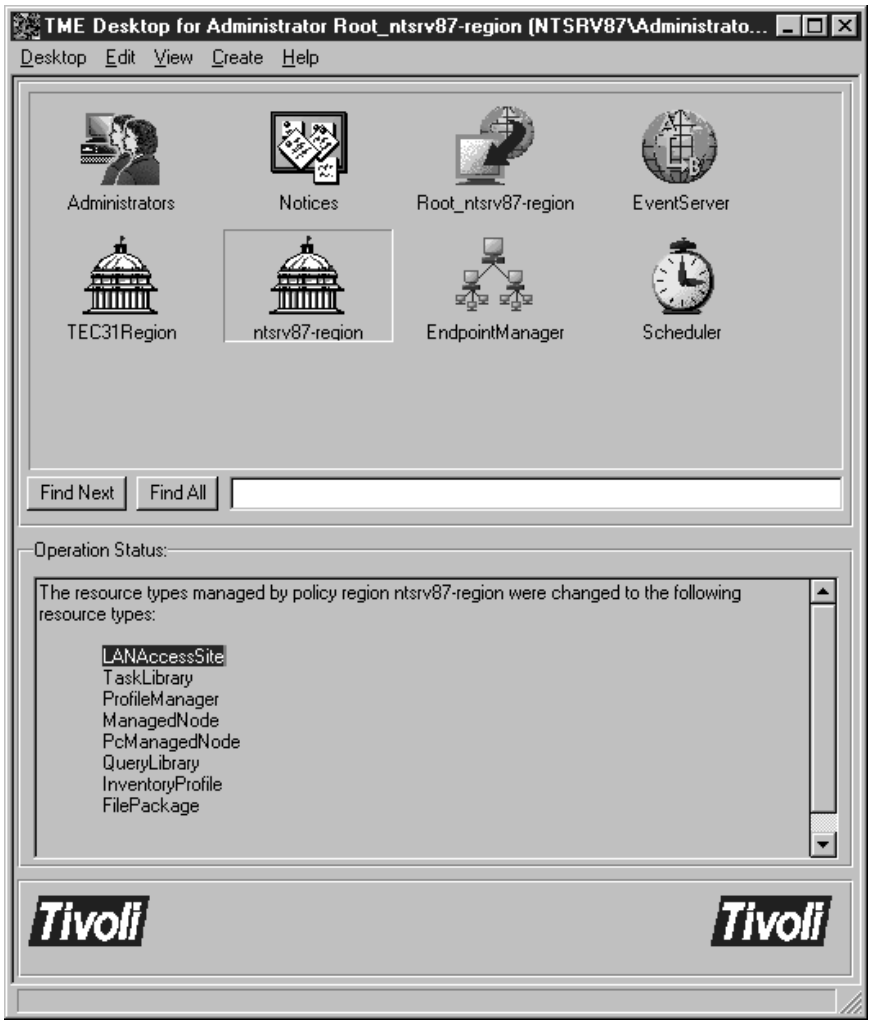


Figure 24. Tivoli Desktop

Now you should check the managed resource policies for the managed resource LANAccessSite. Select **Managed Resources Policies...** from the Context menu of the policy region icon.

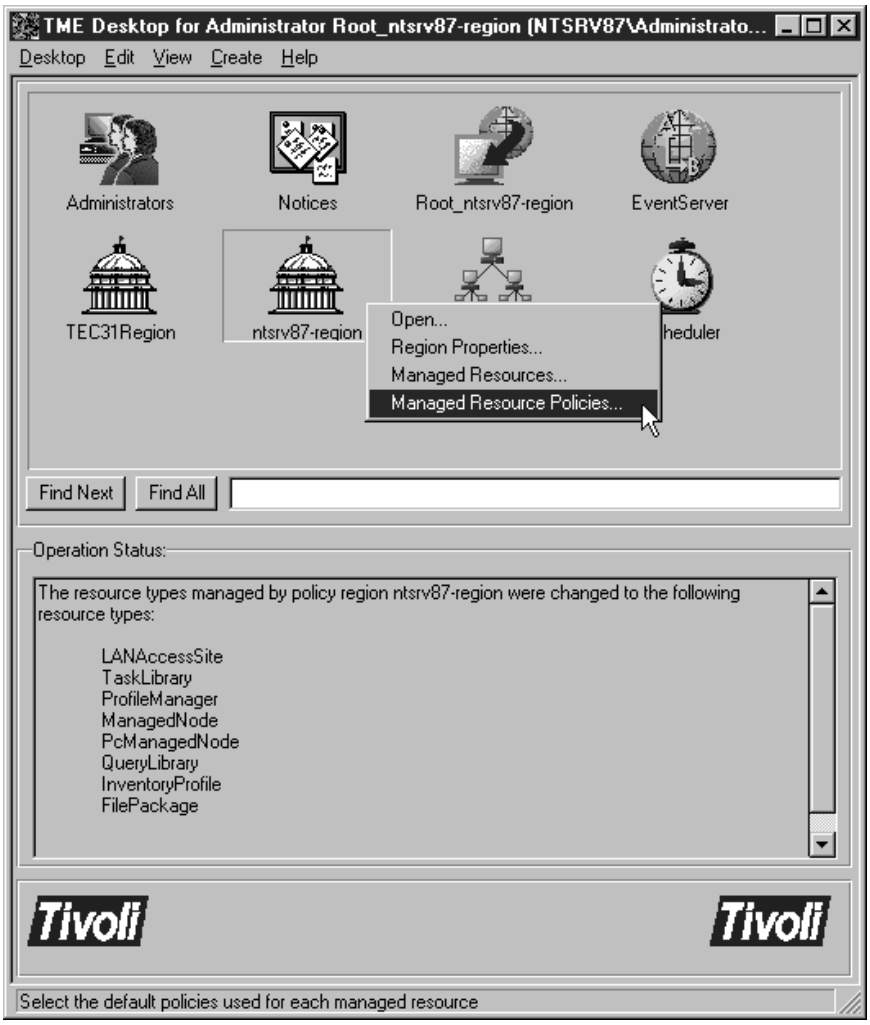


Figure 25. Editing LANAccessSite Policies

Highlight **LANAcccessSite** in the Managed Resources scroll list and set both the Default Policy and Validation Policy fields to BasicLANAccessSite as shown in the figure. Make sure the Validation Enabled box is checked as shown in the following window:

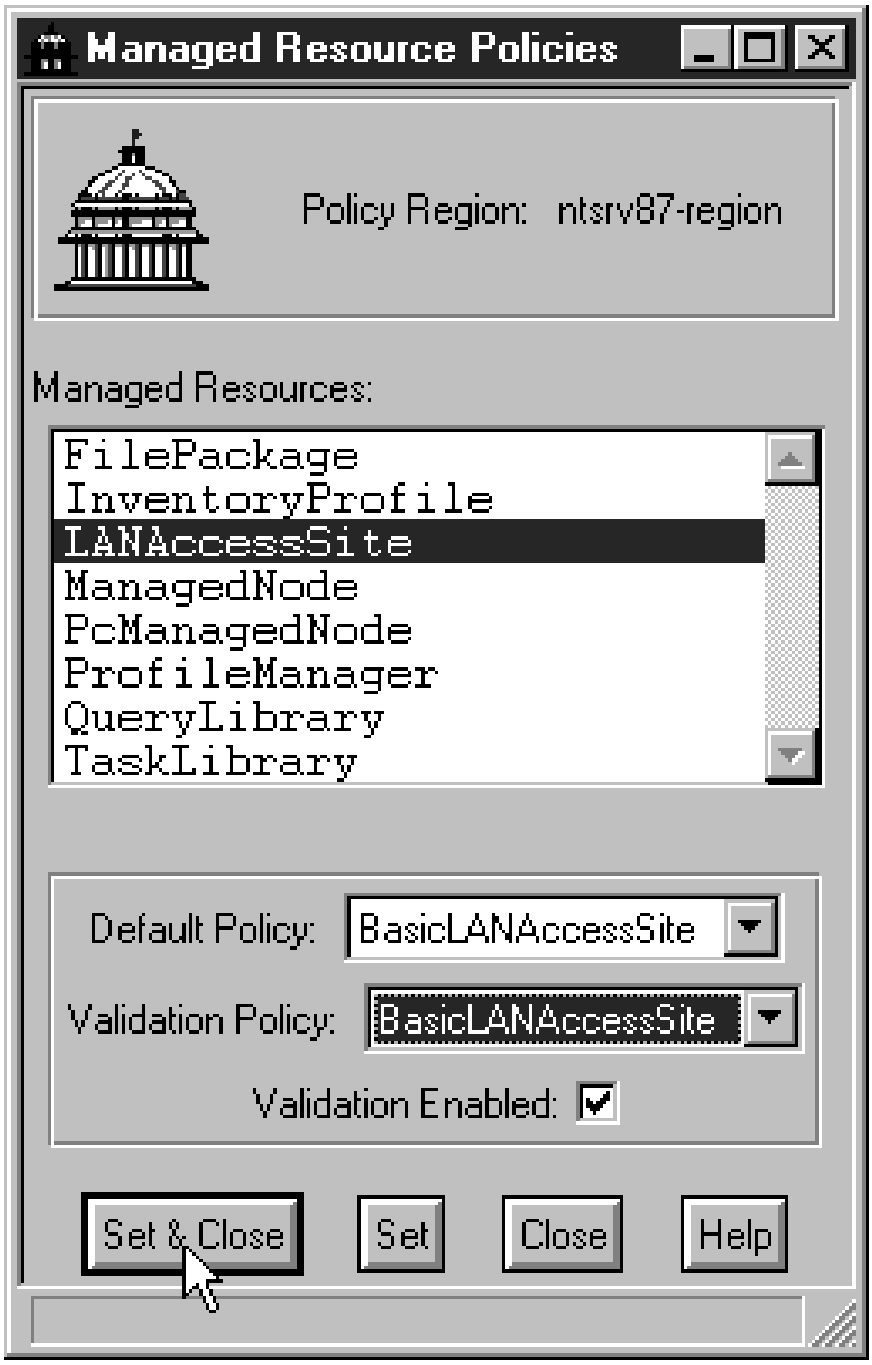


Figure 26. Managed Resource Policies Window

Clicking on **Set & Close** brings you back to the Tivoli desktop and you can see the changes you just made. They are described in the Operation Status part of the following window:

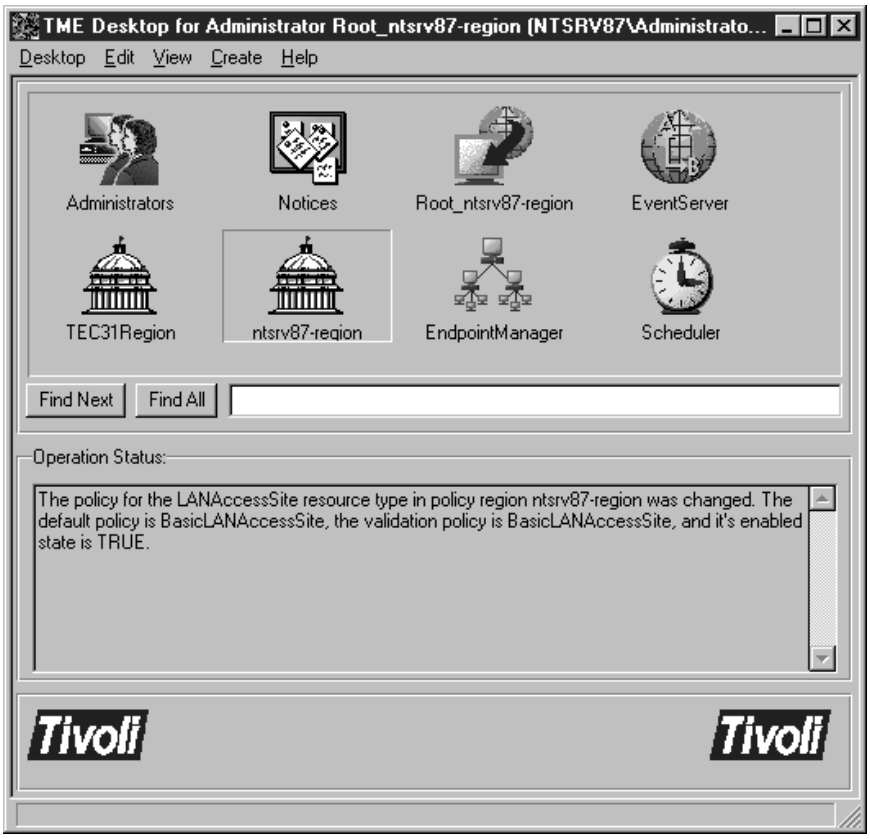


Figure 27. Tivoli Desktop

Note: The Tivoli administrator must have install_client authority in the region where LAN Access objects will be created.

You can list all the information about a Tivoli administrator using the wgetadmin command. You can also check it from the Tivoli desktop. Choose **Edit Resource Roles...** from the administrator's Context menu.

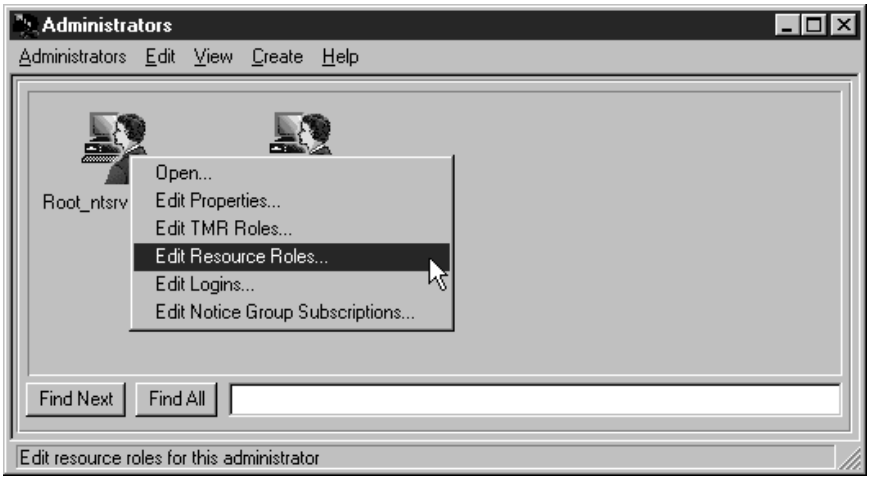


Figure 28. Editing Resource Roles for the Root Administrator

Highlight the region where LAN Access objects will be created and verify that the install_client role is included in the Current Roles list. Include it if it is not already set up. Remember to restart the desktop after you modify the roles.

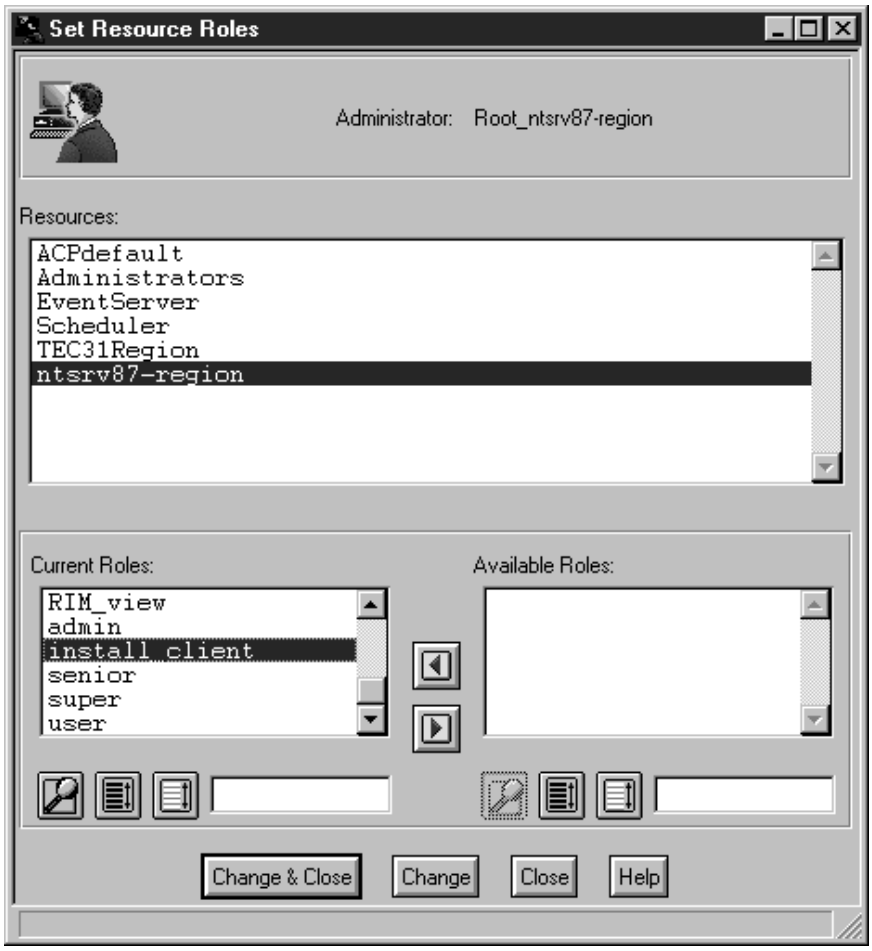


Figure 29. Setting Resource Roles

1.6 Creating LAN Access Objects in TME

This section describes Tivoli LAN Access integration with the Tivoli Framework. We are going to show how to create LAN Access objects. We also see how LAN Access discovers all LAN managing stations and managing nodes as well as creates objects for them on the Tivoli desktop. This is to enable the Tivoli Framework to administer LAN clients.

Three types of LAN Access objects can be created on the TME Desktop:

1. LAN Access Site Object

   A LAN Access site object defines the LAN managing stations where MPM providers are installed. You must create a LAN Access object in a TME policy region as the first step in accessing LAN clients.

   You can create a LAN Access site object for all LAN managing stations configured with MPM providers and you can create multiple LAN Access site objects for a single LAN managing station. How you define LAN Access site objects depends on how you want to represent LAN clients to the Tivoli Framework.

   When the LAN Access site object is created:

- All MPM providers that you identify query their respective LAN management applications for topological data on LAN clients. The data that is returned is then cached on the LAN Access managed node.
- If the LAN Access event adapter is installed and configured, the adapter begins monitoring for alerts from targeted LAN locations. Alerts that are received are routed to the TME event console.

2. LAN Access Collection Object

   A LAN Access collection object represents a filtered group of LAN clients within a LAN Access site object. A LAN Access collection is created using a standard set of selectable filters as shown in Figure 41 on page 34. A LAN Access collection object must be created in a LAN Access site object.

   You can create multiple LAN Access collection objects within a single LAN Access site object. A LAN Access collection object can not be moved outside of a LAN Access site object.

   When a LAN Access collection object is created, the information cached on the LAN Access managed node is used to determine which LAN clients meet the filtering criteria. For each client that meets at least one of the specified filtering criteria, a LAN Access node object is created.

3. LAN Access Node Object

   The LAN Access node object represents a single LAN client. A LAN Access node object cannot be moved outside of a LAN Access collection object, but the same LAN Access node object can exist in multiple LAN Access collection objects.

   When the LAN Access node is created, you can view the data collected for that object.

1.6.1 Creating a LAN Access Site

Before you start creating objects, make sure you have installed and configured your environment correctly, as described in the previous sections of this chapter.

Note: We used SMS for our provider for the following examples but we could have also used Netfinity or Intel LANDesk.

Select **Create -> LANAccessSite...** from the policy region where you want to create the object.

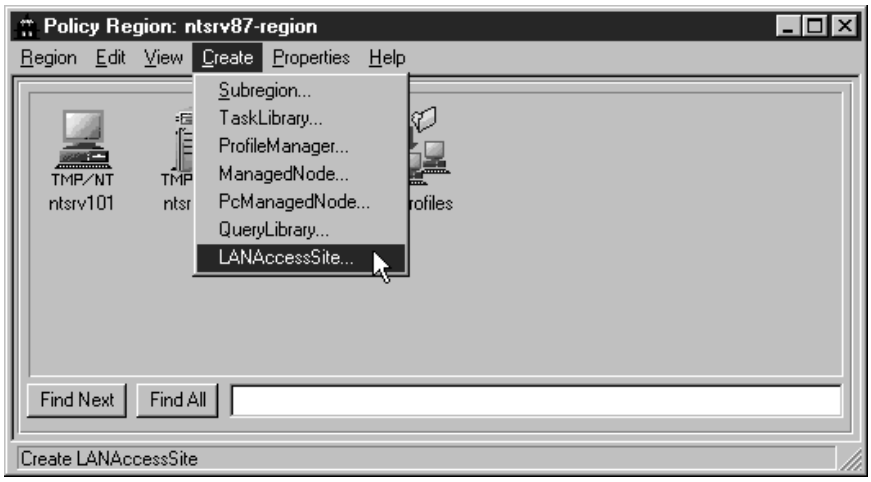


Figure 30. Creating a LAN Access Site Object

Fill in the fields shown in the following figure.

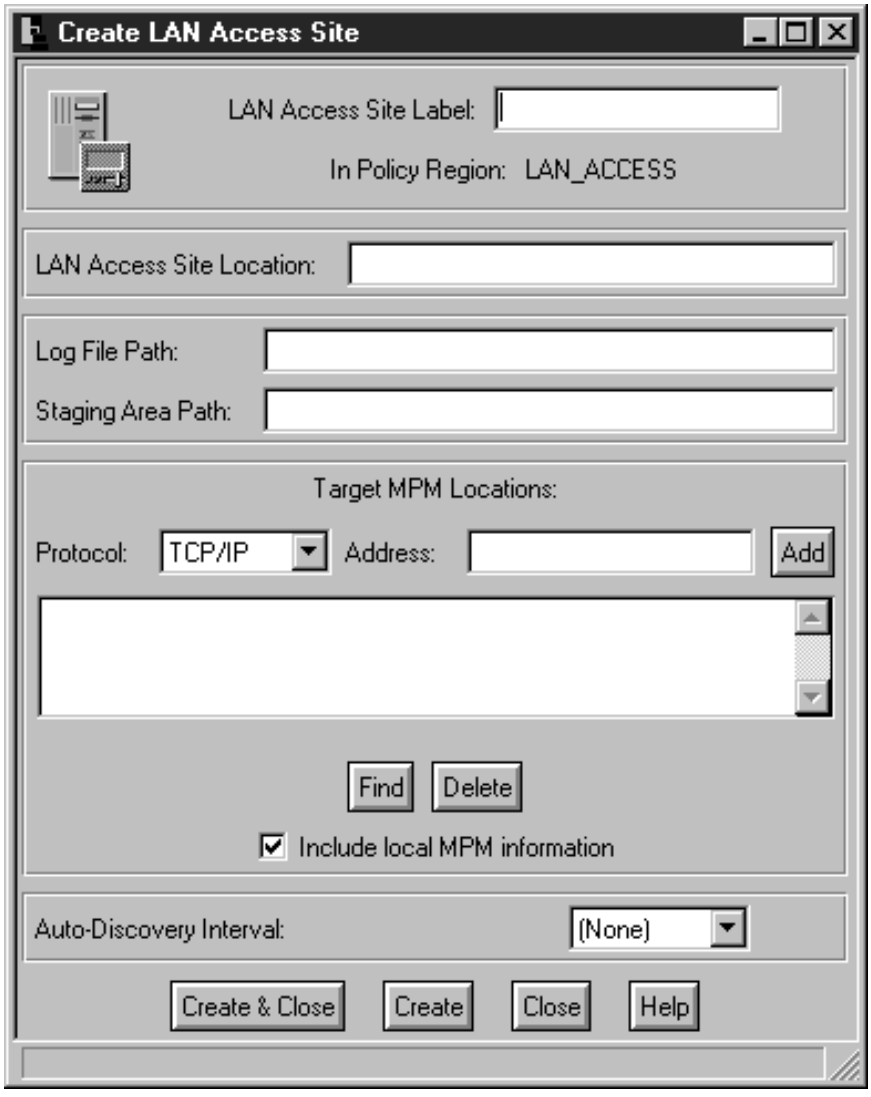


Figure 31. LAN Access Site Creation Window

We are going to outline some important considerations that you should take into account when filling the fields in Figure 31. You can find a complete description of each field selecting the **Help** button in this window.

- LAN Access Site Label

  Enter a unique name within the Tivoli management region and be aware that you will not be able change this name after the object is created.

- LAN Access Site Location

  Enter the name of your LAN Access managed node. This field is case-sensitive.

  The next two fields are optional but we recommend that you specify them as well. The path entered here must already be created in the LAN Access managed node that you specified in the field LAN Access Site Location.

- Log File Path

  Here you must specify a file name as well as the path where it will be created. There is some overhead involved in logging. Following is an extract from one of our logs:

```
11:36:25 1998 : Initializing remote MPM broker (rc = 0)
11:36:25 1998 : MPM_GET_KNOWN_SUBSYSTEMS
11:36:25 1998 :  rc = 0:
11:36:25 1998 :  mpm_CommandBlock = 146794:
11:36:25 1998 :   returnCode = 0
11:36:25 1998 :   headerLen = 44
11:36:25 1998 :   overallLen = 458
11:36:25 1998 :  mpm_GetKnownSubSystems* = 1467c0:
11:36:25 1998 :   numProviders = 1
11:36:25 1998 :  mpm_KnownProviders* = 1467d4:
11:36:25 1998 :   nextRecordOffset = 0
11:36:25 1998 :   provMajorVersion = 1
11:36:25 1998 :   provMinorVersion = 0
11:36:25 1998 :   vendorID = 1
11:36:25 1998 :   copyright string offset = 100
11:36:25 1998 :   vendor string offset = 176
11:36:25 1998 :   home directory string offset = 0
11:36:25 1998 :   product string offset = 242
11:36:25 1998 :   numSubSystems = 2
11:36:25 1998 : Done.
11:36:25 1998 : MSB_93: Sending SVCMGR_START_SVC command,
          destination = NETBIOS::NTSRV48::SvcMgr
11:36:27 1998 : Initializing remote MPM broker (rc = 0)
11:36:27 1998 : MSB_93: SendSync: Sending mpm request, subsystemID = 0, commandID = 0, destination =
NETBIOS::NTSRV48::MSB_Client
11:36:32 1998 : MPM_GET_KNOWN_SUBSYSTEMS
NETBIOS::NTSRV48::MSB_Client
23:10:21 1998 : MPM_DISC_GET_SYSTEMS_BY_GROUP
23:10:21 1998 :  rc = 0:
23:10:21 1998 :  mpm_CommandBlock = 23f1858:
23:10:21 1998 :   returnCode = 0
23:10:21 1998 :   headerLen = 44
23:10:21 1998 :   overallLen = 1032
23:10:21 1998 : MSB_F5: Sending SVCMGR_STOP_SVC command,
          destination = NETBIOS::NTSRV48::SvcMgr
23:10:21 1998 : Done.
23:10:23 1998 : Querying cache
23:10:23 1998 : Providers found = 1
23:10:23 1998 : Systems found = 2
23:10:23 1998 : Provider = MPM Provider For Microsoft SMS
23:10:23 1998 : Node = NETBIOS::NTSRV48::2::3::NTSRV99
23:10:23 1998 : Attribute count = 15
23:10:23 1998 :  0000::MPM Provider For Microsoft SMS
23:10:23 1998 :  0001::S00|SMSDOM|NTSRV99
```

Figure 32. LANAccess Log File

- Staging Area Path

Here you specify a temporary directory where a TME 10 file package created for SMS clients will be put while the connection between the LAN Access managed node and the LAN client is established.

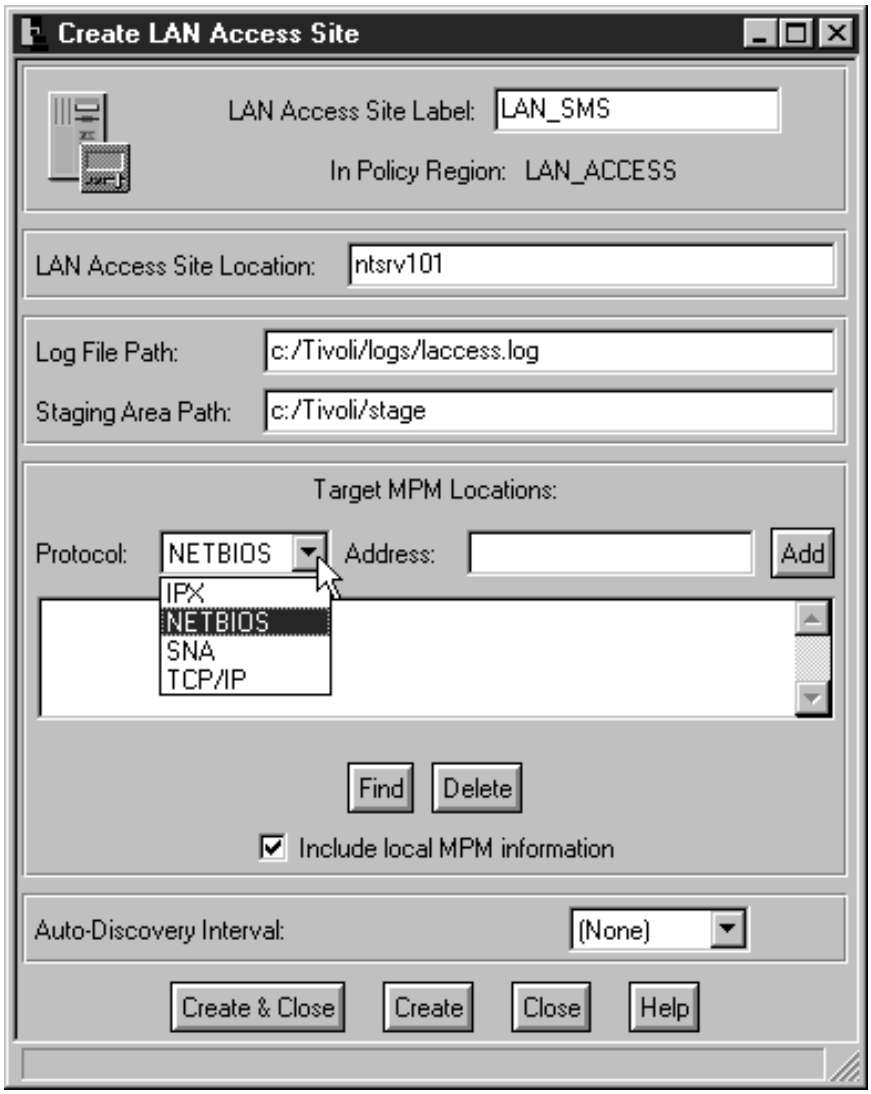


Figure 33. LAN Access Site Creation Window

- Target MPM Locations

  You have two options. You can enter your SMS provider nodes manually or you can click on **Find** to make the system automatically discover them for you.

  To enter the MPM provider nodes manually, you must select the protocol that you want to use to communicate between your LAN Access managed node and your LAN managing station. You select the protocol by clicking on the arrow key in the Protocol field and then you enter the qualified address for the corresponding protocol in the Address field. Click on **Add** to include the MPM provider in the Target MPM Locations scroll list box.

  To let the system look for the MPM providers in your network automatically, click on **Find**.

  While the automatic discovery of the MPM systems is going on, you will see the following panel in your screen.

Figure 34. Searching for MPM Systems

When the discovery of MPM systems ends, you will see several entries in the Target MPM Locations scroll list box. Remove the entries that you will not be using. To remove an entry, highlight it and then click on **Delete**. Only the entry for your LAN managed node should remain. You can have more than one entry for the same system depending on the protocols that you enabled for communication in the Network Driver Configuration panel.

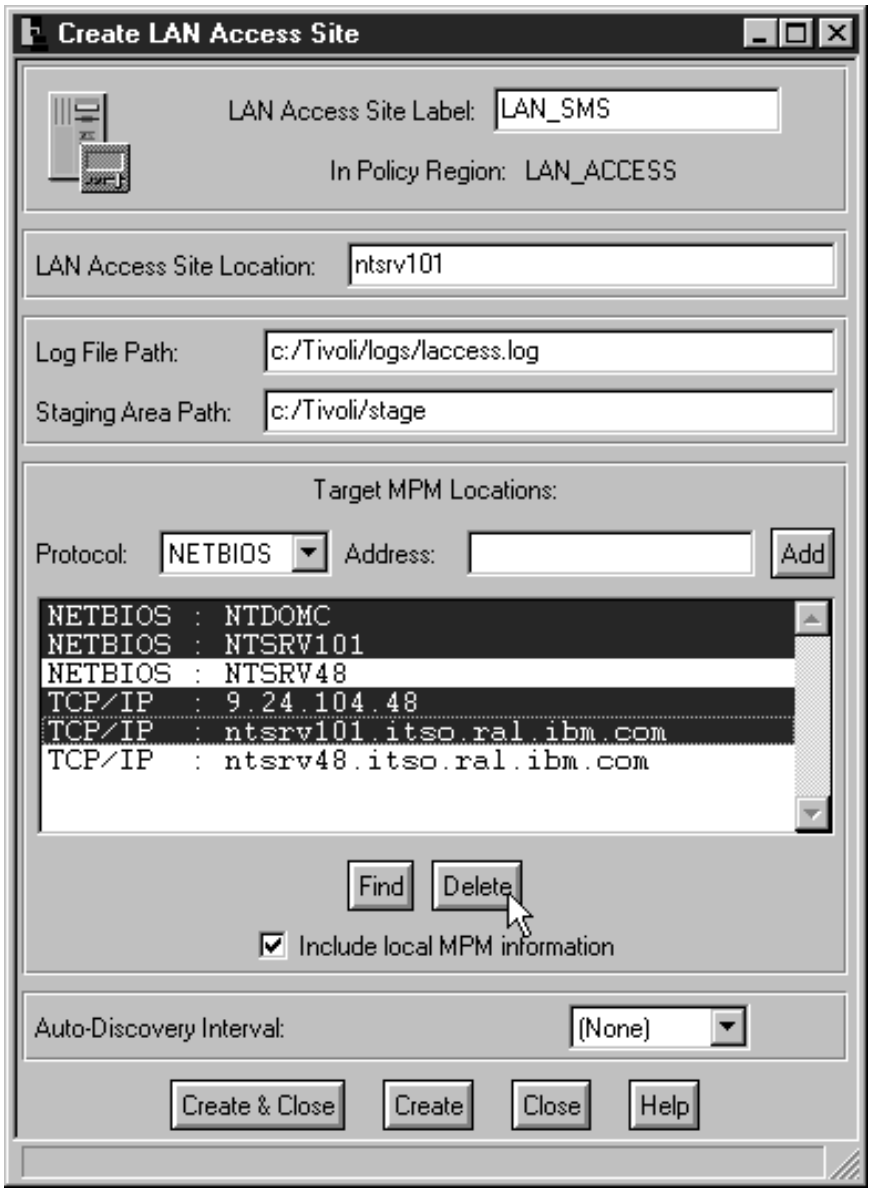


Figure 35. LAN Access Site Creation Window

Other fields to update include:

- Include Local MPM Information

  Clicking on this check box tells LAN Access to query the NT managed node for MPM providers during the creation of the LAN Access site object. It is checked by default. Uncheck this box if the managed node and the LAN managing station are the same system.

- Auto-Discovery Interval

  This field allows you to choose an interval to automatically update this LAN Access site if you make any modifications in your LAN systems. Selecting an interval schedules a job using the Tivoli Scheduler.

  As can be seen in Figure 36 on page 31 we set this interval to 30 minutes. We will show the job scheduled as a result, in 1.7, “Scheduler” on page 60.

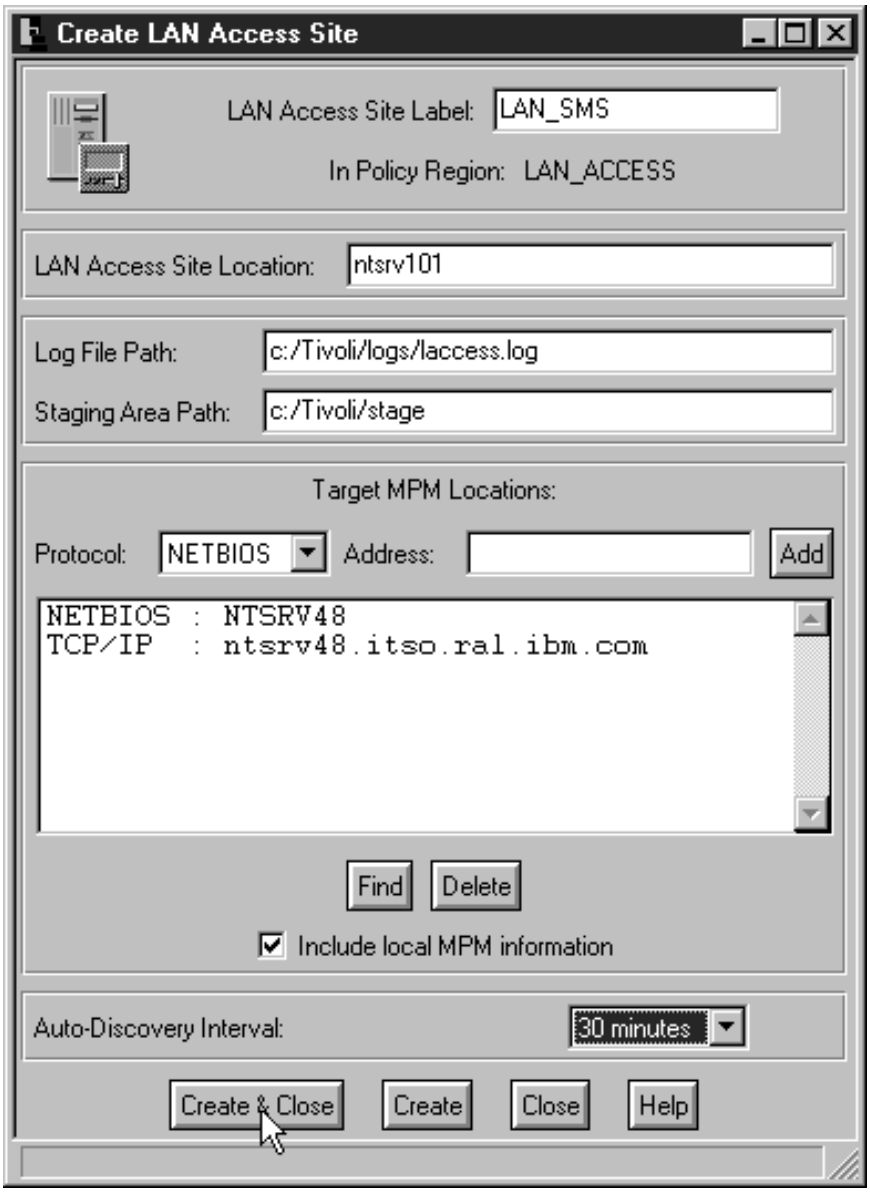


Figure 36. LAN Access Site Creation Window

Click on **Create & Close** for the system to start the discovery of all clients managed by the MPM providers. During the discovery process you will see the following screen.

Figure 37. Discovering Systems

If some of the MPM providers are password protected, you must enter the user ID and password to be able to establish the communication. For more details on security and passwords see 3.2, “Installing on Windows NT” on page 132.

Figure 38. Enter User ID and Password

Then the search will continue until it is done. When the discovery ends, you will see the icon representing the LAN Access Site next to other managed resources for that policy region.

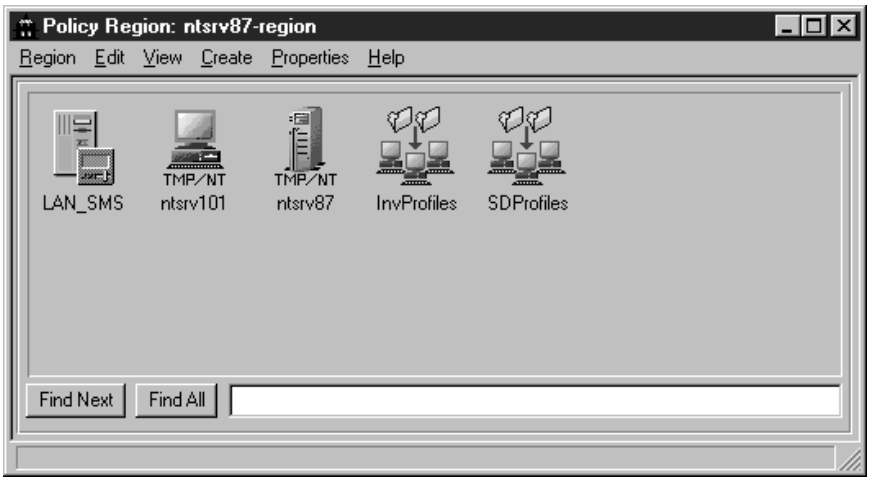


Figure 39. Inside the Policy Region

1.6.2 Creating a LAN Access Collection

Open the LAN Access site icon by double-clicking on it.

Select **Create -> LANAccessCollection...** from the LAN Access site Create menu.

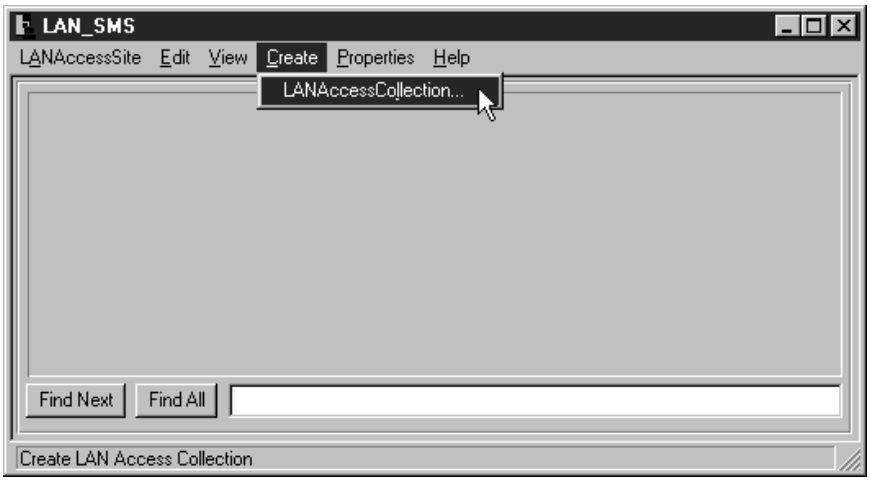


Figure 40. Creating a LAN Access Collection Object

The only required field for the creation of a LAN Access collection is the LAN Access Collection Label field.

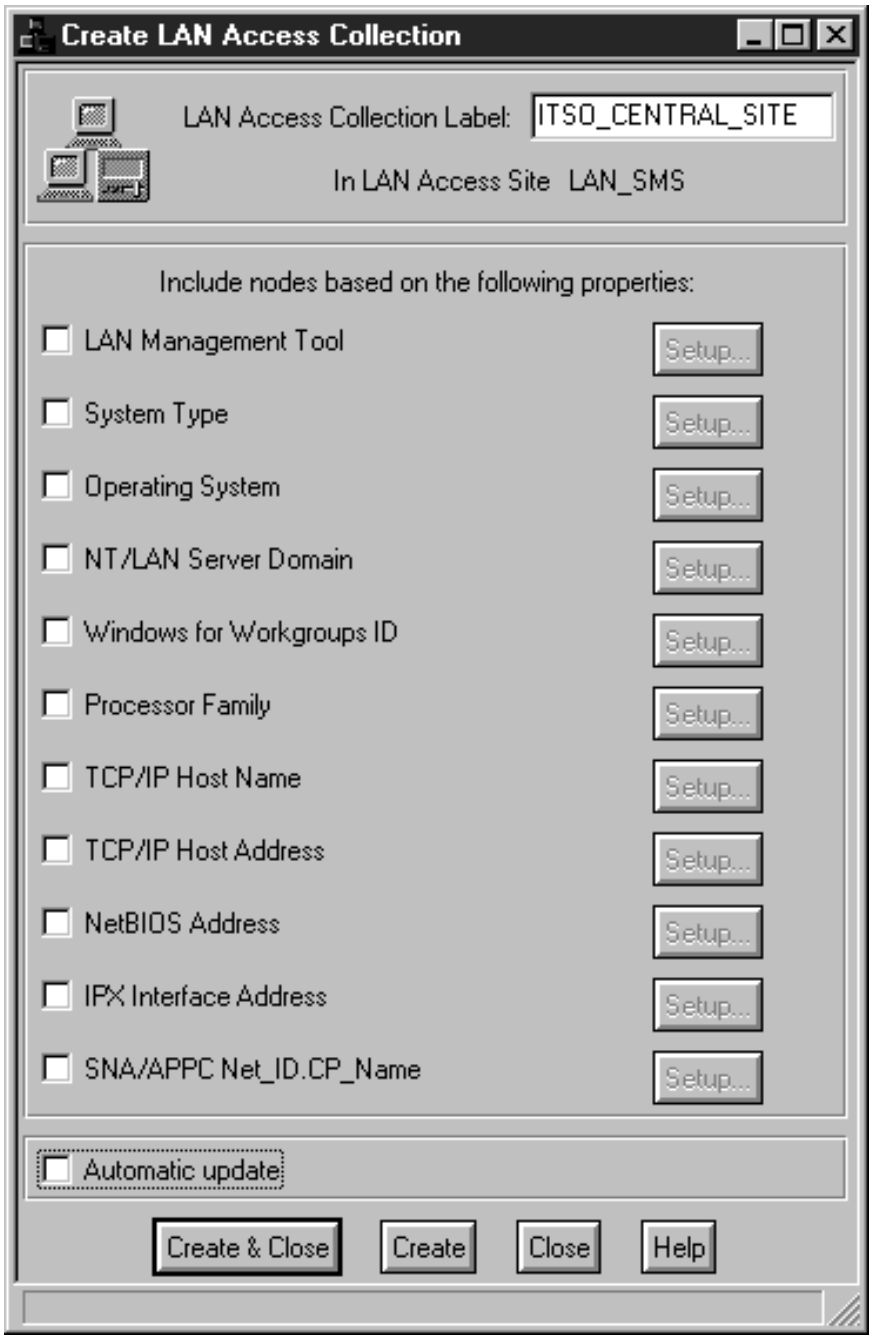


Figure 41. Creation of LAN Access Collection

The following figures show all the filtering categories available that you can use to restrict specific LAN clients to the collection. The filters are exclusive, which means that only the systems that match all the filtering selections will be included in the collection. Selecting filters is optional. If you do not select any filter, then the collection will contain all the systems discovered in your LAN during the creation of the LAN Access site.

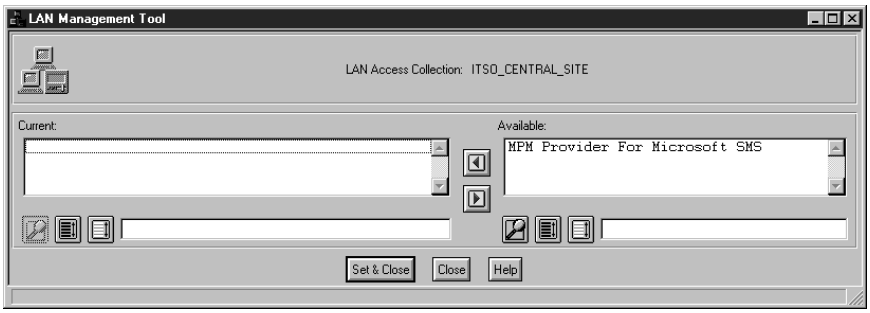


Figure 42. Choose LAN Management Tool

- LAN Management Tool

  This filter groups the clients that are being managed by the same LAN management application and the dialog lists the available MPM providers installed.

  Since we only had the SMS provider on this system that is all that showed up. If we had one of the others installed, it would be in the Available list.

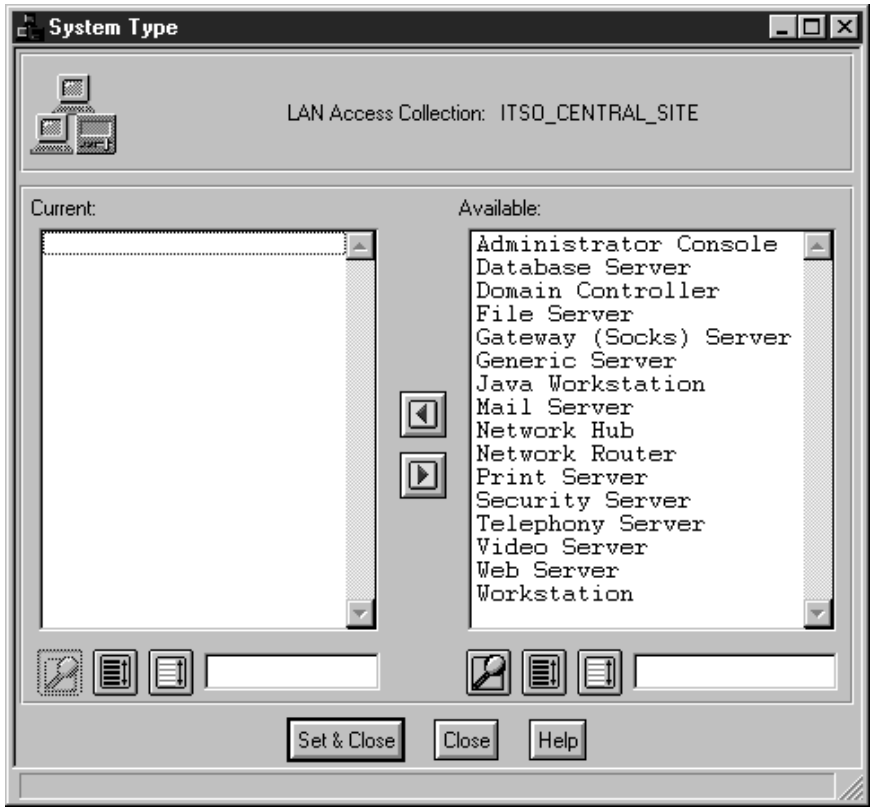


Figure 43. Choose System Type

- System Type

  This filter groups LAN clients depending on their function. The Available scroll list shows all the possible types of clients and not only the ones in your LAN.

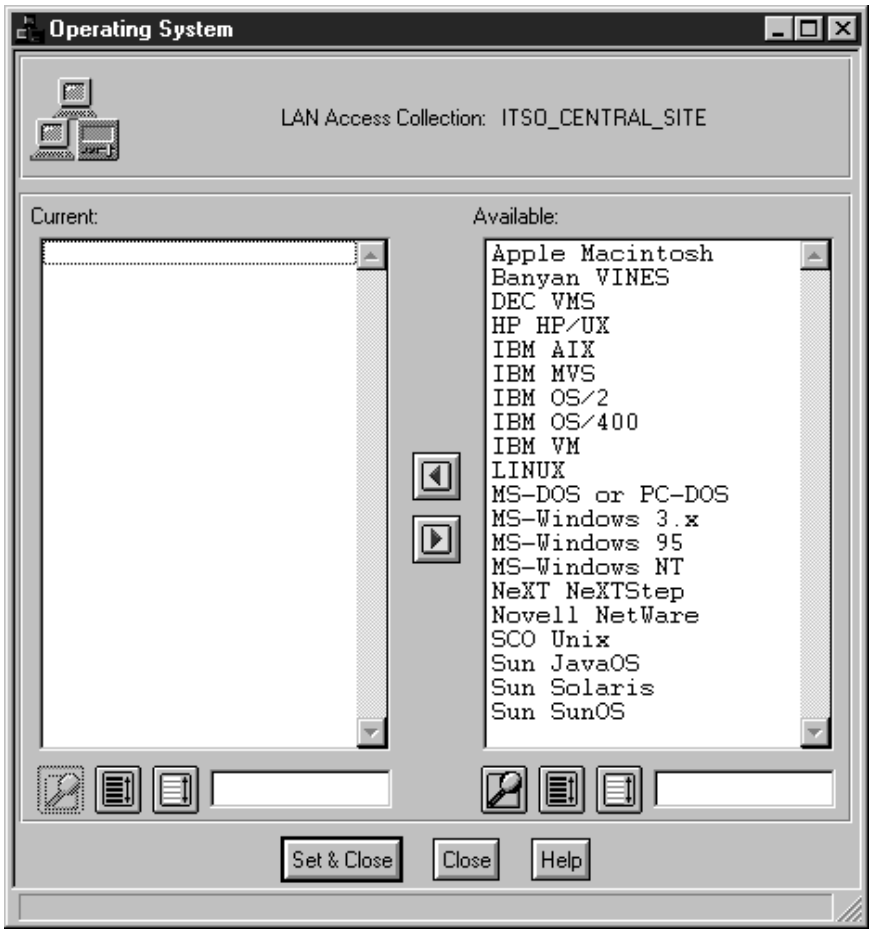


Figure 44. Choose Operating System

- Operating System

  This filter groups LAN clients by operating system. The Available scroll list shows all the possible operating systems that LAN Access can detect.

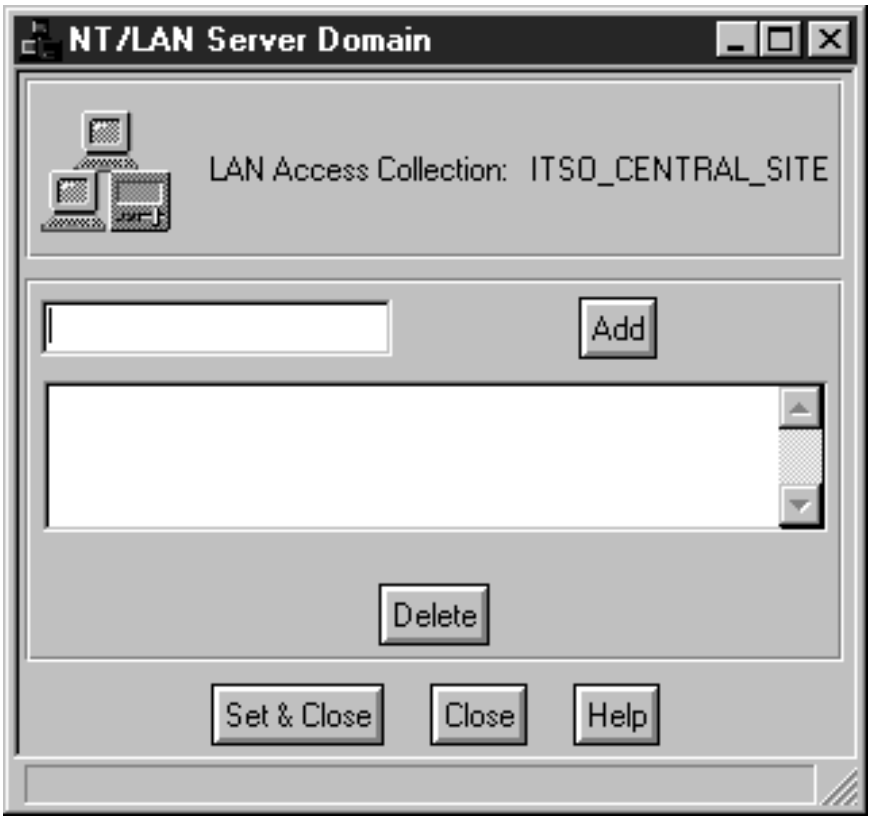


Figure 45. Choose NT/LAN Server Domain

- NT/LAN Server Domain

  This filter groups LAN clients that belong to the same LAN domain.

- Windows for Workgroups ID

  This filter groups windows clients that belong to the same workgroup.

- Processor Family

  This filter groups LAN clients by their processor. The available scroll list contains all the processors that LAN Access can detect.

- TCP/IP Host Name

  This filter enables you to select individual LAN clients specifying the IP host name.

- TCP/IP Host Address

  This filter enables you to select individual LAN clients by specifying the IP address.

- NetBIOS Address

  This filter enables you to select individual LAN clients specifying the NetBIOS address.

- IPX Interface Address

  This filter enables you to select individual LAN clients specifying an IPX address.

- SNA/APPC Net_ID.CP_Name

This filter enables you to select individual LAN clients specifying the SNA address.

- Automatic Update check box

  If you check the Automatic Update check box in Figure 41 on page 34 the LAN Access collection will be automatically updated when the LAN Access site is updated.

When you click on **Create & Close** in the Create LAN Access Collection window, the systems that match the filtering conditions chosen will be put inside this collection. While LAN Access is selecting the appropriate systems, you will see the following window. The four digit number displayed (here 0000) is used as a counter. It will vary as LAN Access finds more systems for the collection.

Figure 46. Selecting Systems

When the selection of the client systems ends, you will have an icon inside the LAN Access site representing the LAN Access collection.

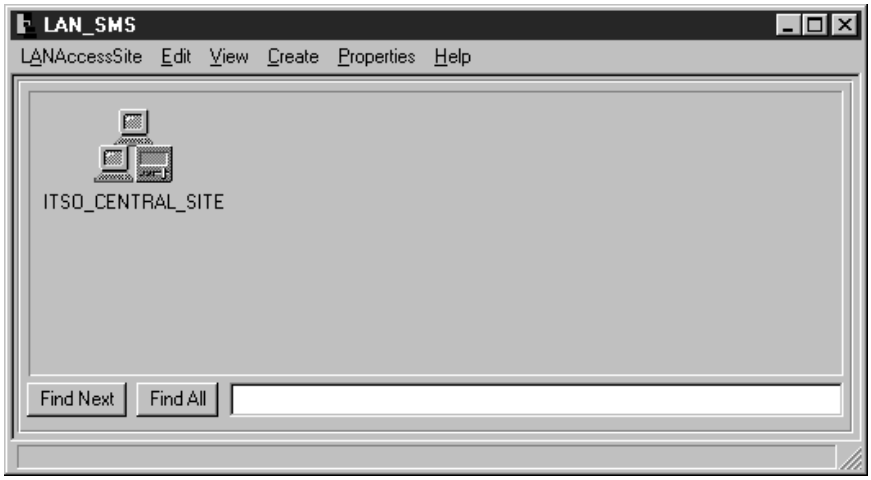


Figure 47. Inside a LAN Access Site

Double-click on the icon for the LAN Access collection to see the LAN clients that were discovered by LAN Access during the creation of the LAN Access site, and that met the filtering selections made when creating the LAN Access collection.

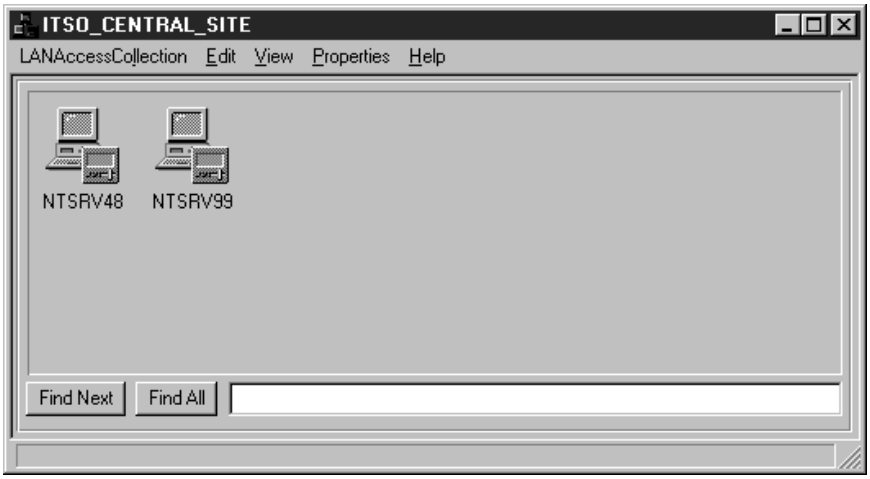


Figure 48. Inside a LAN Access Collection

1.6.3 Deleting a LAN Access Site Object

To delete one or more LAN Access site objects click on each object in the policy region window that you want to delete. Then select **Edit** and **Delete**.

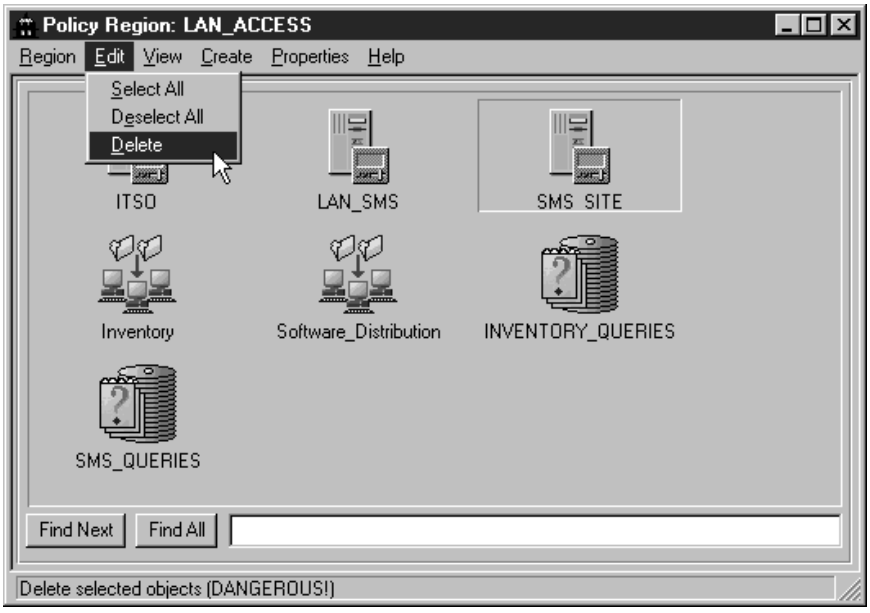


Figure 49. Delete Selected Objects

A Delete Objects? pop-up warning is displayed.

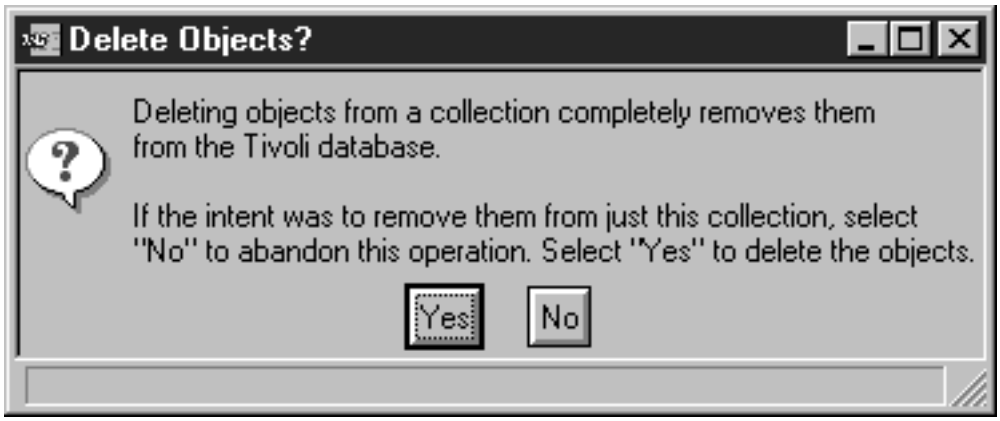


Figure 50. Confirm Deletion of Selected Objects

Make sure you have selected the correct LAN Access site objects then select **Yes** to remove them.

1.6.4 Viewing and Changing LAN Access Collection Properties

To view or change the LAN Access collection objects associated with a specific LAN Access site object you have to open the LAN Access site object to display the window for LAN Access collection objects.

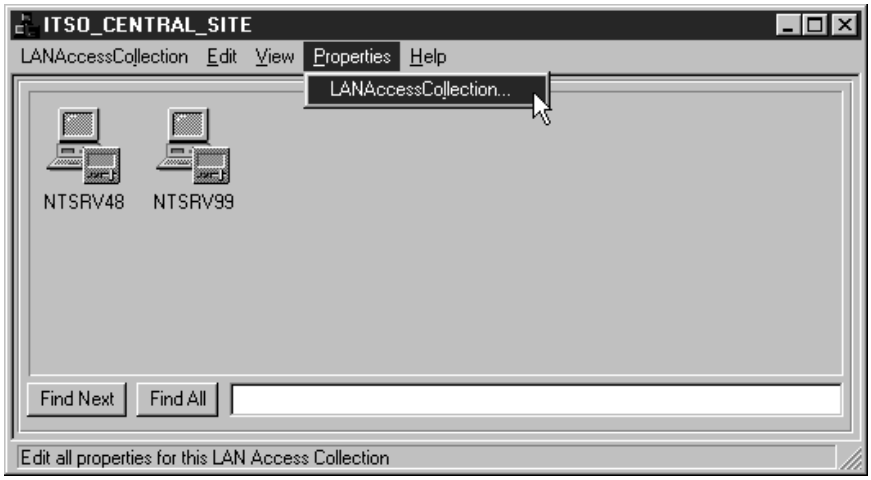


Figure 51. Changing LAN Access Collection Object

Click on the collection object that you want to change, then select **Properties** to display the dialog for the collection object.

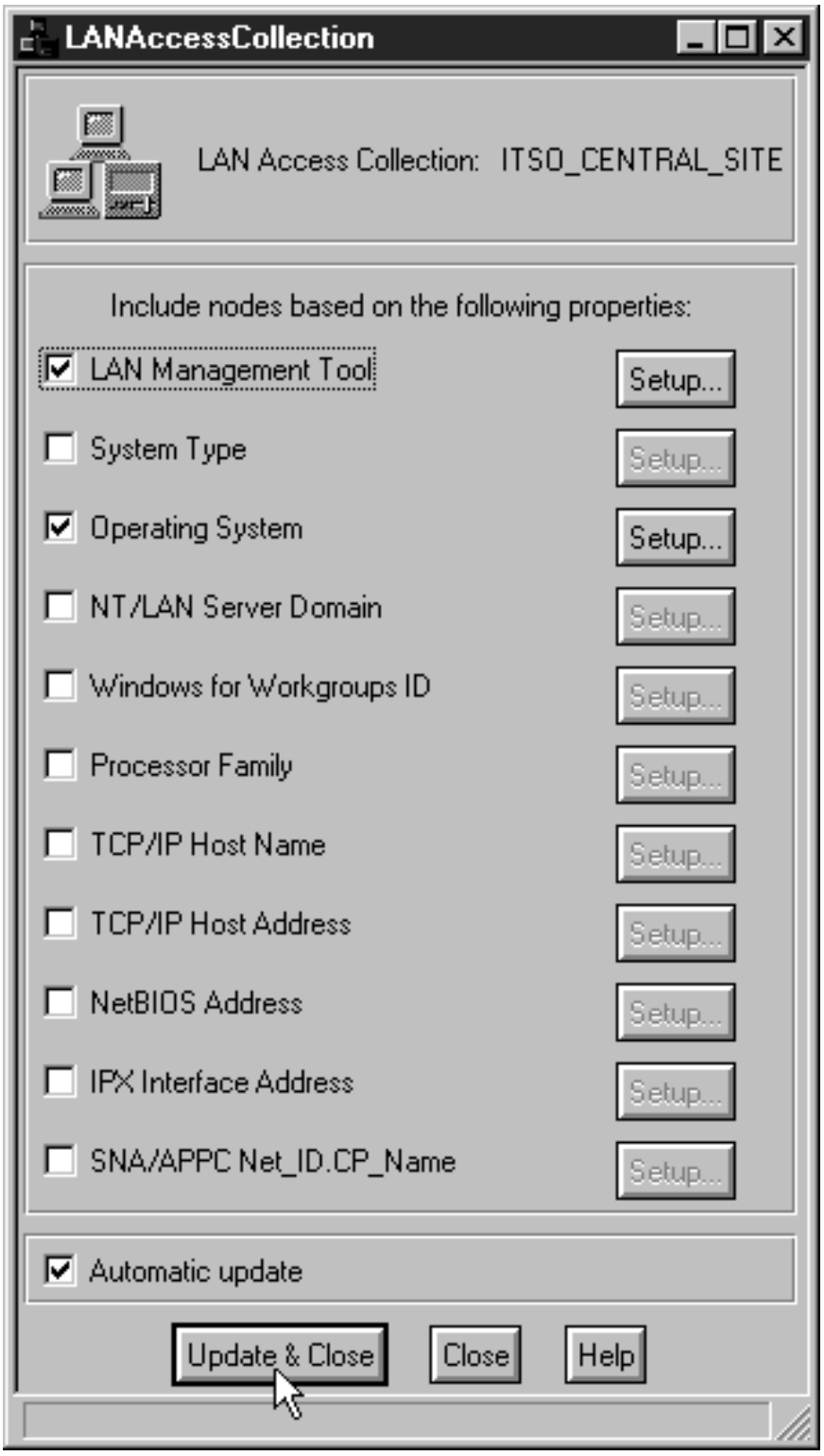


Figure 52. Changing Properties of a LAN Access Collection

Note that the label of the collection object cannot be changed. For information on each field, select the **Help** button at the bottom of the window. Make any desired changes then select **Update & Close** to update the information. To exit without making any changes, select the **Close** button.

1.6.5 Deleting a LAN Access Collection Object

To delete one or more LAN Access collection objects you have to double-click on the LAN Access site object to display the LAN Access collection objects.

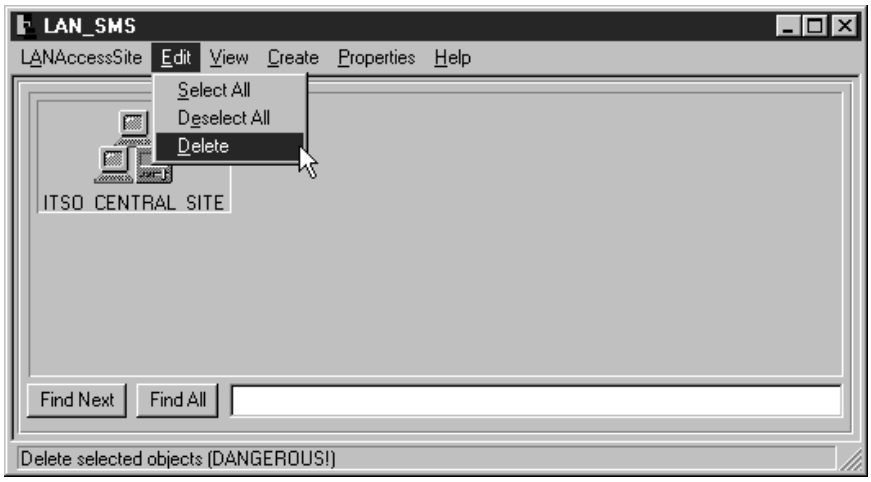


Figure 53. Select Objects to Delete

Select the collection objects you want to delete. You can use the Select All or De-select All or just select individual sites.

If you have a large number of collections, the Find Next and Find All buttons can be useful in locating one or more collection objects. If you click on **Find Next**, it locates and highlights the next label that matches the text string you entered in the data-entry field. Click on **Find All** to locate and highlight all labels that contain the text string you entered in the data-entry field. The search string you enter is not case-sensitive.

Select **Edit** and **Delete** to remove the entry.

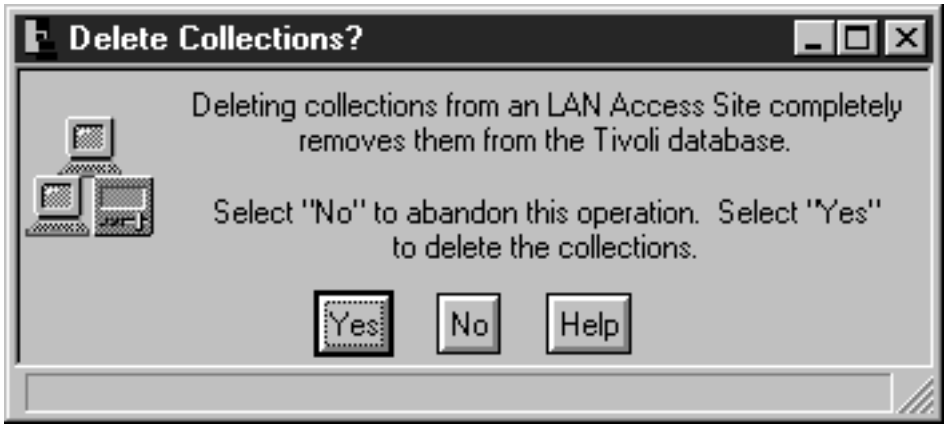


Figure 54. Confirming Deletion of Object

A Delete Objects? pop-up warning is displayed. Make sure you have selected the correct collections then click on **Yes** to finish.

1.6.6 Viewing the Properties of a LAN Access Object Node

To view the properties of a LAN Access object node you have to double-click on the LAN Access collection object to display the icons of the LAN Access object nodes in the collection.

Double-click on the node to view a list of properties collected for that node.

If you have a large number of nodes, the Find Next and Find All buttons can be useful in locating one or more object nodes. Find Next locates and highlights the next name that matches the text string you enter in the data-entry field. Find All locates and highlights all names that contain the text string you enter in the data-entry field. The search string you enter is not case-sensitive.

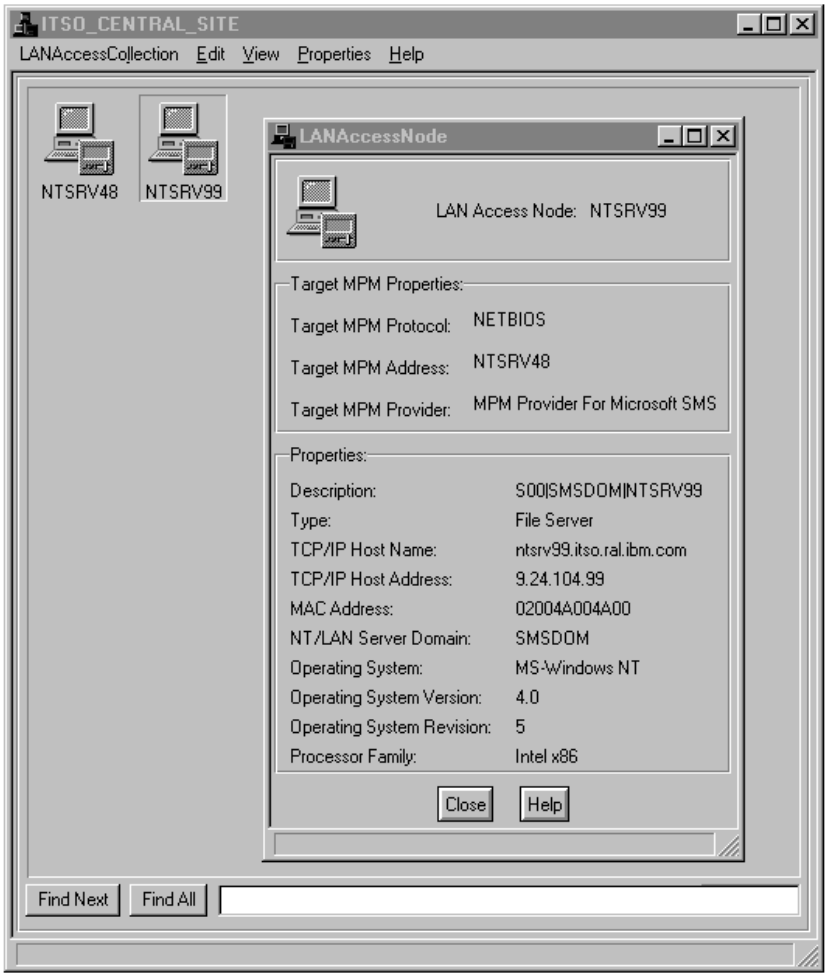


Figure 55. LAN Access Object Node - Properties

The following is a description of the properties displayed. To view these descriptions from the window, select the **Help** button at the bottom of the window:

- Target MPM Properties

  This group of properties shows the MPM provider that is used to access the LAN client.

- Target MPM Protocol

The transport used between the LAN managing stations and the NT managed node.

- Target MPM Address

  The network address or network name of the node where the MPM provider is located.

- Target MPM Provider

  The name of the MPM provider used to access this LAN client.

- Properties

  This group of properties reflects the information returned by the MPM for this node. The number and types of properties displayed in this section vary according to the information supplied by the MPM provider.

Select **Close** to finish viewing the information.

1.6.6.1 A Filtering Example

What we did here was to install a LAN Access site with only one provider feeding information in. Therefore, we select all unwanted providers from the list and delete them. Creating this LAN Access site then gives us a site in which the machine winnt100 is functioning as a provider only using the TCP/IP protocol. The following is an example of the LAN Access site before we filtered out the other protocols:

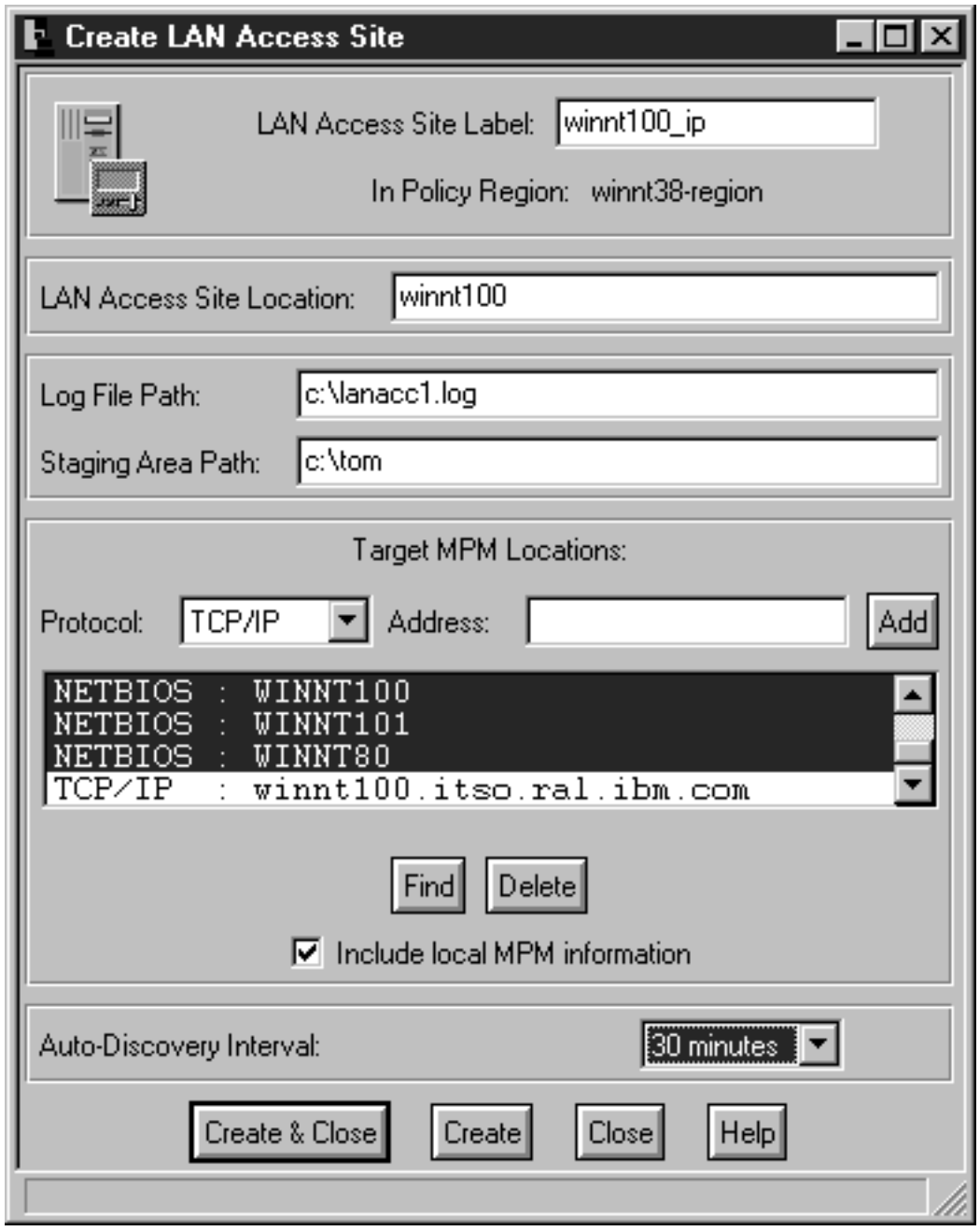


Figure 56. Create LAN Access Site - Delete Unwanted MPM Providers

We then selected all non-IP locations and deleted them. Then we prepared to set up another filter using Netfinity as the only valid provider.

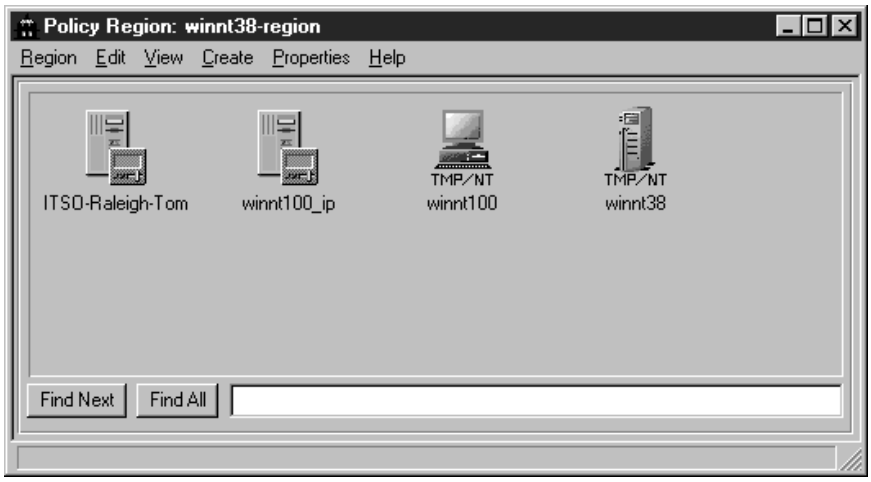


Figure 57. Newly Created LAN Access Site - winnt100_ip

Then we opened the LAN Access site. The only filter criteria we set was to select Netfinity as the management platform. (At that point in time we did not have any other provider installed, so it was the only one available in the list.)

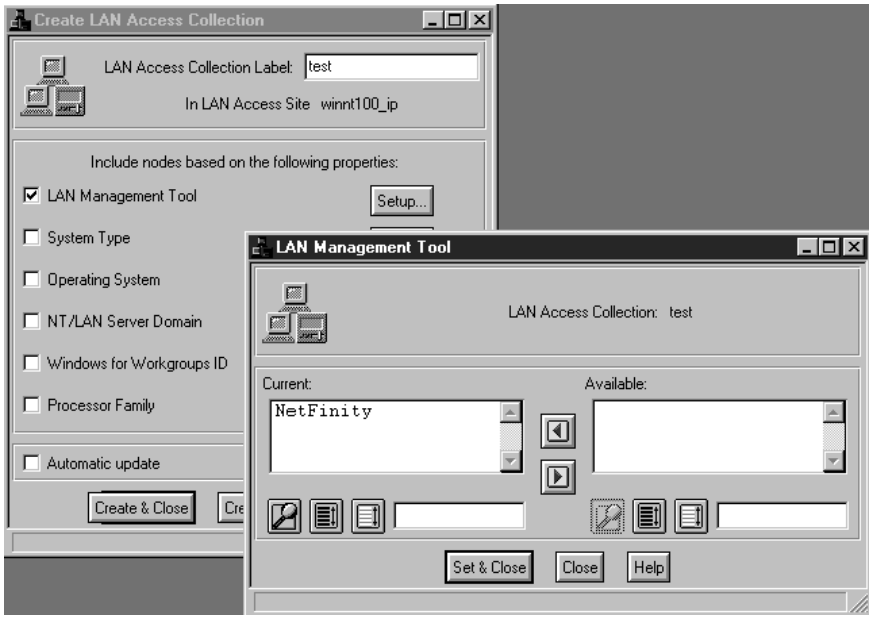


Figure 58. Setting Filter Criteria

We then clicked on **Set & Close** and **Create and Close**, which started selecting all possible clients from the chosen management platform that met the specified filter criteria.

Figure 59. Selecting the Client Systems

In our environment we found over 100 clients that had a Netfinity client installed.

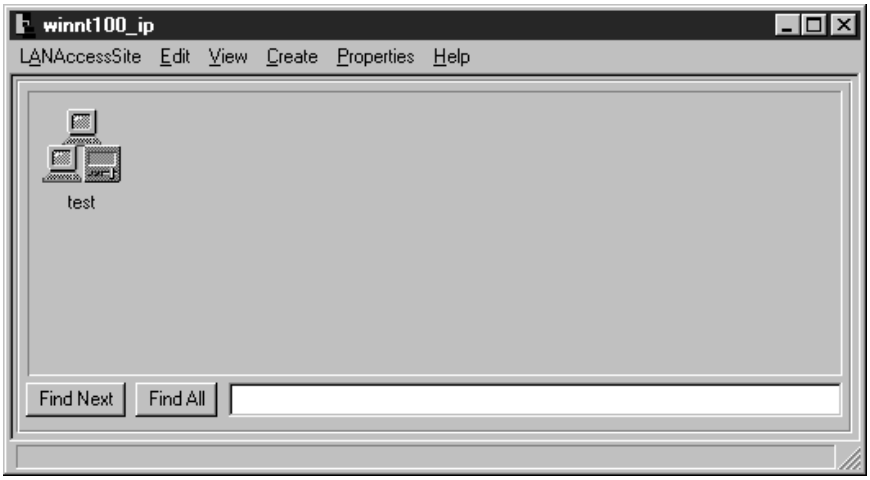


Figure 60. LAN Access Collection Test Created

In the above figure you see the new created LAN Access Collection called test. Double-clicking on this icon shows you the client systems that were discovered.

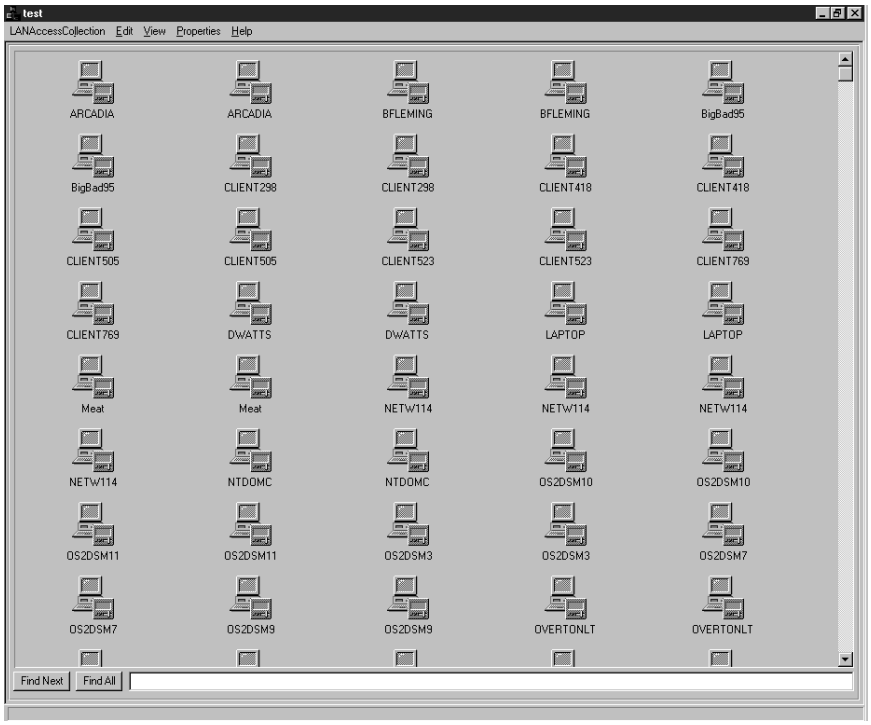


Figure 61. Discovered Client Systems

If you double-click on any of the machines that passed the filtering process, you will see the properties of the system. As an example, we selected **winnt80**. The results are shown in Figure 62 on page 49. Notice that the target protocol is TPCIP and the target provider is Netfinity. Of course, there is other useful information in the properties list but the main point here was to show the filtering process.

Figure 62. Properties of a Selected Client System - Online

In this example you can see that the machine winnt80 was running at this time (Availability = Running).

1.6.6.2 Filtering on Operating System and Transport Protocol

In this example we chose an OS/2 MPM provider using the NetBIOS protocol to communicate with Tivoli LAN Access.

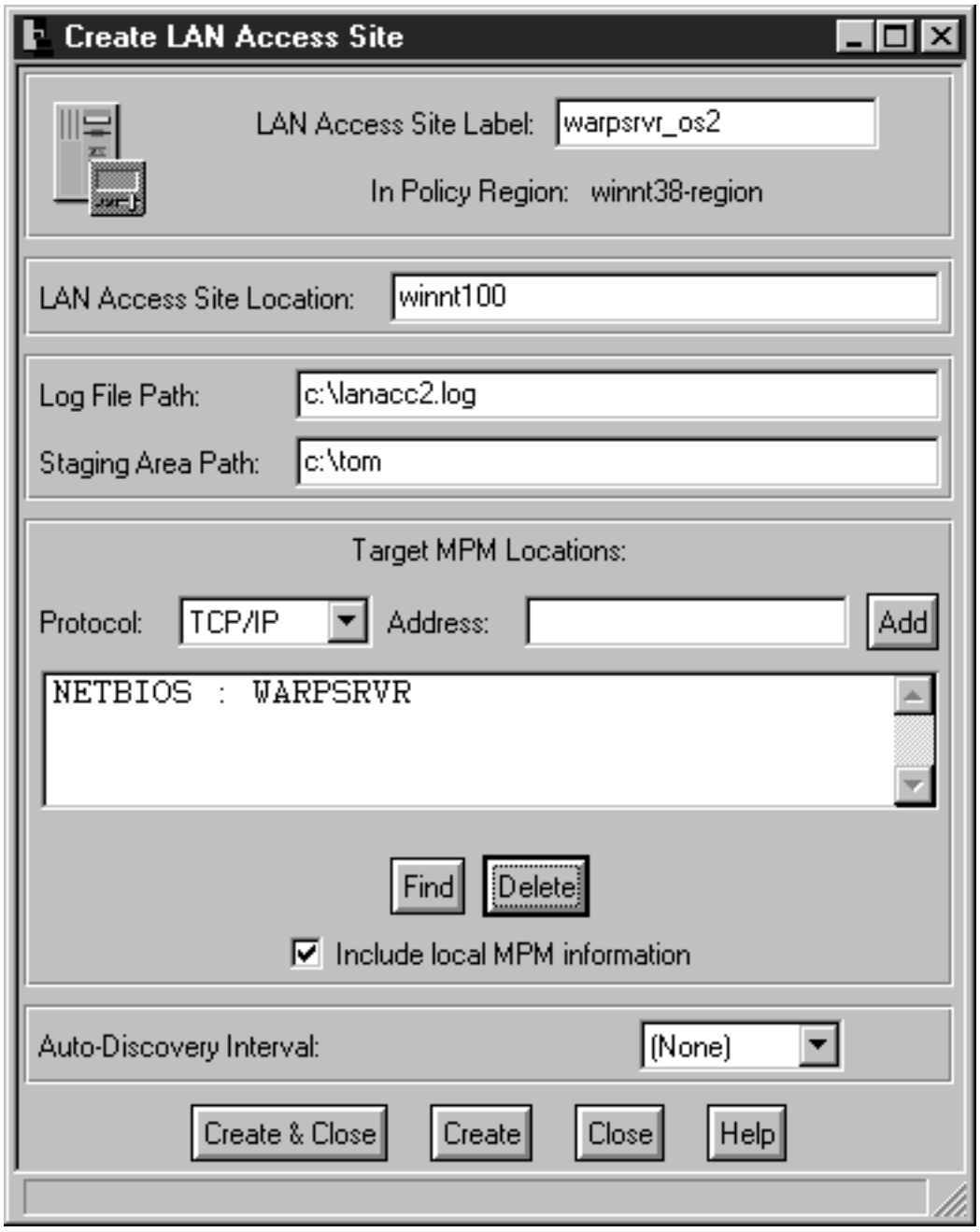


Figure 63. Create LAN Access Site

In some cases, access to systems might be restricted. If you did not specify an incoming user ID and password in the Security Manager of the Netfinity product, you are prompted to enter this security information.

Figure 64. Entering the Netfinity UID and PW

As with our previous example, we created a new LAN Access site for this filter.

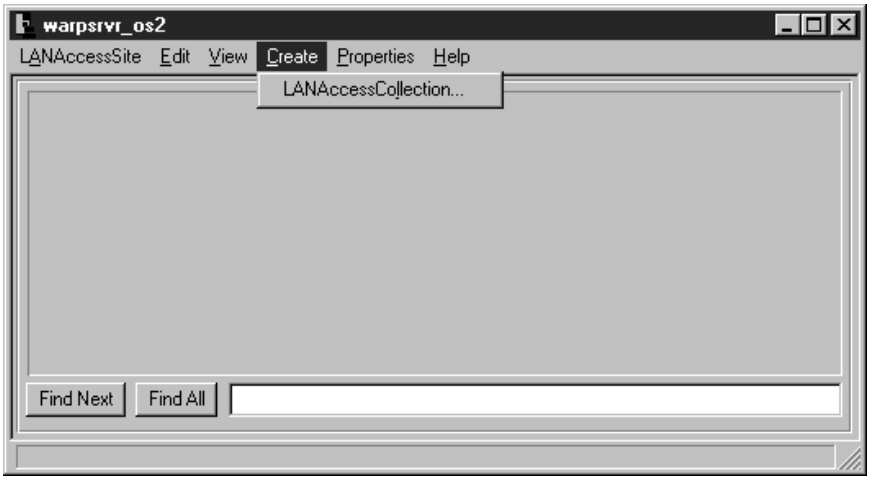


Figure 65. Creating LAN Access Collection in the LAN Access Site

After creating this site we created a new LAN Access collection.

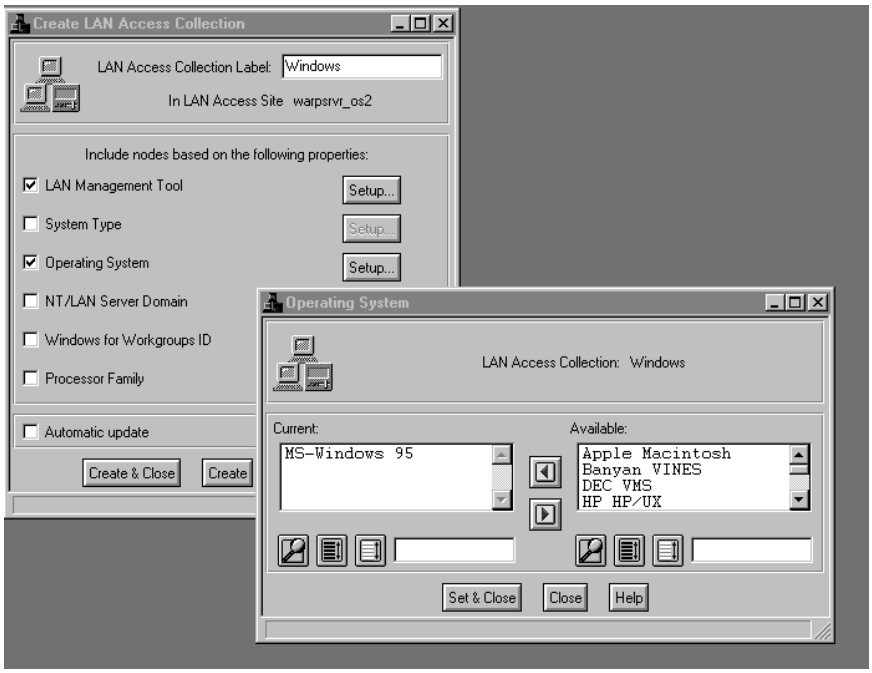


Figure 66. Set MS-Windows 95 As a Filter Criteria

In this example, we chose the operating system **MS-Windows 95** as the filter criteria.

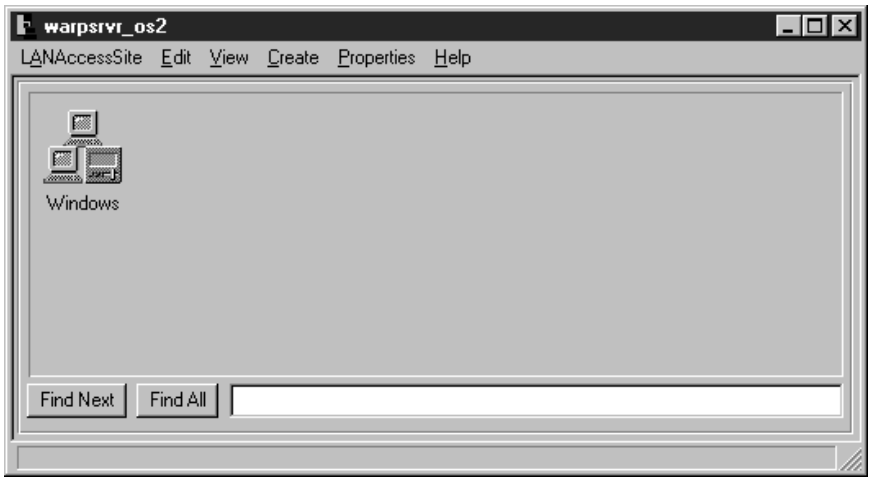


Figure 67. New LAN Access Collection Windows

The next thing that was done was to create the LAN Access collection. In this case we called it Windows. This also shows up in the title bar in the following figure:

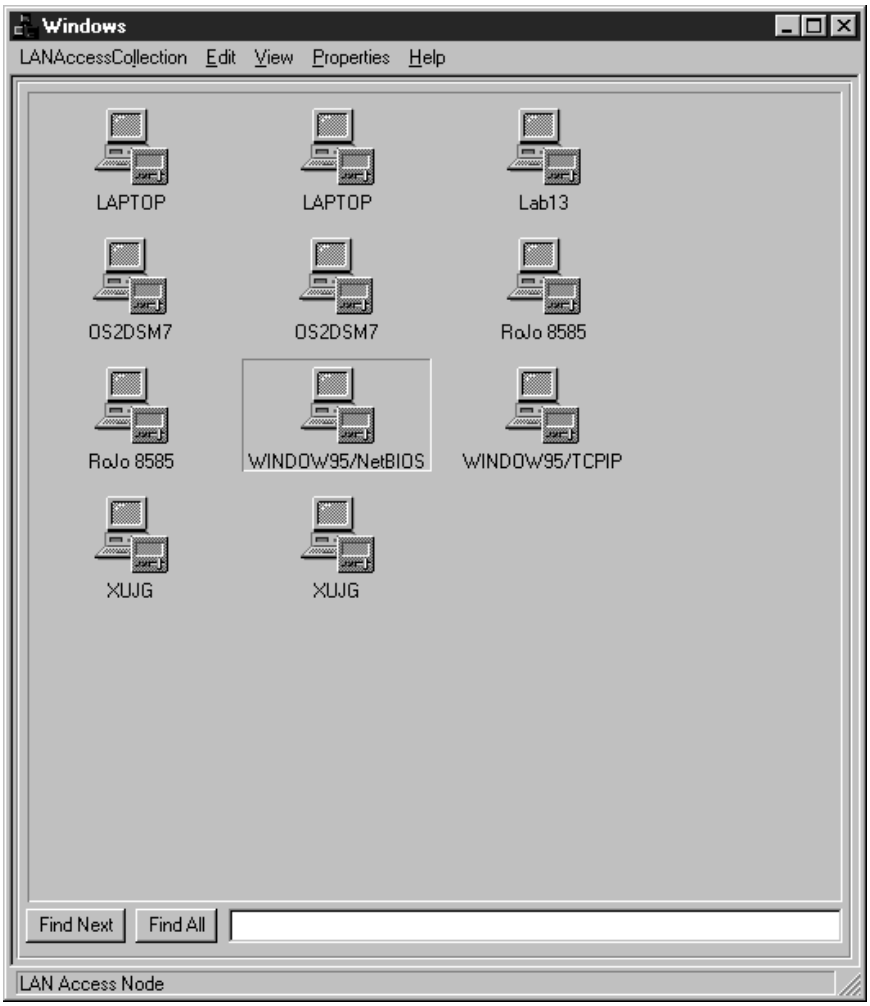


Figure 68. 11 Windows 95 Systems Found

This filtering showed us 11 systems in our collection. We selected one of them as shown below:

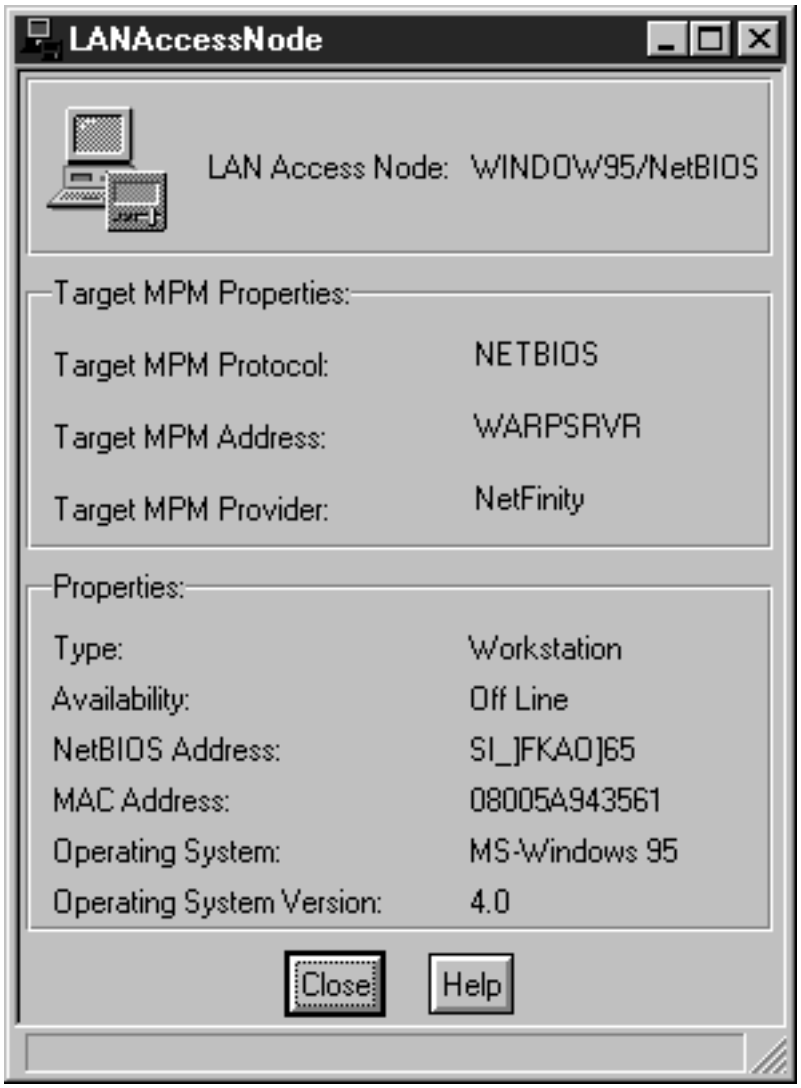


Figure 69. Properties of Machine - WINDOW95/NetBIOS

In this example the selected client is offline. That is reflected in the Availability field.

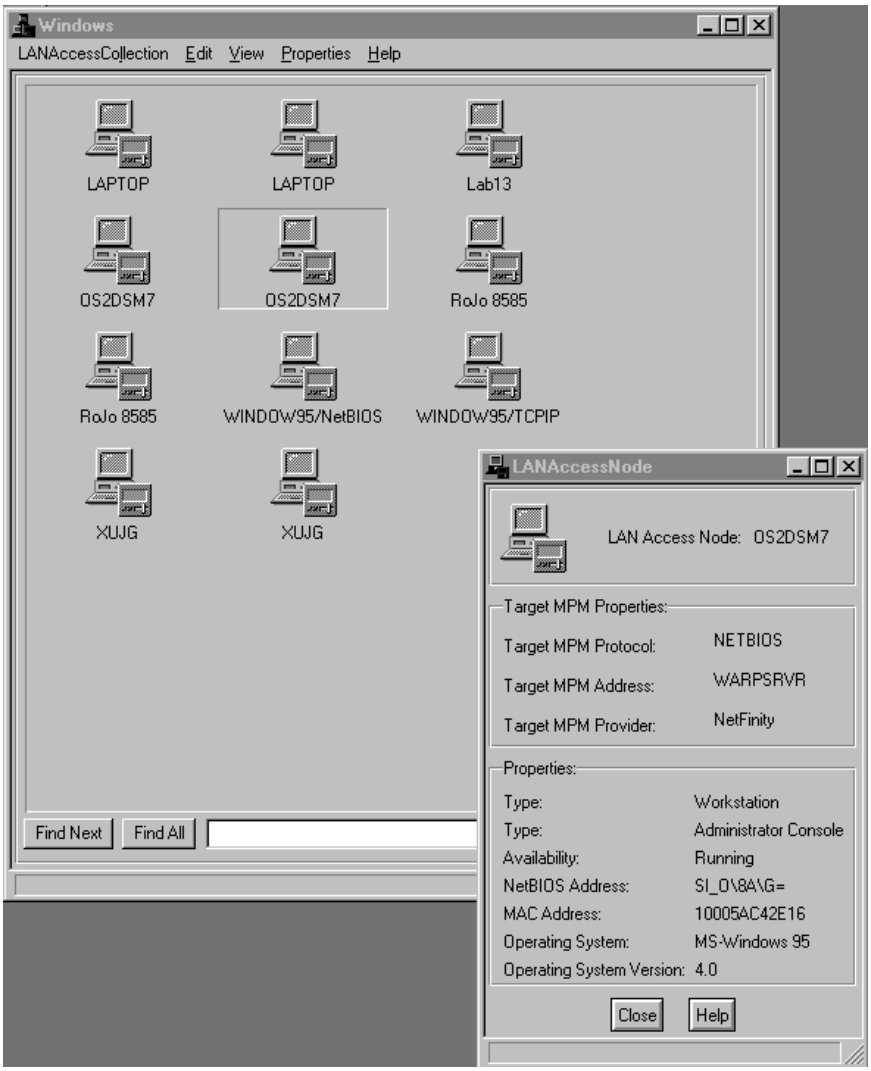


Figure 70. Properties of Machine - OS2DSM7

Looking at one of the other systems, you can see its properties. In this case, OS2DSM7 is running.

1.6.6.3 Filtering for Non-Windows NT Systems

In this example we created a collection that only filters Windows NT systems out.

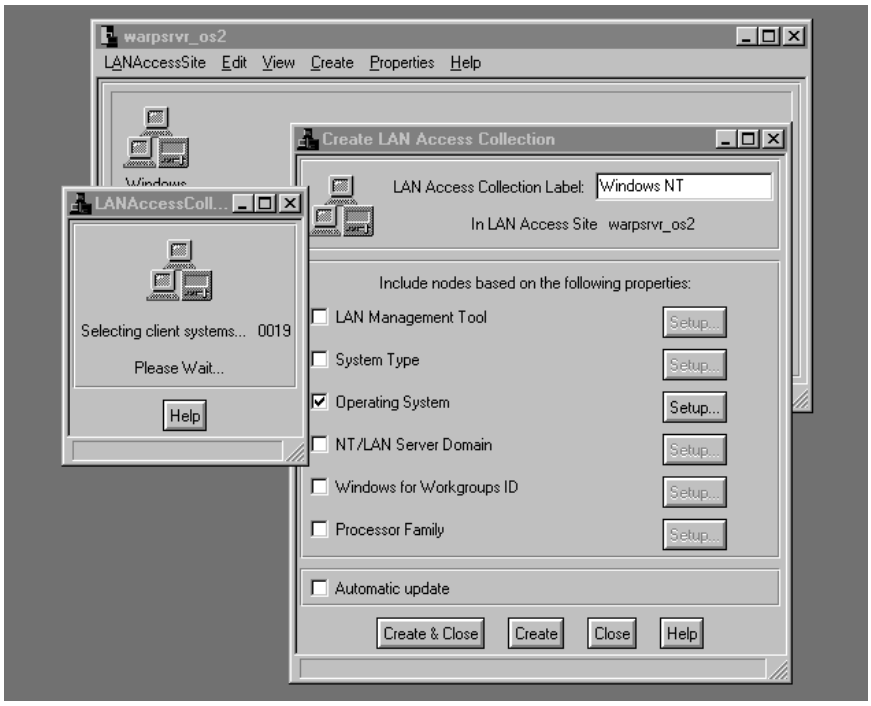


Figure 71. Creating a LAN Access Collection with Windows NT Clients

Using the same process as in the previous examples, we selected all operating systems except Windows NT.

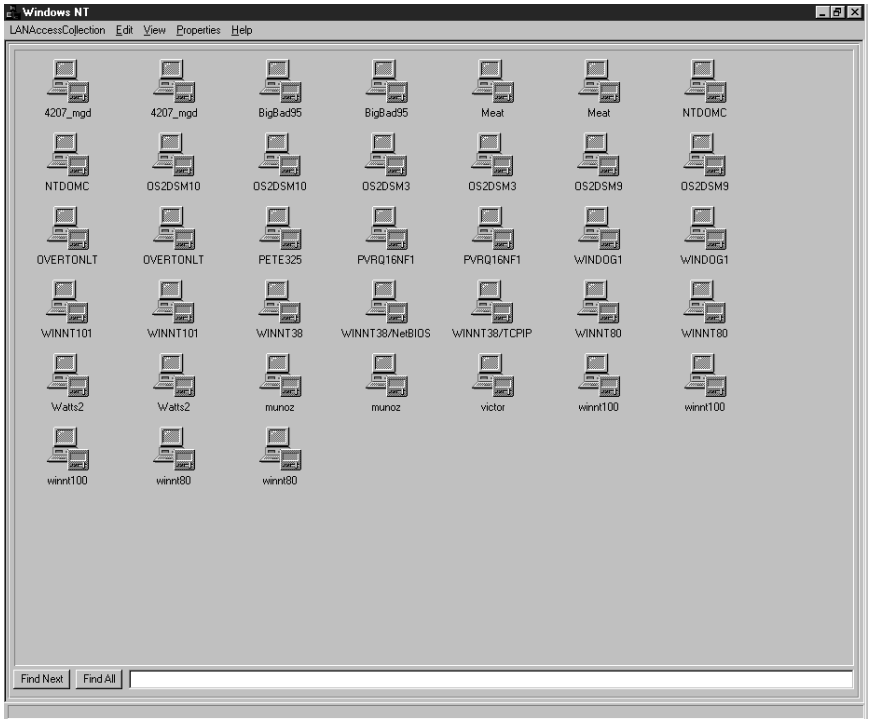


Figure 72. Netfinity Provider - Install Panel

We found 38 client systems that met this condition. If there are too many clients to fit on one panel, you can also choose a list view which will show you a lot more systems on the panel.

To do that you have to choose the **View** option and select **By Name** instead of By Icon:

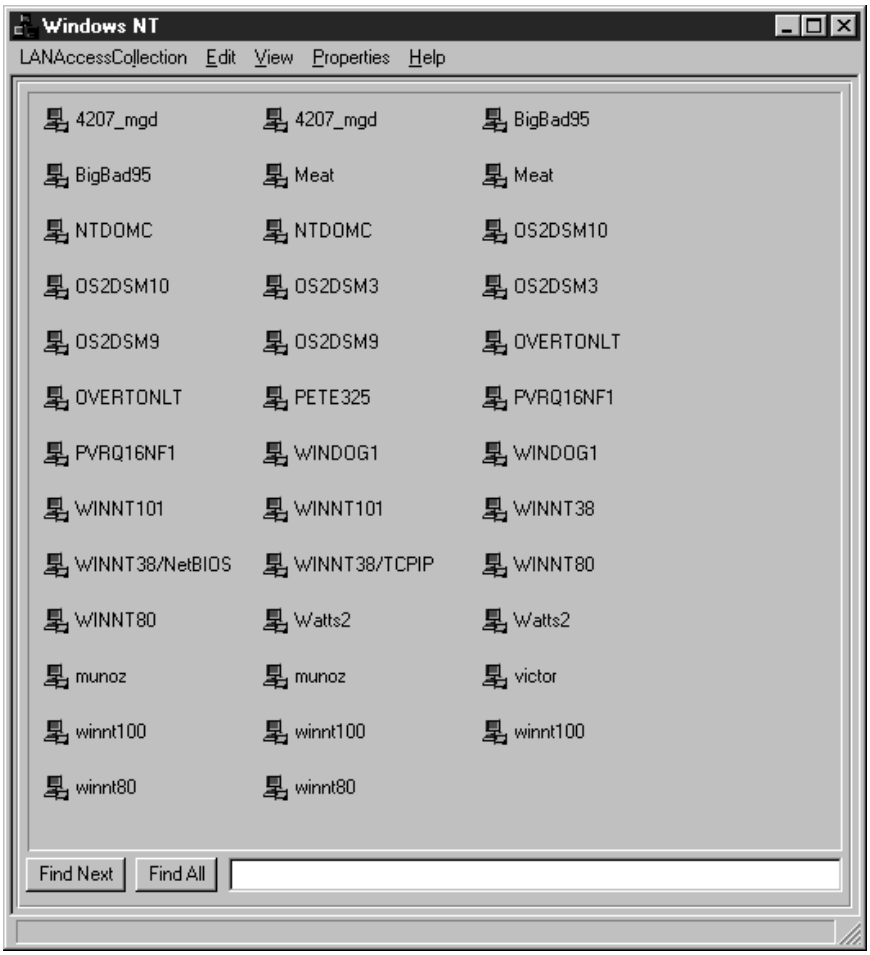


Figure 73. List View of the Clients

1.6.6.4 Combining Filters

In this example, we show how to combine multiple filters together. We selected the OS/2 LAN Access Collection that we had created and then selected the domain **wtrdm**.

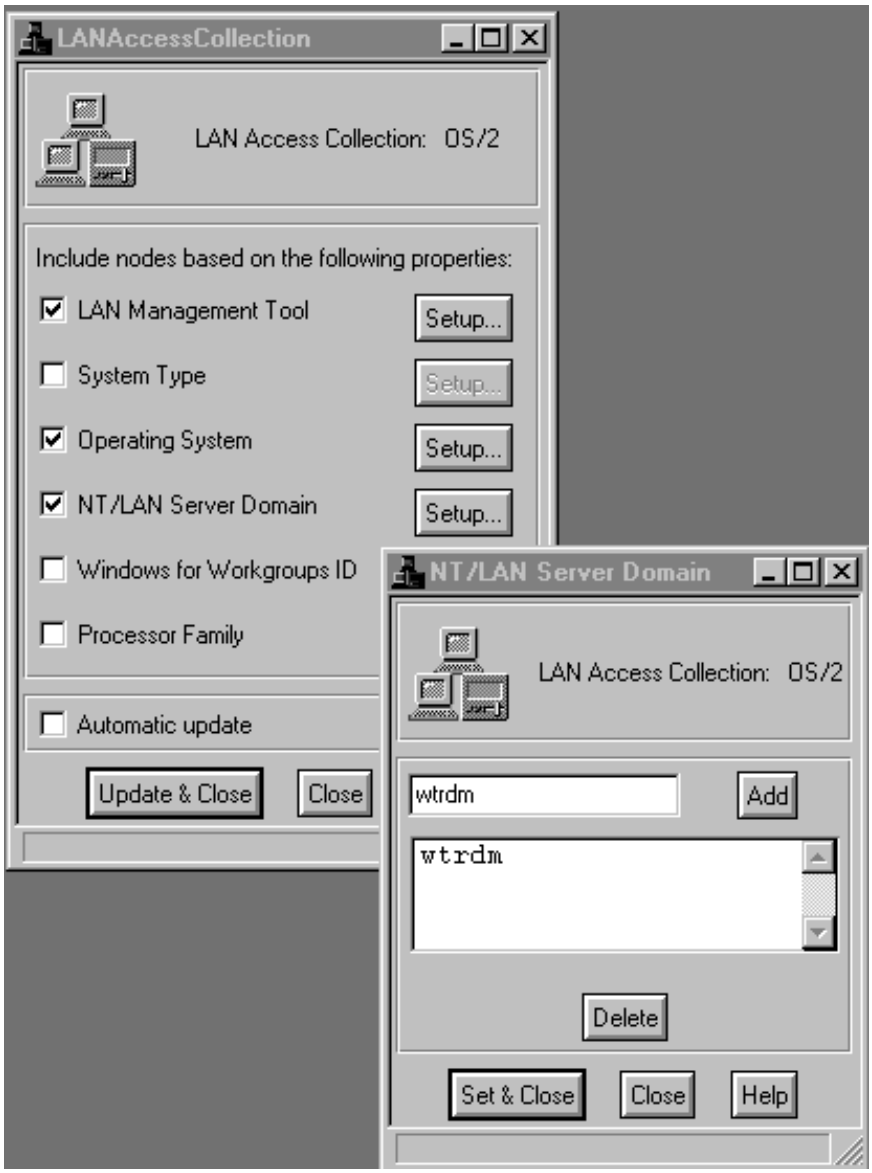


Figure 74. Selecting OS/2 and Domain Name

We select **OS/2** as the operating system and **wtrdm** as the domain.

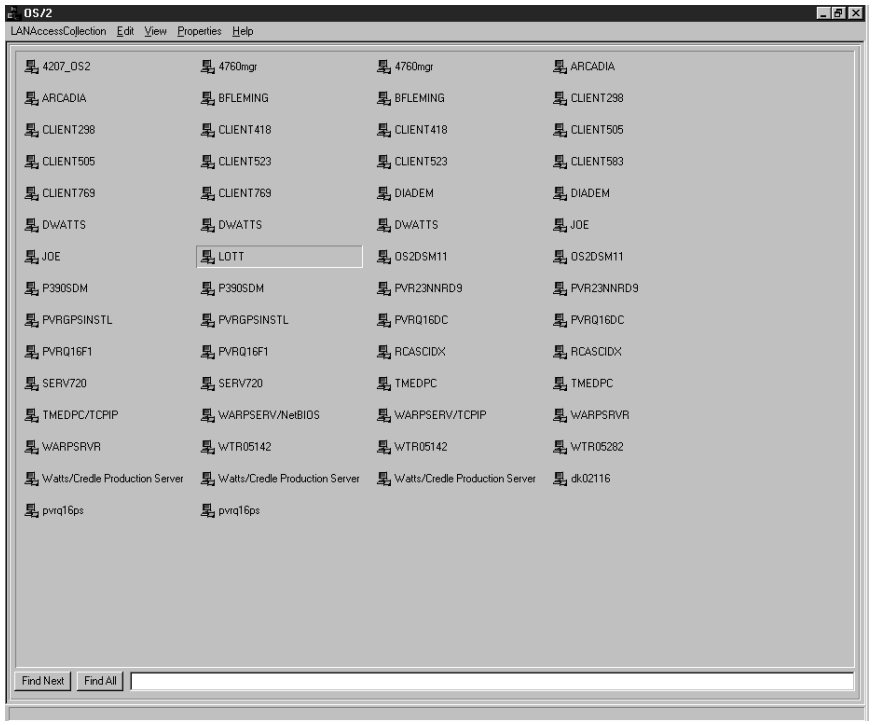


Figure 75. Name View of Clients Found

This filtering combination showed 58 OS/2 systems in the wtrdm domain.

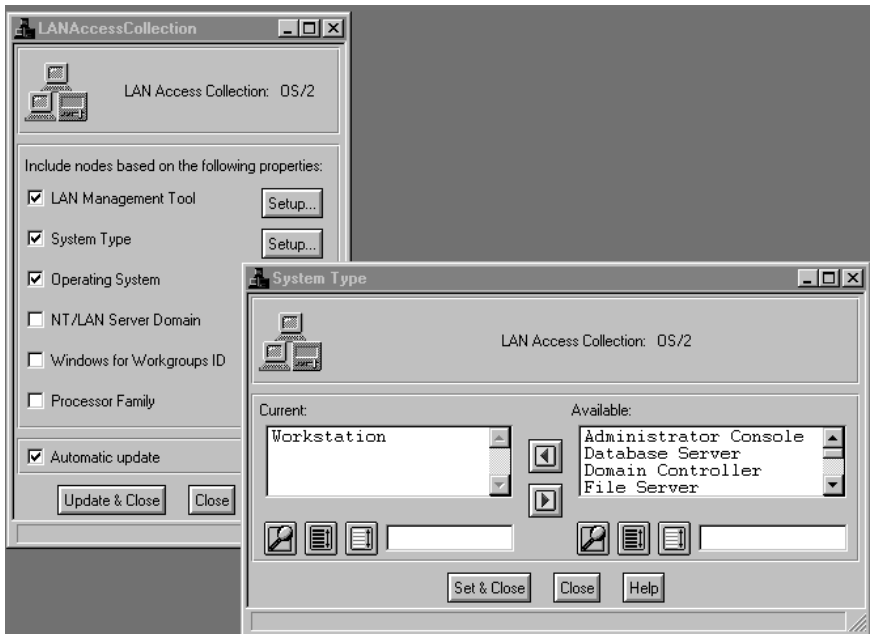


Figure 76. Adding System Type Workstation

After that we an added an additional property which will be logically ANDed to the one already defined. We chose a system type of **Workstation** as the additional filter criteria.

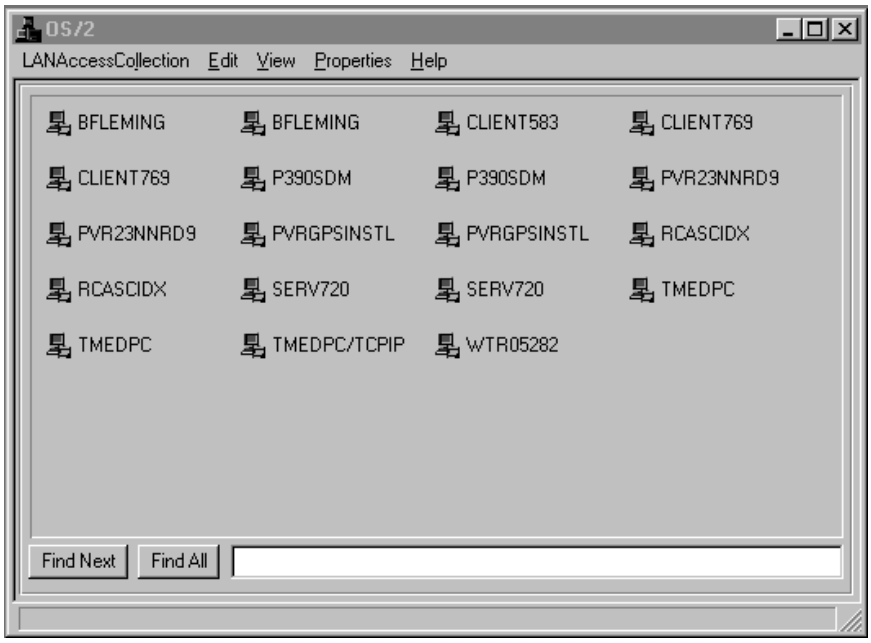


Figure 77. All OS/2 Clients Plus the New Setting

The result is that the number of OS/2 systems that were located was reduced to 19 systems.

1.7 Scheduler

If you selected an Auto-Discovery Interval when you created your LAN Access site (see Figure 36 on page 31), a job was automatically scheduled in the Tivoli Scheduler. To see this job, open the Tivoli desktop.

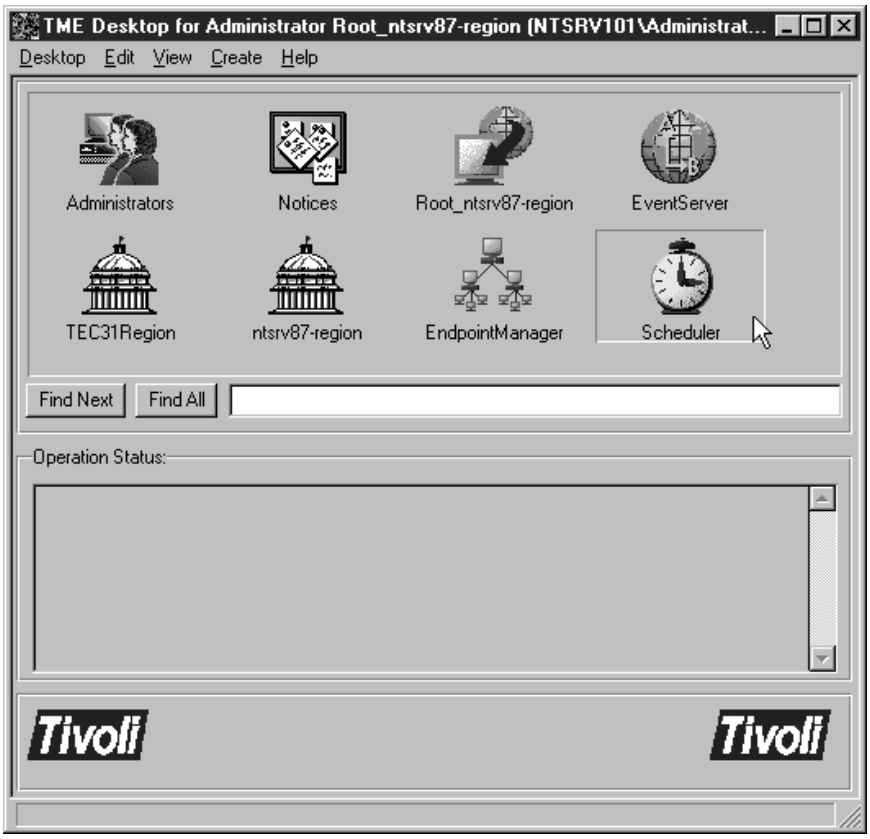


Figure 78. Tivoli Desktop

Double-click on the **Scheduler** icon.

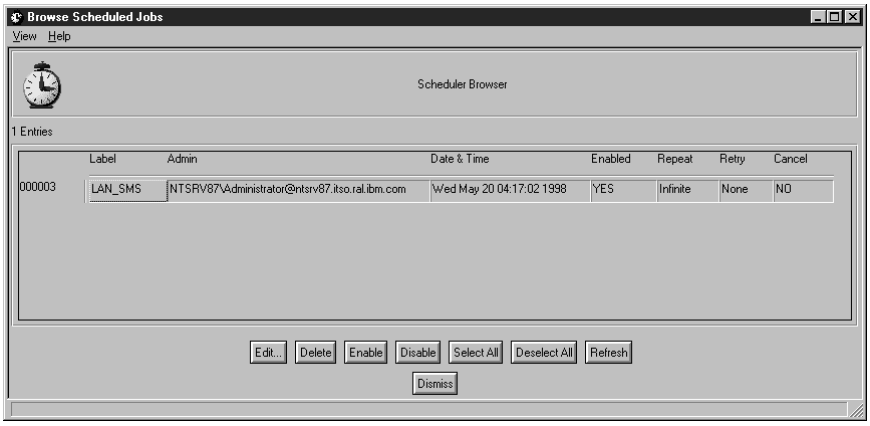


Figure 79. Browse Scheduled Jobs

You will see all the jobs scheduled in your TMR. In this case we only have the job for the automatic update of LAN Access resources. To edit the properties of the schedule job, just double-click on it.

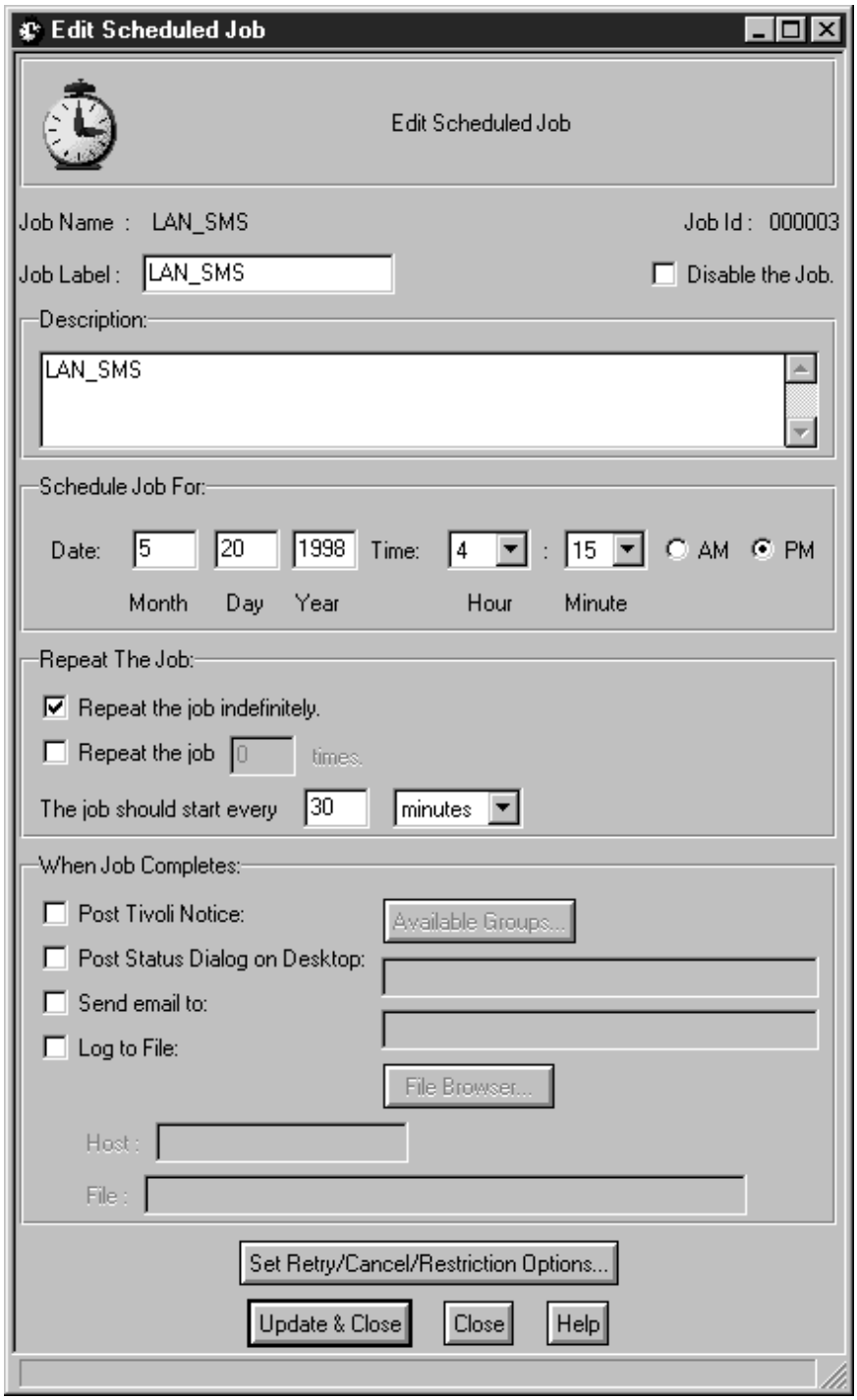


Figure 80. Information about a Scheduled Job

1.8 Configuring Support for LAN Alerts

This section describes the files and procedures required to enable TEC support for alerts received by the LAN Access event adapter from LAN clients. As described in 1.2.3, “Installation of LAN Access Components on the NT Managed Node” on page 7, the following files were installed during the execution of \w32\setup.exe:

- tecad_msb.exe

This is the executable for the event adapter. During installation, the svcmgr.ini file is updated to enable the LAN Access event adapter to start up as an auto-start service. The file size before installation is 5,329 bytes. After the install process the size is 5,908 bytes.

- tecad_msb.map

  This is the provider UID-to-TEC class name map file. This file contains the mappings between TEC event class names and the MPM provider UIDs of supported alerts. See Appendix A, “Configuration Files” on page 259 for configuration files.

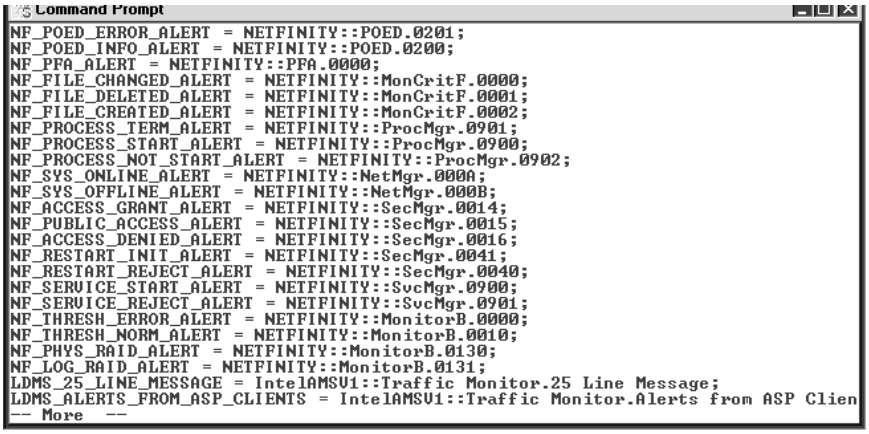


Figure 81. Provider UID-to-TEC Example

- tecad_msb.log

  This is the event adapter log file. This file is automatically generated by the LAN Access event adapter. It is not created during installation.

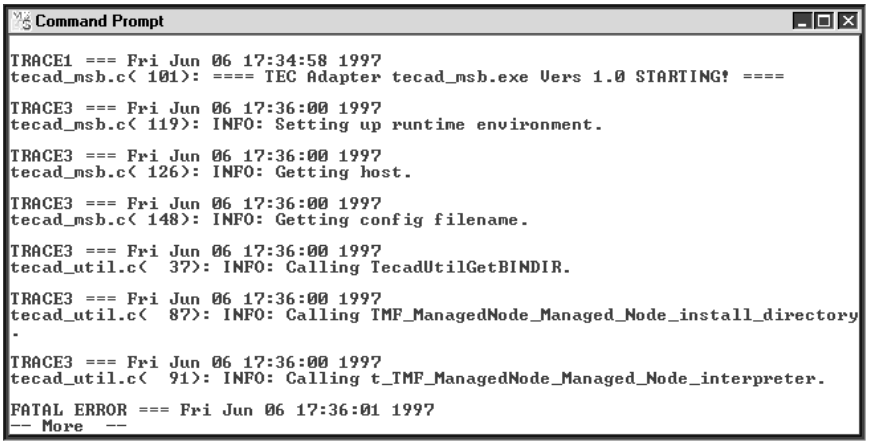


Figure 82. Event Adapter Log File Example

1.9 Importing LAN Access Event Classes

This section applies to all three LAN management suites (Netfinity, LANDesk and SMS) described in this book. To enable the TEC event server to present alert information on the Tivoli Enterprise Console, the following LAN Access event class files must be compiled into the run-time service of the TEC event server. These files are stored on the NT managed node during installation of the LAN Access event adapter.

- lanacc.baroc

  Main LAN Access classes used for all LAN Access event class files.

- la_netf.baroc

  Netfinity provider TEC event classes (or la_ldms / la_sms for LANDesk or SMS respectively).

You have to recompile the rule base on the event server with the LAN Access event classes. In the following sequence, steps 2 and 3 are required only if you are installing LAN Access for the first time and you are creating a new rule base for LAN Access.

Note: Make sure you have set the Tivoli environment variables before you try to issue a command from the command line interface. This can be done with the following command:

```
\winnt\system32\drivers\etc\tivoli\setup_env.cmd
```

You can also set them by setting the base environment variables from the System icon in the Control panel.

To see what the GUI looks like see 5.4.4, “Configuring the TEC Event Server” on page 249.

1. Copy the *.baroc files to the system that contains the event server.
2. If this is the first time you are installing LAN Access and you do not have a rule base for your environment, you have to create one by running the wcrtrb.exe CLI command. An example of this follows:

```
C:\Tivoli\bin\w32-ix86\bin>wcrtrb tom_base
C:\Tivoli\bin\w32-ix86\bin>
```

   The command is in the \Tivoli\bin\w32-ix86\bin directory. The syntax of this command is:

   ```
   wcrtrb (-S server) (-d (host:)directory) rulebase
   ```

   where

   - `-S server`

     Specifies the name of the event server in name registry format. The default is the local event server.

   - `-d host:directory`

     Specifies the directory where all event class definitions and rule sets reside.

The wcrtrb command creates the rule base at an event server. The event server in the current Tivoli Management Region (TMR) is used unless otherwise specified.

A rule base consists of event class specifications and rule sets. The event adapter event class specification and rule set must be in the rule base directory.

3. The default rule base can not be changed or compiled. If it is the first time it is being installed, you have to create a rule base by copying the contents of the default into your rule base using the wcprb.exe command. For example:

```
C:\Tivoli\bin\w32-ix86\bin>wcprb Default tom_base
C:\Tivoli\bin\w32-ix86\bin>
```

This executable is stored in the \Tivoli\bin\w32-ix86\bin directory. The syntax for this command is:

```
wcprb (-c)(-r)(-f)(-o)(-S source_server)(-D target_server)
source_rulebase target_rulebase
```

Where:

- `-c`

  Copies the class definitions. All class definitions in the target rule base are overwritten.

- `-r`

  Copies the rules sets. All rule sets in the target rule base are overwritten.

- `-f`

  Forces duplicate files to be replaced in the destination rule base.

- `-o`

  Deletes all existing files in the destination rule base.

- `-S source_server`

  Specifies the name of the event server from which to copy, in name registry format.

- `-D target_server`

  Specifies the name of the event server to copy to, in name registry format.

- `source_rulebase`

  Specifies the name of the rule base to copy.

- `target_rulebase`

  Specifies the name of the new rule base.

The wcprb command copies an existing rule base to another existing rule base. You can specify the -c argument to copy the class definitions, or the -r argument to copy the rule sets. If you do not specify either the -c or -r argument, both the class definitions and the rule sets are copied.

4. To import the event classes contained in the *.baroc files to the rule base, you have to run the wimprbclass.exe command located in the \Tivoli\bin\w32-ix86\bin directory. The format of this command is:

```
wimprbclass (-S server)(-a class_file | -b class_file) class_file rulebase
```

The wimprbclass command imports a file of event class specifications into a rule base, appending it to the end of the class specifications unless otherwise specified with arguments. The existing event class specifications are not deleted. Senior authorization is needed to execute this task. For a description of authorization roles see *Understanding Tivoli's TME 3.0 and Tivoli*.

Where:

- `-S server`

  Specifies the name of the event server in name registry format. The default is the local event server.

- `-a class_file`

  Adds the class after the named class.

- `-b class_file`

  Adds the class before the named class.

- `class_file`

  Specifies the full path of the class definition file to import. You can specify the class file in the format host:class_file.

- `Rulebase`

  Specifies the name of the rule base.

For our installation we did the following:

```
C:\Tivoli\bin\w32-ix86\bin>wimprbclass lanacc.baroc tom_base
C:\Tivoli\bin\w32-ix86\bin>
C:\Tivoli\bin\w32-ix86\bin>wimprbclass la_netf.baroc tom_base
C:\Tivoli\bin\w32-ix86\bin>
```

If you were implementing for Intel LANDesk or Netfinity, you would use la_ldms.baroc or la_sms.baroc respectively.

5. Run the wcomprules command to compile the rule base. For example:

```
C:>wccomprules tom_base
C:>
```

The syntax of this command is:

```
wcomprules (-t) rulebase
```

Where:

- `-t`

  Turns on tracing.

- `Rulebase`

  Specifies the name of the rule base to compile.

The wcopmrules command compiles the rules in the rules base, specified by rulebase, into Prolog object files that the rules engine can process.

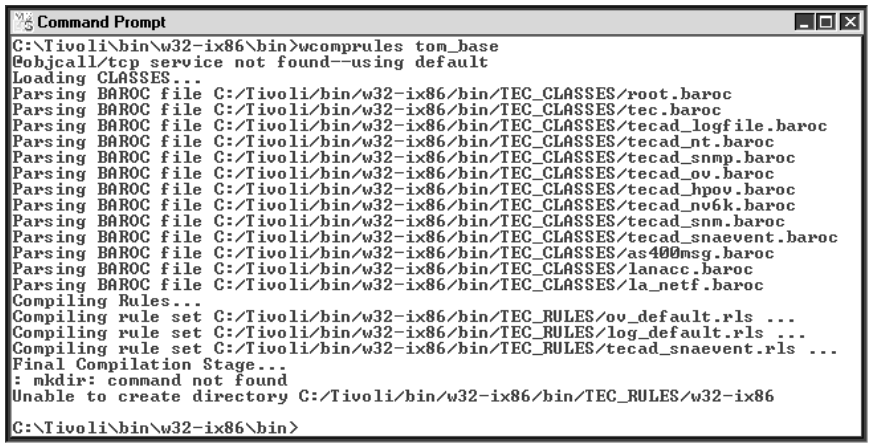


Figure 83. Compiling the Rule Base - Done

Note: The reason for the error `Unable to create directory` in Figure 83 is that the command was not started from the root directory. Make sure to start these commands from C:> and that the setup_env.cmd has been run. The error message `@objcall/tcp service not found-using default` was because setup_env.cmd had not been executed.

6. Stop the event server by running the wstopesvr command. The wstopesvr command stops the event server or database server in the local Tivoli Management Region (TMR). If any running consoles are connected to the event server, the consoles are also stopped. If no -d flag is specified, the database server is not stopped. If the database server is not stopped, you can still use the database commands.
7. Load the rule base containing the LAN Access event classes using the wloadrb command, for example, wloadrb tom_base.

   The wloadrb command loads a rule base into an event server. The rule base must already be defined at the server, and any event class specification files and rules files in the directory must be valid. The server in the current Tivoli Management Region is used unless specified otherwise. The loaded rule base replaces all event class specifications and rules currently defined at the server. Only one rule base can be active at a time. Loading another rule base overwrites the currently active rule base. The syntax is:

   ```
   wloadrb (-S server)(-u) rulebase
   ```

   If option -u is specified, the loaded rule base is used immediately. If this argument is not specified, the new rulebase will not be used until the event server is restarted. This argument only reloads rules. If you change any event classes, you must stop and restart the event server to load the changes to the classes.
8. Restart the event server by running the wstartesvr command.

```
C:>wstartesvr
C:>The Tivoli Enterprise Console Server is initializing...
C:>
```

By default, the wstartesvr command starts the event server in the local Tivoli Management Region (TMR). If the database server was shut down with the

wstopesvr command, it is also restarted. The event server reads configuration files to set up its database of event classes and rules, reads configuration file of pending events, then makes itself available for communication with event adapters. It begins processing pending events and incoming events immediately.

You need to have senior administrator rights to perform the above commands.

For further information on the above commands refer to the *Tivoli/Enterprise Console User's Guide Volume II* and the *Tivoli/Enterprise Console Rule Builder's Guide*.

After successfully completing these steps you may want to have a look on the TME Notice board and check for notifications messages for the group TME Administration.

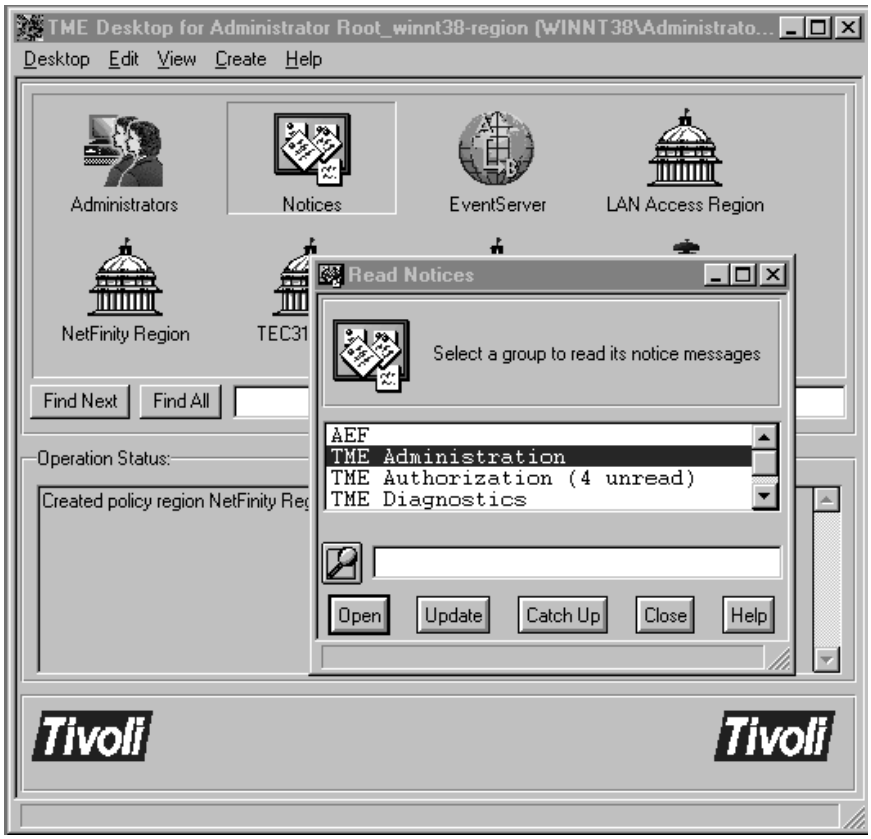


Figure 84. Event Adapter Log File Example

In addition, a new Administrator was created. You can verify by looking at the TME Authorization Notice group or by double-clicking on the **Administrators** icon on the TME Desktop.

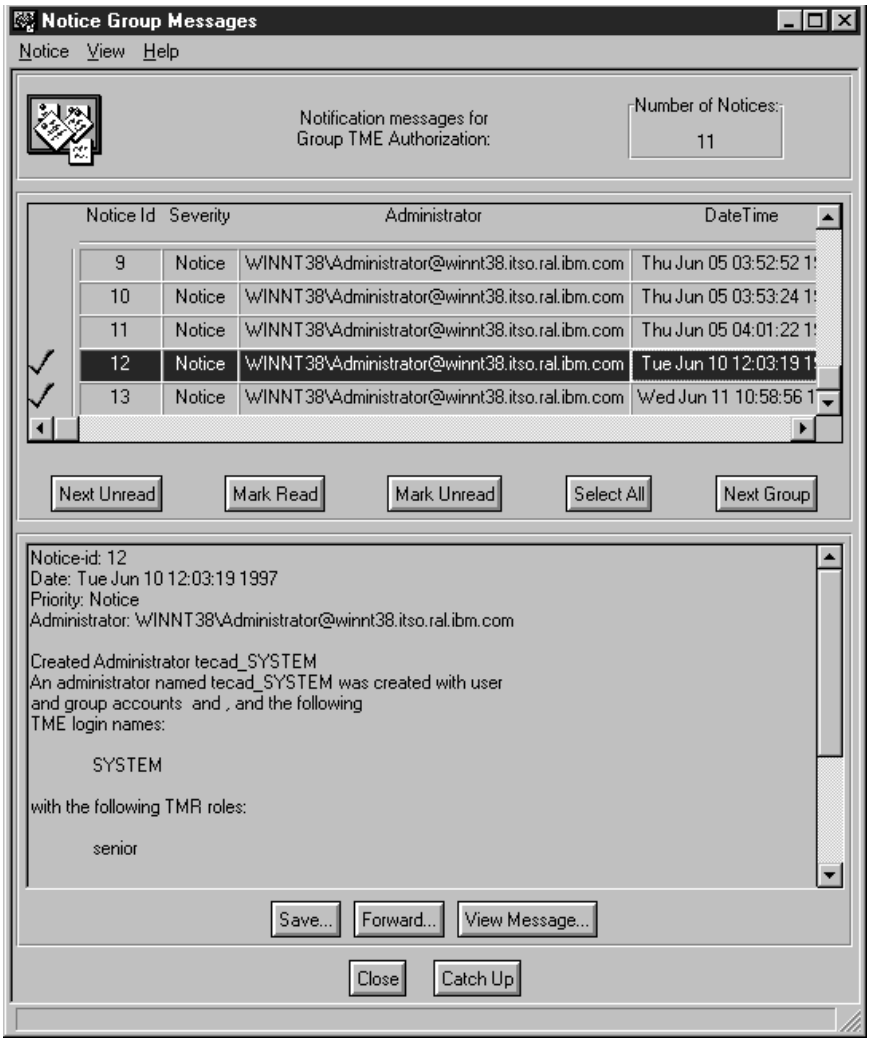


Figure 85. Event Adapter Log File Example

You should notice that a new Administrator tecad_SYSTEM has been created as shown in the following figure:

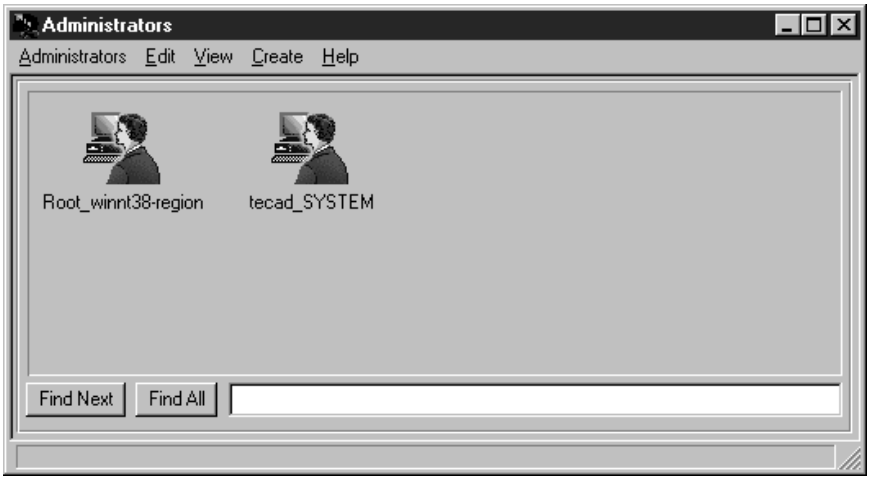


Figure 86. Event Adapter Log File Example

1.10 Editing the Configuration File

The LAN Access event adapter configuration file, tecad_msb.cfg, is stored on the NT managed node during the installation of the LAN Access event adapter. This file contains the default settings for trace and error log levels and a required entry representing the location of the TEC event server. These settings do not need to be changed for normal operation.

If you edit tecad_msb.cfg to add or delete an entry, you must stop and restart the event adapter for the changes to take effect.

```
#**********************************************************************
#
# Tivoli LANAccess TEC Adapter Configuration File
#
# Author:    TIVOLI
# Date:        March 11, 1997
# Version: Version 1.0
#
# Copyright (c) 1997, Tivoli Systems, Inc.  All rights reserved.
# Licensed Materials - Property of Tivoli Systems
#
# tecad_msb.cfg - Tivoli LANAccess TEC adapter configuration.
#
# File format:
#    <keyword>=<value>
# where <keyword> is
#   ServerLocation      - Hostname of the TEC server.
#   ServerPort          - Port number on which the TEC server is listening.
#   EventMaxSize        - Maximum length of TEC event message.
#   ConnectionMode      - connection_oriented OR connection_less
#   WellBehavedDaemon   - TRUE/FALSE
#   ErrorLogLevel       - FATAL/MAJOR/MINOR.
#   TracingLevel        - LOW/NORMAL/VERBOSE.
#
#**********************************************************************
ServerLocation=@EventServer
EventMaxSize=4096
ConnectionMode=connection_less
TracingLevel=NORMAL
ErrorLogLevel=MAJOR
```

Figure 87. tecad_msb.cfg

Chapter 2. Intel LANDesk with Tivoli LAN Access V1.1

This chapter documents the installation and customization of Intel LANDesk for our environment, as well as shows all the configuration-related files.

2.1 TMR Server

For our test environment for the Tivoli LAN Access management of LANDesk, we used the following hardware and software:

Hardware:

- IBM PC 350-P133 with 80 MB of memory and a 1-GB hard drive

Operating system:

- Windows NT 4.0
- Service Pack 3
  - Windows NT 4.0 with Service Pack 2 is a prerequisite for Tivoli LAN Access.

TMR prerequisite software:

- TMR Server with Tivoli Framework Version 3.1
- Patch 3.1.1 (Service Pack 1)
- Patch 3.1.2

The following are optional components for event-driven support:

- Tivoli Enterprise Console 3.1
- Tivoli Inventory 3.2
- Sybase SQL Server Professional (or Oracle Server)

2.2 Managed Node

For our managed node for the Tivoli LAN Access management of LANDesk we used the following:

Hardware:

- IBM ValuePoint 100DX4/TP with a 486/DX4-100 processor and 32 MB of RAM memory

Operating system:

- Windows NT 4.0
- Service Pack 3
  - Windows NT 4.0 with Service Pack 2 is a prerequisite for Tivoli LAN Access.
- Tivoli Framework Version 3.1
- Patch 3.1.1 (Service Pack 1)

- Patch 3.1.2
- Tivoli Enterprise Console's NT Adapter
- Tivoli Enterprise Console's SNMP Adapter

2.2.1 Sybase Server

Hardware:

- IBM 760EL ThinkPad with a P120 processor and 72 MB of RAM memory

Operating system:

- Windows NT 4.0
- Service Pack 3

Database:

- Sybase SQL Server Professional

2.2.2 LANDesk Management Workstation

Hardware:

- IBM PS/77 with a 486/DX2-66 processor and 24 MB of RAM memory

Operating system:

- Windows 95

LANDesk Software:

- LANDesk Management Suite Version 2.51
- Btrieve 6.15
- Patch 6.15.440

2.2.3 LANDesk Management Server

Hardware:

- IBM PS/2 Server 95 with a 486/DX2-66 processor and 32 MB of RAM memory

Operating system:

- NetWare 4.10
  - Library upgrade C (libupc.exe)
  - 410 patch 7 (410pt7.exe)
  - Log Upgrade (log412.exe)
  - Map Upgrade (map412.exe)
  - NetWare Admin Upgrade (nwamn2.exe)
- TCP/IP for communicating with Windows NT Servers
- LANDesk Management Suite Version 2.51 (installed from the :LANDesk management workstation)
- Btrieve 6.15 (installed from the LANDesk management workstation)
- Patch 6.15.440 (installed from the LANDesk management workstation)

2.3 Prerequisites for Installing LANDesk

You should have the system components described in the following sections in place before installing LANDesk Management Suite for use with Tivoli LAN Access.

2.3.1 Management Server

- Novell NetWare 3.1x or 4.x.
- 5 MB of system memory dedicated to the LANDesk Management Suite NLMs.
- A minimum of 24 MB of total system memory is recommended for a server running only NetWare and LANDesk Management Suite.
- 125 MB of free disk space for the following:
  - 30 MB of disk space for the Management Database.
  - 95 MB of disk space for the LANDesk Management Suite.
- An account on the SYS volume with supervisor or admin equivalent rights.
- CLIB Version 3.11g installed on the NetWare Server.
- Btrieve Version 6.15 or later.
- Btrieve Patch 6.15.440.
  - To manage Windows NT servers, the TCP/IP protocol must be loaded on both Windows NT and the NetWare Server.

2.3.2 Management Workstation

- 80486 66 MHz IBM-compatible workstation or better.
- 16 MB of system RAM.
- 10 MB of local hard disk space for local data gathering.
- MS-DOS 5.0 or later.
- Network interface card with an ODI device driver capable of operating in promiscuous mode.
  - A promiscuous mode ODI driver is not necessary if you are just using the Software Probe function to gather data for Traffic Monitor and Performance Monitor.
- Windows 95 configured for NetWare or Windows NT networking.
- Windows 95 Client for NetWare networks (Client32 not supported).
- LSL.COM Version 2.02 or later.

2.3.3 NetWare

- Novell NetWare 3.1x or 4.x
- 12 MB of free disk space
- 2 MB additional system RAM above your current requirements

2.3.4 Windows NT

- Windows NT Version 3.5 or later
- 12 MB of free disk space
- TCP/IP

2.3.5 Software Probe Stations

- 80486 33 MHz IBM-compatible workstation or better
- 8 MB of system RAM
- 25 MB of local hard disk space for Performance Monitors logs
- Network adapter or interface card with an ODI device driver capable of operating in promiscuous mode

2.3.6 Client Workstations

- IBM-compatible Windows 95, Windows NT workstations/servers or OS/2
- 16 KB of system RAM available for optional TSRs
- Novell NetWare Client for Windows Version 1.2 or later or Windows 95 Client for NetWare networks
- Microsoft Network client software

2.4 Installation and Configuration of Btrieve

This section shows the installation and configuration considerations for Btrieve as it is used with LANDesk Management Suite 2.51.

From a Windows 95 workstation that you intend to use as your management console, you will need to be logged into your NetWare Server with administrator or supervisor rights. Point to the Btrieve.615 directory on the LANDesk Management Suite 2.51 (LDMS 2.51) CD or copy the code to a local/network drive. Open the Btrieve.615 directory and run the install.exe.

2.4.1 Indicating Installation Targets

During the installation of Btrieve, the first information you must provide is an installation target for the NetWare server components of Btrieve.

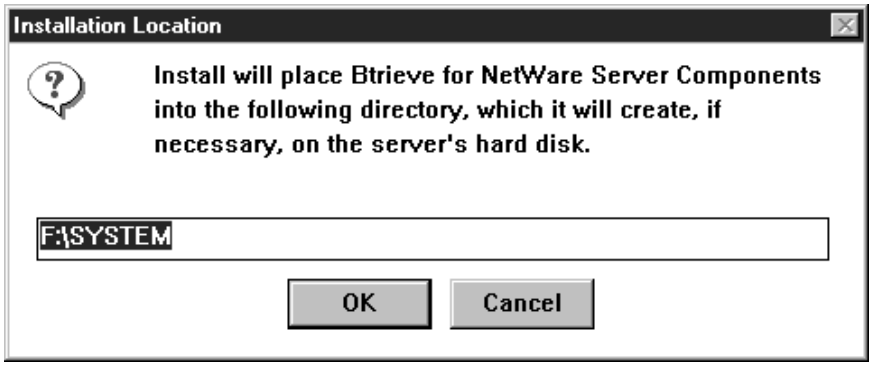


Figure 88. Server Component Installation Target Directory

By default this target is the SYS:SYSTEM volume.

You will be prompted to confirm your choice.

You will then need to select the target for the NetWare workstation requester and other utilities. The default location is: SYS:bti\NetWare. This directory will be created for you if it isn't present.

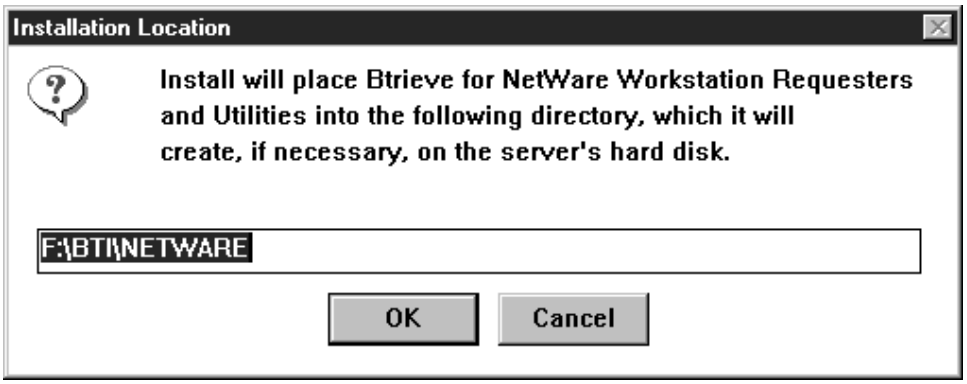


Figure 89. Requesters and Utilities Installation Target Directory

You can use the default directory location if you wish, which is what we did. You will then be prompted to confirm your choice.

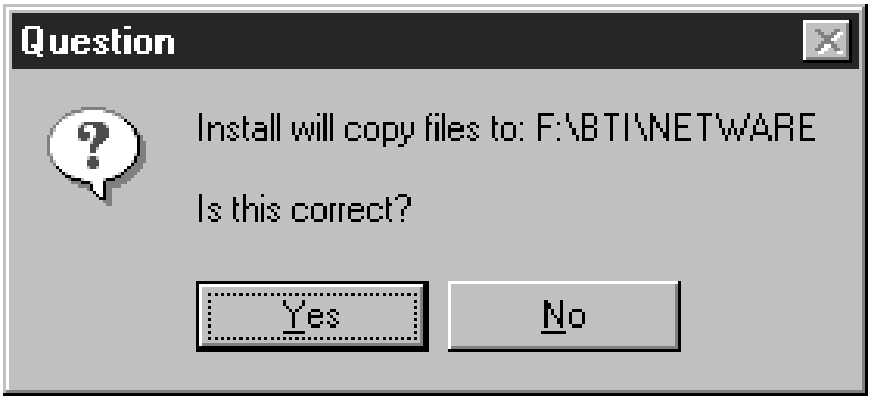


Figure 90. Requesters and Utilities Installation Target Confirmation

2.4.2 Installation

As with any installation, always accept the option to back up any files that the installation process may modify. It is always a good idea to have a way to go back to where you started if you run into any problems.

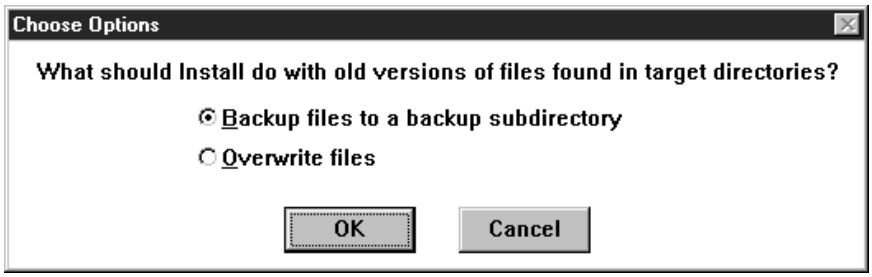


Figure 91. Backup Overwrite Option

Even if there are no files to back up, the installation window will show a progress bar and show you the names that it is checking.

- When you install Btrieve 6.15, you may see an error during file decompression stating `Unable to write to destination`. This prompt is generated when the existing Btrieve files are marked read only. To fix this problem, change the Btrieve files to read/write.

2.4.3 Change Btrieve Files from Read-Only to Normal

You need to change the attributes of the Btrieve files. The process to do that follows:

1. Select all of the Btrieve files listed below using the Windows 95 Explorer and click on **Tools** → **Find** → **File or Folders**.

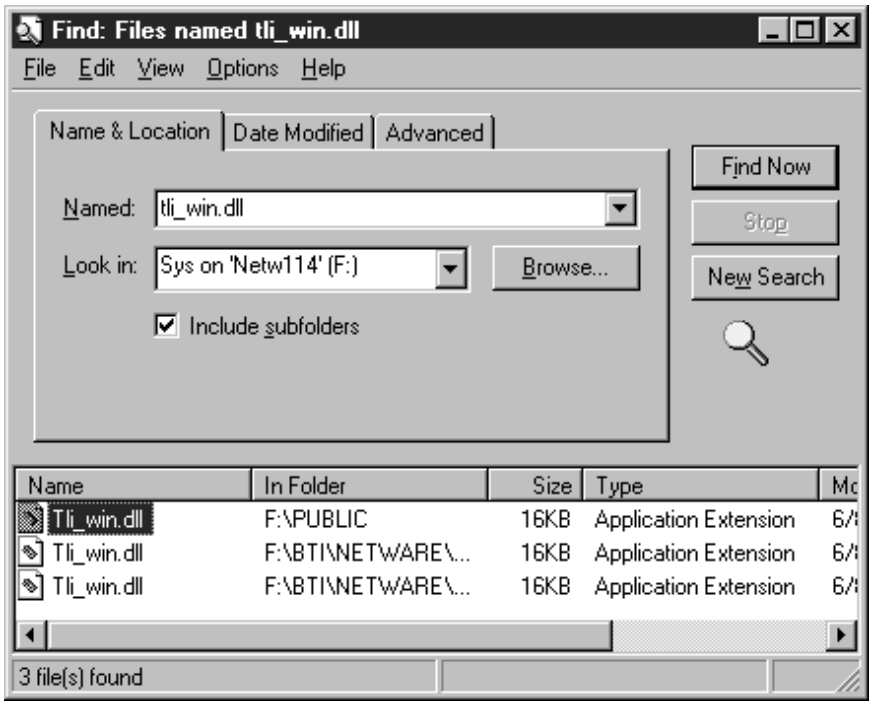


Figure 92. Find File Panel

The files beginning with WBT are located in the SYSTEM directory.

- TLI_WIN.DLL
- TLI_SPX.DLL
- WBTRVRES.DLL

- WBTRTHNK.DLL
- WBTRCALL.DLL
- WBTICOMM.DLL

2. Click on **File** and **Properties** to open the properties dialog.

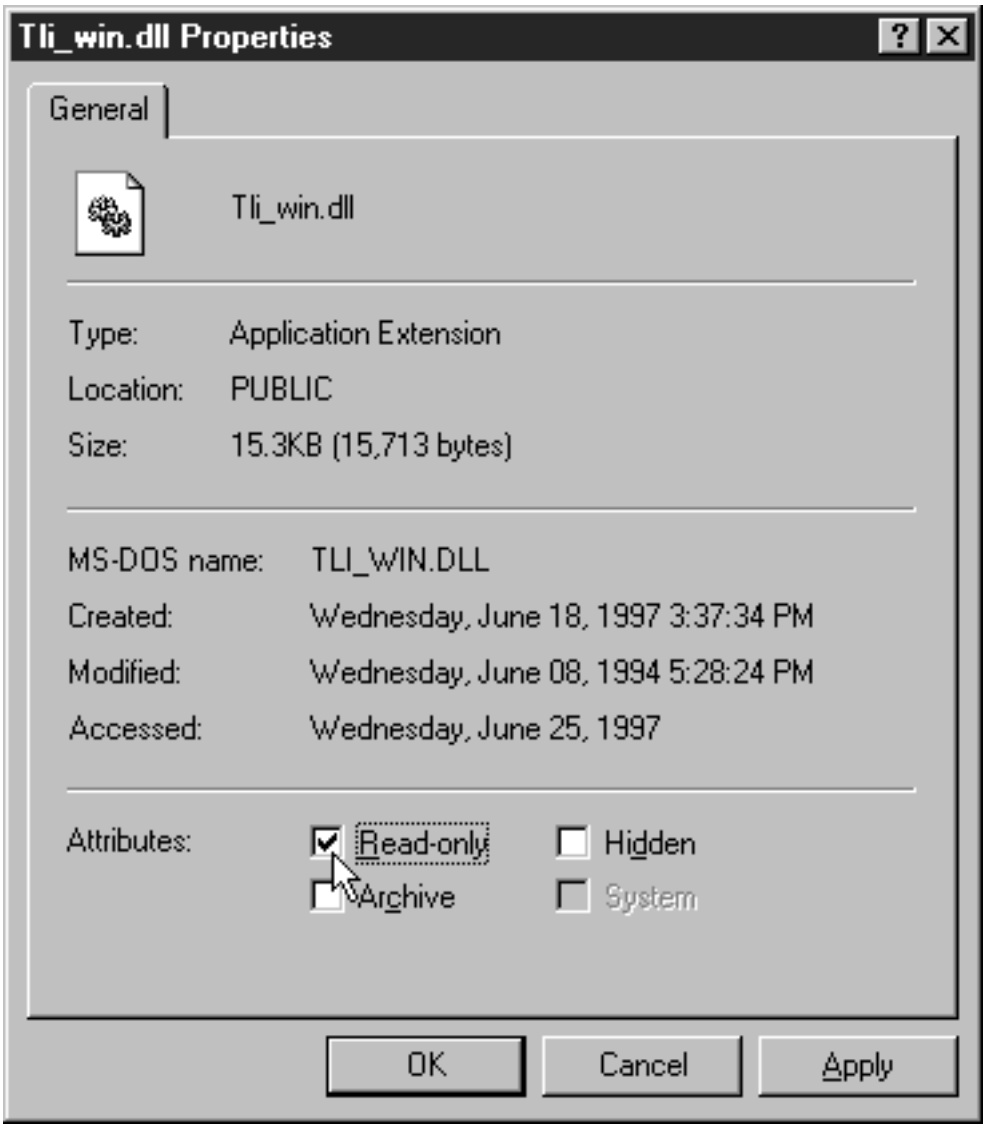


Figure 93. File Properties

3. Check on the **Read-only** check box in the attributes from the bottom of the dialog.
4. Click on **OK** to save the changes made to the file attributes.

In our case we had to check and change the attributes of the files listed below.

- \SYSTEM
  - BSTART.NCF
  - BSTOP.NCF
  - BSPXCOM.NLM

  - BSPXSTUB.NLM
  - RSPXSTUB.NLM
  - BROUTER.NLM
  - BTRIEVE.NLM
  - BREBUILD.NLM
  - BTIMSG.NLM
  - BDROUTER.NLM
  - BSETUP.NLM
  - BDIRECT.NLM
  - BUTIL.NLM
  - BTRMON.NLM
- \BTI\NETWARE\SYSTEM
  - AFTER311.NLM
  - A3112.NLM
  - NWSNUT.NLM
- \BTI\NETWARE\DOC
  - README.TXT
  - BTICFG.TXT
  - BTIINI.WRI
- \BTI\NETWARE\DEMODATA
  - UPPER.ALT
- \BTI\NETWARE\WIN\BIN
  - WBTICOMM.DLL
  - WBTRCALL.DLL
  - WBTRVRES.DLL
  - WBROLL.EXE
  - WBROLLRS.DLL
  - DBU_UI.DLL
  - NWLOCALE.DLL
  - TLI_WIN.DLL
  - TLI_SPX.DLL
  - BTI.INI
  - WBTRTHNK.DLL
- \BTI\NETWARE\WINNT\BIN
  - WBTRV32.DLL
  - NTBTICOM.DLL
- \BTI\NETWARE\DOS\BIN

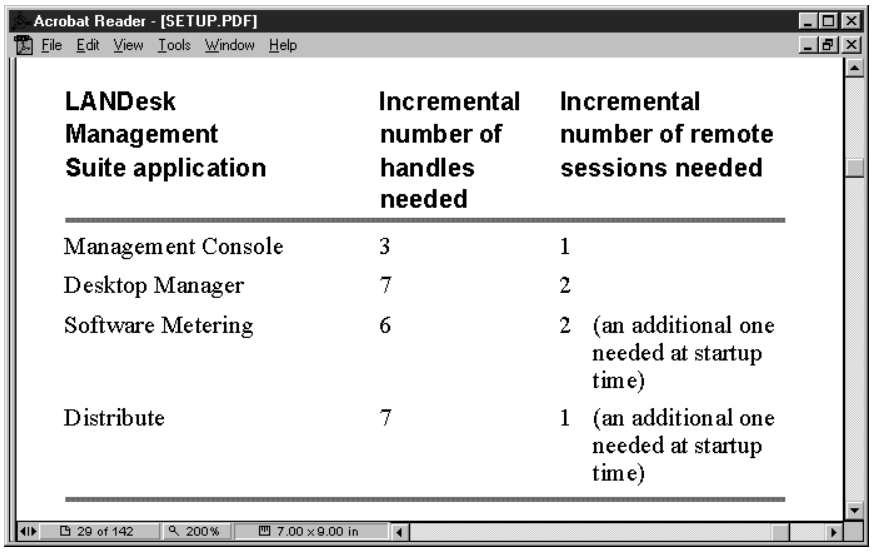
  - BTI.CFG
  - BREQUEST.EXE
  - BREQUEST.MSG
  - BROLLFWD.EXE
  - BROLLFWD.MSG
  - BREQUTIL.EXE
  - BREQUTIL.MSG
  - BREQNT.EXE
  - BREQNT.MSG
- \BTI\NETWARE\OS2\BIN
  - BTICOMM.DLL
  - BTRCALLS.DLL
  - PBROLL.EXE
  - PBTRVRES.DLL
  - NWLOCALE.DLL
  - OS2NWBRQ.DLL
  - MKDESVCS.DLL
  - MKDELINK.DLL

Btrieve 6.15 can now be installed without the warning `Unable to write to destination` appearing.

2.4.4 Btrieve Configuration to Accommodate LANDesk Management Suite

To properly operate the LANDesk Management Suite you will need to change some of the Btrieve parameters.

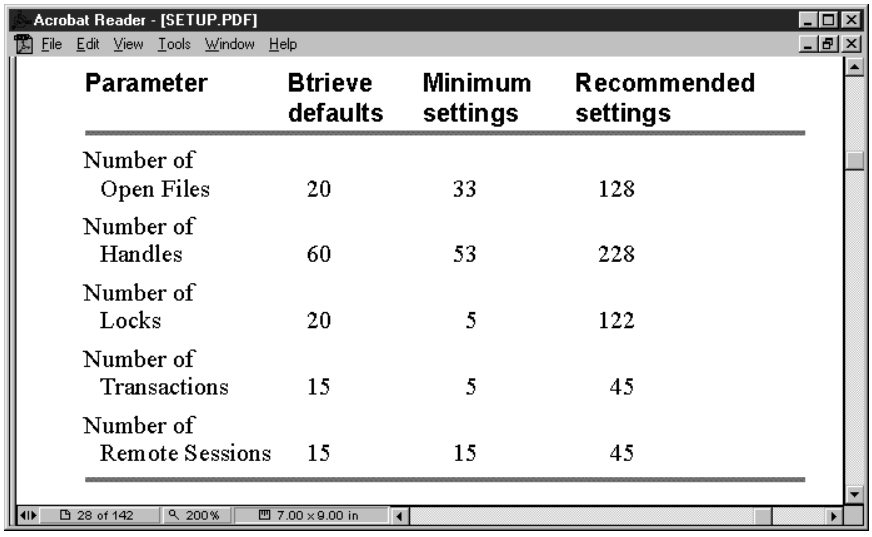
Figure 95 on page 80 lists the parameters you should change and the values you should set. Before you make any changes, review Figure 94 on page 80.



LANDesk Management Suite application	Incremental number of handles needed	Incremental number of remote sessions needed
Management Console	3	1
Desktop Manager	7	2
Software Metering	6	2 (an additional one needed at startup time)
Distribute	7	1 (an additional one needed at startup time)

Figure 94. Things to Consider When Adjusting Btrieve's Parameters

These settings are for the Management Suite only. You should add them to your current Btrieve requirements. The minimum settings are the minimum that Management Suite can run on. However, you may encounter performance problems. Management Suite runs with fewer problems if you use the recommended settings.



Parameter	Btrieve defaults	Minimum settings	Recommended settings
Number of Open Files	20	33	128
Number of Handles	60	53	228
Number of Locks	20	5	122
Number of Transactions	15	5	45
Number of Remote Sessions	15	15	45

Figure 95. Defining Btrieve Parameter to Work with LANDesk Management Suite

Increasing the values consumes very few server resources, but it greatly increases the reliability of the Management Suite. The other Btrieve parameters can be left at the default values.

2.4.4.1 Configuring BSTART.NCF

The following steps should be taken to configure the bstart.ncf file:

1. From the NetWare Server or an rconsole session, load the install NLM.
2. Choose the NCF files options (create/edit server startup files).
3. Edit the autoexec.ncf file.

4. Find and REM out the LD_AUTO.NCF statement.
5. Save and exit.
6. Restart the server. To do this go to the NetWare console and enter `down` then `restart server`.

   This will restart the server with no Btrieve NLMs, provided you are only loading Btrieve for LDMS.
7. Load BSETUP.NLM.
8. Change the Btrieve defaults to the appropriate settings.

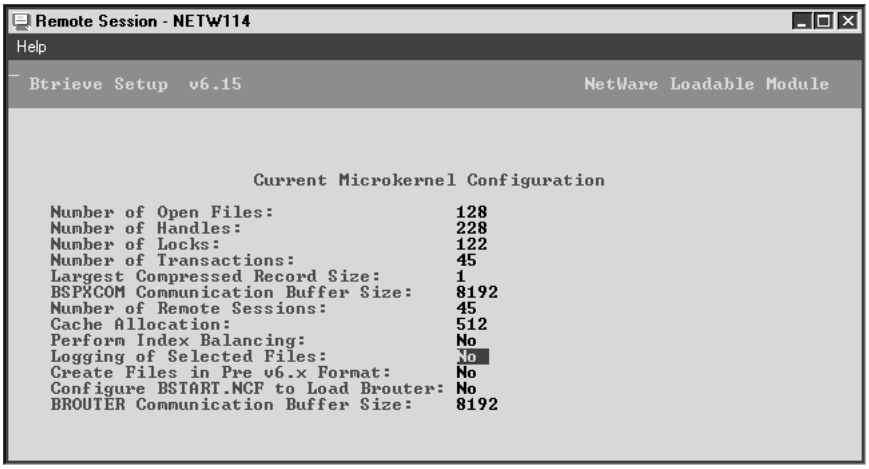


Figure 96. Configuration Panel on the NetWare Server

9. Exit BSETUP.NLM and save the settings.
10. From the NetWare Server or an rconsole session, load install.
11. Choose the NCF file options (create/edit server startup files).
12. Edit the autoexec.ncf file.
13. Find the statement REM LD_AUTO.NCF and remove the REM.
14. Save and exit.
15. Load the Btrieve NLMs using BSTART.
16. Load the Management Suite NLMs by entering the following command at the server console: `LD_AUTO`.

2.4.5 Applying the Btrieve 615.440 Update

There is some maintenance that needs to be applyed to Btrieve. The process to do that follows:

1. Copy BTRNW615.EXE (a self-extracting zip file) to the directory that contains copies of the files to be updated on the NetWare file server (where the product was originally installed) for example, \SYSTEM.

   Note: When you install Btrieve 6.15, you may see an error during file decompression stating `Unable to write to destination`. This prompt is generated when the existing Btrieve files are marked read-only.

   To fix this problem, change the Btrieve files to read-write. From the command line, you can use the attrib command or follow steps 1 to 4 (see 2.4.3, “Change

Btrieve Files from Read-Only to Normal" on page 76). You must do this to every file listed below that will be updated or replaced. This change allows the installation program to overwrite the Btrieve files and update the version.

Here is a list of files that will be either updated or replaced. For all files that are updated, a valid copy of the file must exist or the update will fail:

- SYSTEM directory
  - BTRIEVE.NLM - Updated
  - BSPXCOM.NLM - Updated
  - BROUTER.NLM - Replaced
  - BDROUTER.NLM - Replaced
- WIN\BIN directory
  - WBTICOMM.DLL - Updated
  - WBTRCALL.DLL - Replaced
  - WBTRVRES.DLL - Replaced
  - DBU_UI.DLL - Replaced
- OS2\BIN directory
  - BTICOMM.DLL - Updated
  - BTRCALLS.DLL - Replaced
  - OS2NWBRQ.DLL - Replaced
  - MKDELINK.DLL - Replaced
  - MKDESVCS.DLL - Replaced
- WIN32\BIN directory
  - NTBTICOM.DLL - Replaced with W32BTICM.DLL
  - W32BTICM.DLL - Updated
  - WBTRTHNK.DLL - Replaced
  - WBTRV32.DLL - Replaced
  - W16NR.DLL - Replaced
  - W32NR.DLL - Replaced
  - W32RQCFG.EXE - Added
- BIN directory
  - BREQUEST.EXE - Replaced
  - BREQUEST.MSG - Replaced
  - BREQNT.EXE - Replaced
  - BREQNT.MSG - Replaced

Except for the files in the WIN32\BIN directory, all of the files to be updated must exist in the directories specified above, or the update will fail.

2. Run BTRNW615.EXE to extract the batch and patch update files.

```
PKSFX (R)   FAST!   Self Extract Utility   Version 2.04g  02-01-93
Copr. 1989-1993 PKWARE Inc. All Rights Reserved. Shareware version
PKSFX Reg. U.S. Pat. and Tm. Off.

Searching EXE: F:/SYSTEM/BTRNW615.EXE
  Inflating: V6155.RTP
  Inflating: V6151O.RTP
  Inflating: V6152O.RTP
  Inflating: V6155O.RTP
  Inflating: V615100.RTP
  Inflating: V615U.RTP
  Inflating: BTRREQNW.RTP
  Inflating: BTRNW.EXE
  Inflating: PATBTRNW.BAT
  Inflating: PATCH.EXE
  Inflating: README.TXT
```

Figure 97. Btrieve Update Utility

3. From a DOS command line, run PATBTRNW v615x, a batch command, where x is:
   - 5 to update a 5-user version of Btrieve
   - 10 to update a 10-user version of Btrieve
   - 20 to update a 20-user version of Btrieve
   - 50 to update a 50-user version of Btrieve
   - 100 to update a 100-user version of Btrieve
   - U to update an unlimited user count

   Note: If you are not sure what the MicroKernel user count is, load Btrieve and use the modules command from the NetWare file server console to display module information. The user count is displayed for the module BTRIEVE.NLM.
4. After the batch file completes, check the v615x.LST output file, where x is one of the values listed above. Look at this file for the patch update status. If you see the following status message, you have attempted to apply the patch update against an invalid file:

   ```
   Error ept0036: Old File not found. However, a file of the
   same name was found.
   No update done since file contents do not match.
   ```

   Check to be sure that you have the files as listed in 2.4.5, “Applying the Btrieve 615.440 Update” on page 81. If these files are not present, this update will not successfully complete.

```
F:\>patbtrnw v6155
Updating Btrieve for NetWare v6.15 to current version.
Output is redirected to v6155.lst.
Please wait.  This may take a few minutes...
Directory already exists
Updates applied successfully.  See v6155.lst for update status.
```

Figure 98. Successful Update Panel

After the patch update has been successfully applied, you may delete all of the files listed in the following list:

- PATBTRNW.BAT

- V6155.RTP
- V61510.RTP
- V61520.RTP
- V61550.RTP
- V615100.RTP
- V615U.RTP
- BTRREQNW.RTP
- BTRNW.EXE
- PATCH.EXE
- README.TXT

Also delete the v615x.LST file created during the patch update process, where x is:

- 5 to update a 5-user version of Btrieve
- 10 to update a 10-user version of Btrieve
- 20 to update a 20-user version of Btrieve
- 50 to update a 50-user version of Btrieve
- 100 to update a 100-user version of Btrieve
- u to update an unlimited user count

2.5 Installation and Configuration of LANDesk

From your management workstation, log in to your NetWare management server (not into an NDS) and be sure you have admin or supervisor permission. Point to the LANDesk Management Suite 2.51 (LDMS 2.51) CD or copy the code to a hard drive. Open the DISK1 directory and run setup.exe.

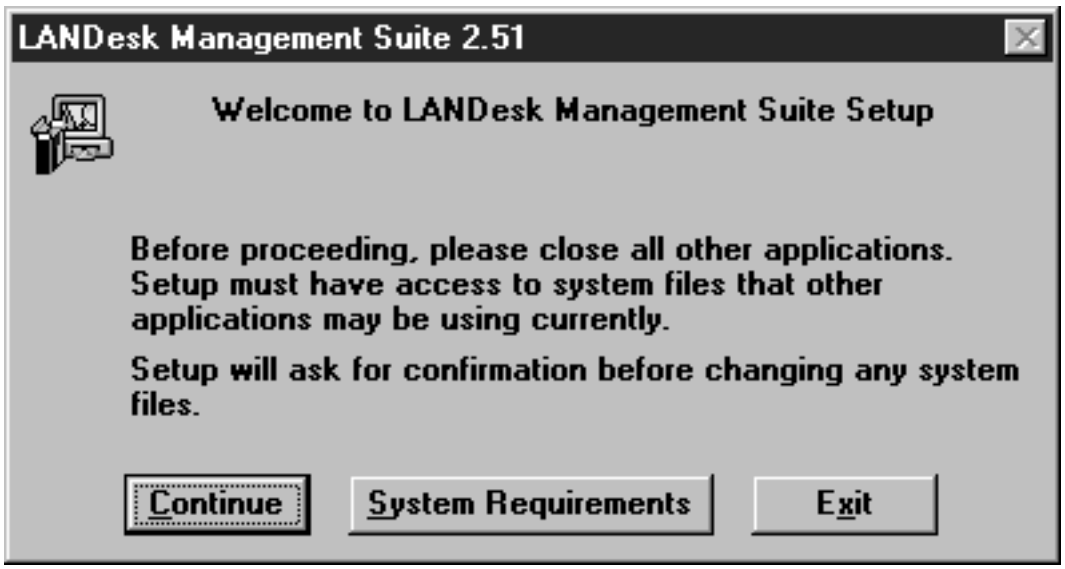


Figure 99. Installation Reminder

This means all unnecessary and or similar programs on the management workstation. If you are already using LANDesk, you must unload the NLMs running on your 2.3.1, “Management Server” on page 73. If you are running Btrieve, you should run bstop at 2.3.1, “Management Server” on page 73.

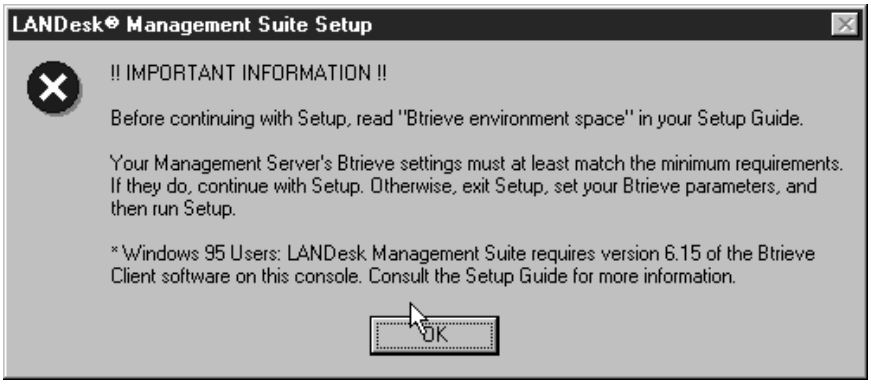


Figure 100. Btrieve Information

2.5.1 Indicating an Installation Target

During the installation of LANDesk Management Suite (LDMS), for use with Tivoli LAN Access, the first piece of information you have to provide to the setup program is the target directory for the code. You must then choose a server running ether NetWare 3.1x or 4.x. They can not be utilizing a NetWare Directory Services (NDS) tree. The name of the NetWare server that we used for this project was NETW114.

Windows NT servers can only be managed servers. This means you can expand your management domain to include Windows NT servers. Once this is done all the Windows NT Server's clients can be managed by LDMS. Windows NT Servers can not be a managed server or a management workstation.

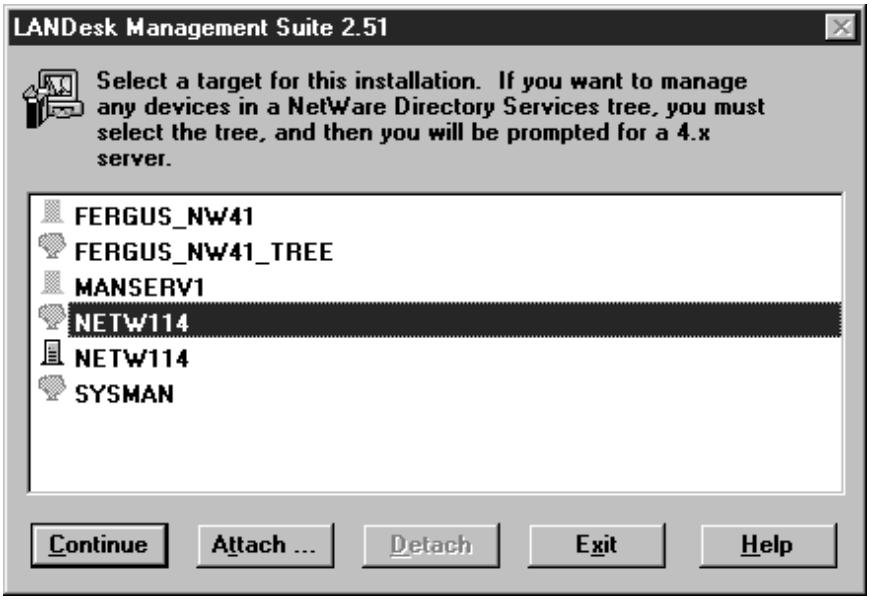


Figure 101. Indicate an Installation Target

You need to be logged in as supervisor or have administrator permissions when setting up Tivoli LAN Access. Assuming you are logged in as one of those, if you get Figure 102 on page 86 you must click on **Yes**.

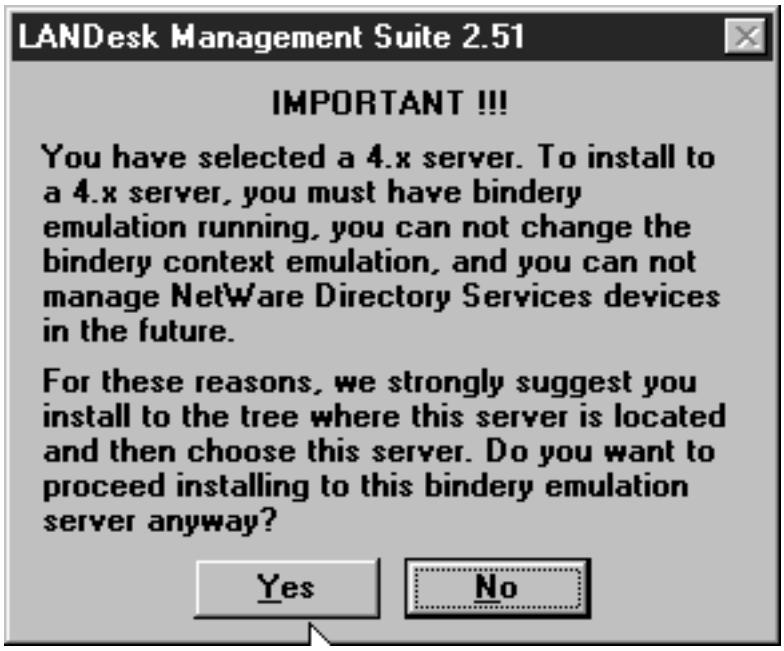


Figure 102. NDS Information

2.5.1.1 Installing to a Bindery Server

Bindery servers include NetWare 3.1x servers and NetWare 4.x servers running with bindery emulation on. When you install to a bindery server, your default domain includes the server and any clients that log in to that server. When you install to a bindery server, you can only expand your domain to include other bindery servers and their clients. This includes Windows NT Servers and their clients.

2.5.1.2 Verify Your Installation Paths

After choosing the target you want to install to, based on that target, you are prompted to indicate specific installation paths. You can accept the defaults or you can specify other directories.

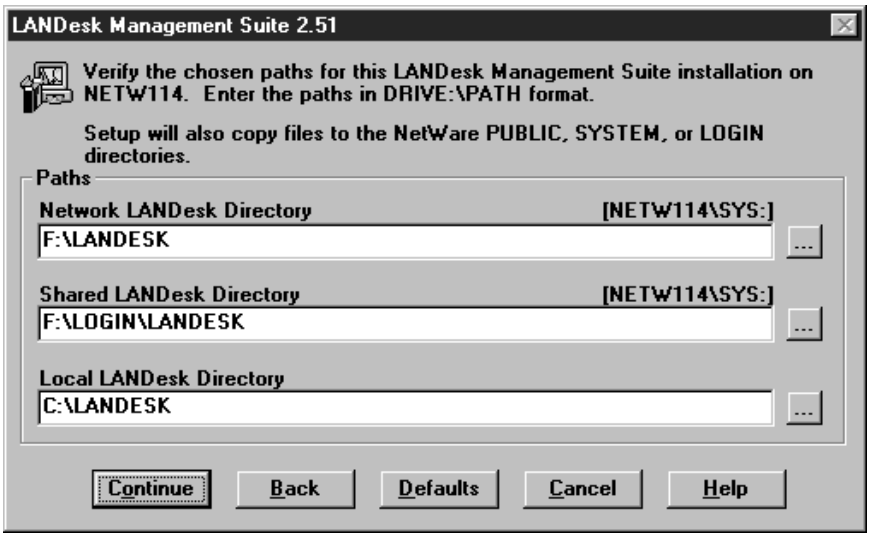


Figure 103. Verifying the Installation Paths

The shared LANDesk directory must be installed on the SYS volume of the server. Other LANDesk directories can be installed in other volumes.

The amount of drive space required depends on whether or not you choose to install all of the Management Suites tools. More details on the management tools can be found in 2.5.2, “Management Suite Tools” on page 89.

2.5.1.3 Network LANDesk Directory

Setup asks you to indicate a network directory for LDMS's largest group of files. This directory must be accessible to LDMS administrators but does not need to be available to managed clients. Anyone with write access to this directory can run the Management Console. You will want to restrict the users that have access to this directory. To help you manage who can access the Management Console, setup creates a LANDESKADMINGROUP NetWare user group. This group is given full rights to the network LANDesk directory.

After a full installation this directory (SYS:LANDESK, by default) contains about 60 MB of executables and data.

2.5.1.4 Shared LANDesk Directory

Setup places a group of files in SYS:LANDESK. This shared directory contains executable and help files for the client elements, Network Printer Manager, utilities and TSRs that LDMS requires each client workstation to access.

After a full installation this directory (SYS:LOGIN\LANDESK, by default) contains about 12 MB.

2.5.1.5 Local LANDesk Directory

The directory for Performance Monitor log files no longer has to be a local directory. Previous versions of LANDesk Manager required it to be a local directory. However, if you make this a network directory, think about the increased network traffic.

After a full installation this directory (C:\LANDesk, by default) contains about 3.5 MB.

Note: Traffic Monitor and Performance Monitor require data to be collected from the network via a network adapter or interface card with an ODI driver capable of operating in promiscuous mode. Set up a Software Probe station on each segment you want to monitor. That station also requires an ODI driver capable of operating in promiscuous mode. To collect data using the LANDesk management workstation's NIC also requires an ODI driver capable of operating in promiscuous mode. This data is collected and sent to the management server. If you chose to send it to a remote drive, you will just double your network traffic.

2.5.1.6 SYS:LOGIN Directory

Setup places two files in the sys:login directory. You are not prompted for a path to this directory during setup.

2.5.1.7 SYS:SYSTEM Directory

Setup places LDMS's NLM files in this directory. You are not prompted for a path to this directory during setup.

After a full installation this directory (SYS:SYSTEM, by default) is enlarged by about 3 MB.

2.5.1.8 SYS:PUBLIC Directory

Setup places executable and data files required by CLNTCFG.EXE and Desktop Manager in this directory. You are not prompted for a path to this directory.

Setup adds about 1 MB to this directory (SYS:PUBLIC, by default).

If LANDesk detects a previous installation of LANDesk or if you had a partial install of this version of LANDesk, you will get a pop-up window similar to the one in Figure 104.

If you are going to just add a tool you must run setup.exe again. Immediately after the first setup completes this will go through the same set of panels and bring up Figure 105 on page 89.

Figure 104. Updating

If you start LANDesk before you run setup again, you will get Figure 104 again.

Figure 105. Adding a Tool

Note: If you get the window shown in Figure 105 and you click on **Overwrite**, you will lose all your management domain information. It will be as if you just installed from the beginning. If you think the code needs updating, run LANDesk, then run setup again so you get to the point shown in Figure 104 on page 88. This will allow you to update the code without losing or changing your domain settings.

2.5.2 Management Suite Tools

Choose which of the management tools to install. The tools are grouped into four categories:

1. Workstation management tools - Desktop Manager, Distribute, Software Metering, Desktop Remote
2. Server management tools - Server Manager, Server Status
3. Wire management tools - Performance Monitor, Traffic Monitor, Software Probe
4. Network services tools - Network Printer Manager, Queue Monitor, Virus Scan

Figure 106 on page 90 allows you to select or de-select entire categories for installation. For a more detailed listing of tools in each category just click on **More Info** beside each category (see Figure 107 on page 90 through Figure 110 on page 93).

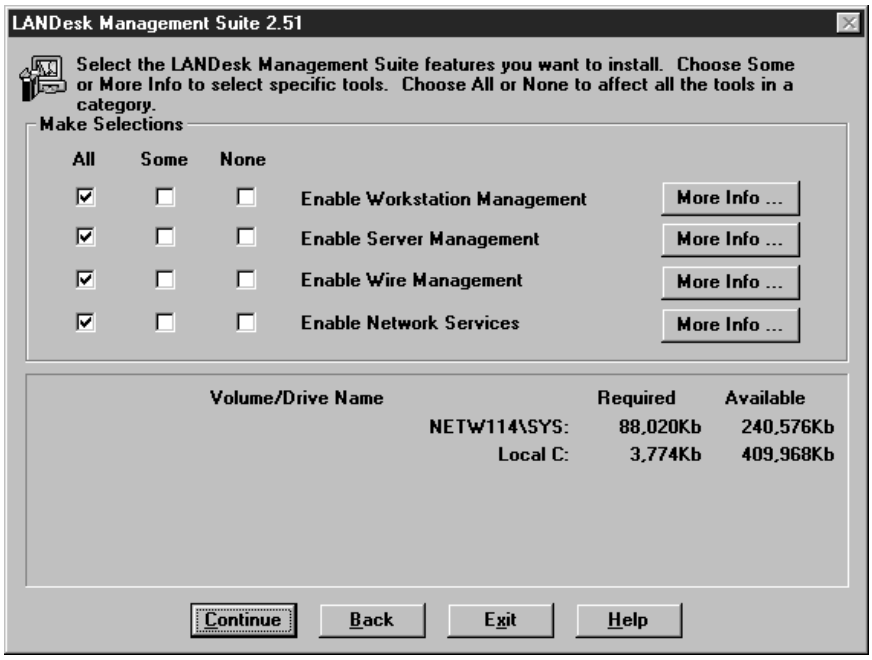


Figure 106. Category Selection

You can get a better idea of what each tool will do by clicking on **View**. This will allow you to make the choice of whether to install the tool or not. It will also show what files will be changed.

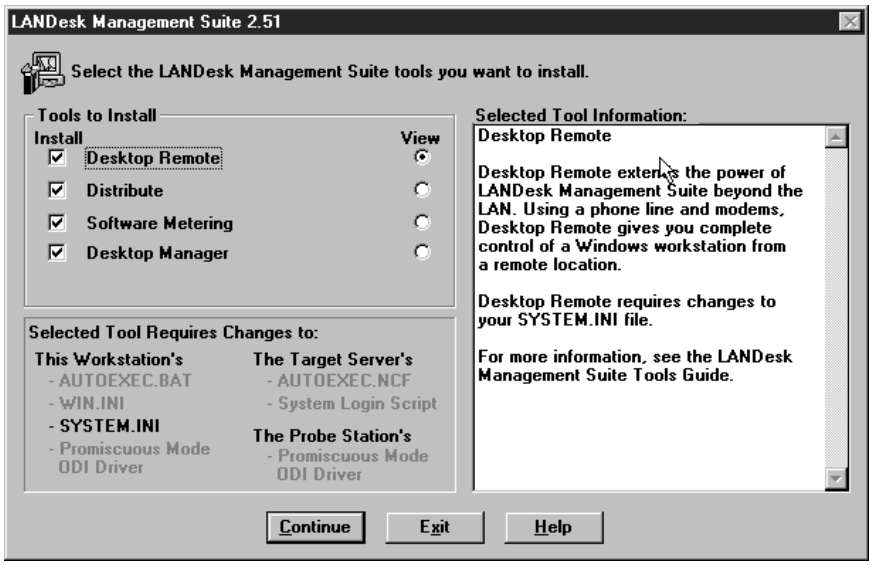


Figure 107. Workstation Management

- Desktop Remote - Enables you to control Windows workstations at remote sites that do not have network connections using phone lines and modems.
- Distribute - Automates the distribution and installation of Windows or DOS-based software applications and file collections across the network to workstations. Distribute creates packages containing the data and commands necessary to install software.

- Software Metering - Provides immediate information on license usage and availability. You can meter applications executed from NetWare 3.1x and 4.x and from Windows NT servers. You can meter local drive execution for Windows, Windows for Workgroups, and Windows 95 workstations. DOS application metering is minimally supported. Software Metering can also monitor single or suite applications across multiple servers.
- Desktop Manager - Integrates remote control with inventory gathering and reporting. Desktop Manager helps you manage your network by enabling you to do the following:
  - Remote control workstations and servers
  - Manage system configuration files
  - View real-time information for workstations and servers
  - Perform network diagnostics
  - Create inventory reports

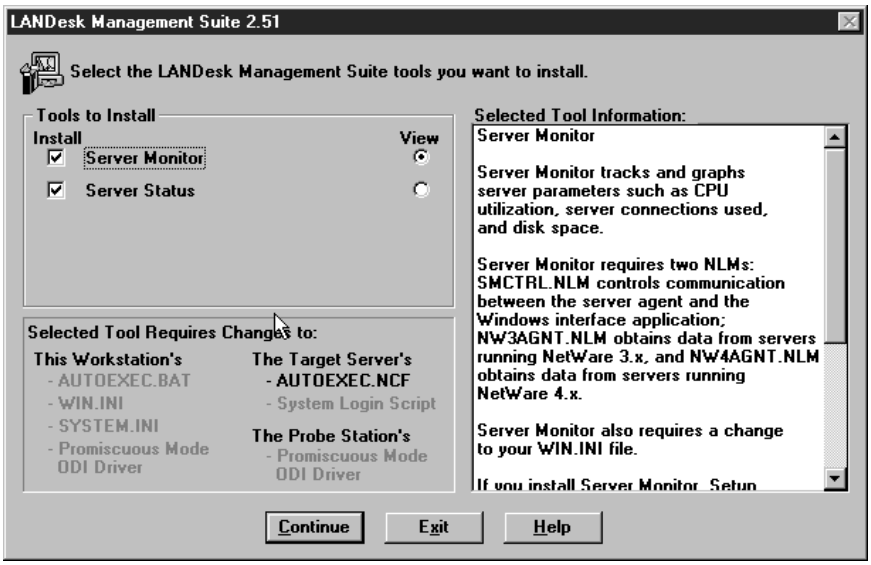


Figure 108. Server Management

- Server Manager is a server management solution that gives you the ability to monitor critical server parameters on both NetWare servers and Windows NT systems. With Server Manager you can:
  - View in real-time more than 100 parameters on a NetWare 3.1x or 4.x server.
  - View in real-time more than 200 parameters on a Windows NT computer.
  - Set thresholds on parameters that can notify you of failures or impending failures.
- Server Status watches the binderies of up to eight servers you select and notifies you if any become unavailable.

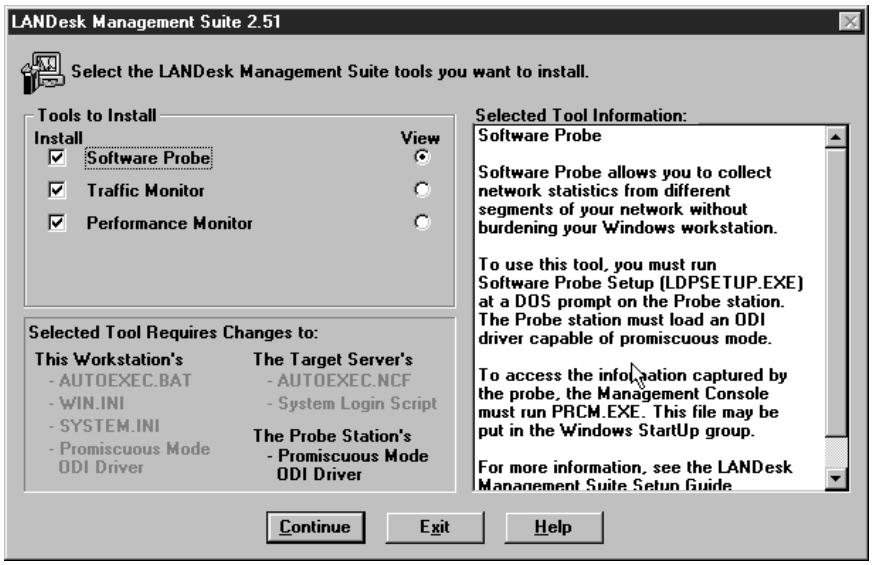


Figure 109. Wire Management

- Software Probe runs on a dedicated DOS workstation, collecting network traffic statistics for probe-enabled applications such as Performance Monitor and Traffic Monitor. Use Software Probe to:
  - View network statistics from other segments of your network.
  - Collect persistent Performance Monitor statistics so they can be displayed at a later time.
  - Reduce overhead on your management workstation.
- Traffic Monitor provides you with easy-to-use traffic monitoring tools. Each window displays real-time statistics such as total packets per second (packet rate), the percent capacity used (% utilization) and the number of errors per second (error rate). The Traffic Monitors Station Log also displays packet, byte, and error counts for up to 512 stations.
- Performance Monitor tracks network application traffic to provide statistical information. It enables you to determine which applications are running on the network, which stations are accessing the applications, and how often they are run.

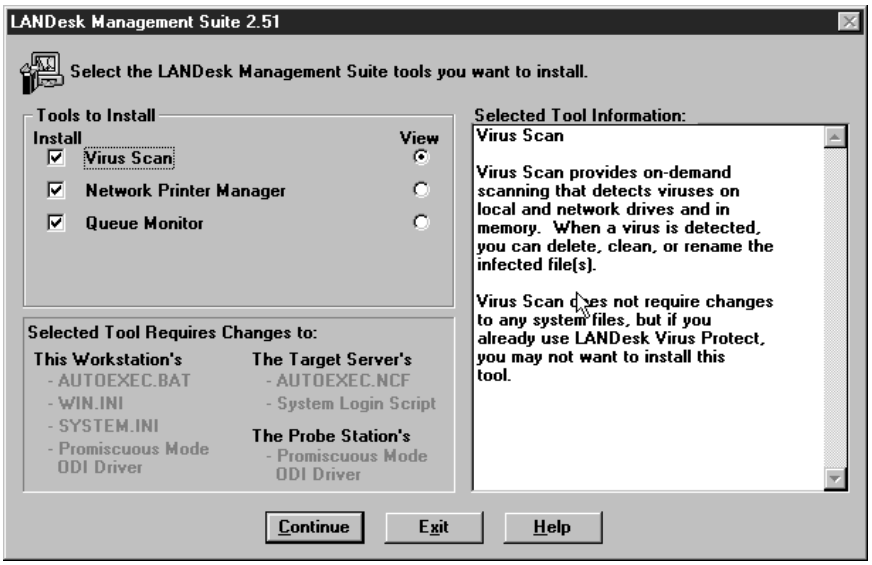


Figure 110. Network Services

- WProtect for Windows WPROTECT.EXE and Virus Scan for DOS VSCAND.EXE are on-demand scans that detect viruses on local drives, network drives, in critical disk areas, and in memory.
- Network Printer Manager is a tool that helps you control network printing. Use it to diagnose and solve network printing problems by:
  - Configuring network printing parameters
  - Monitoring network printer status
  - Managing workstation printing
- Queue Monitor is a tool that helps you control network print queues. Use it to:
  - Monitor print queues and print jobs
  - Manage network print queues
  - Manipulate queued print jobs

For our scenarios we installed all the tools in all of the categories.

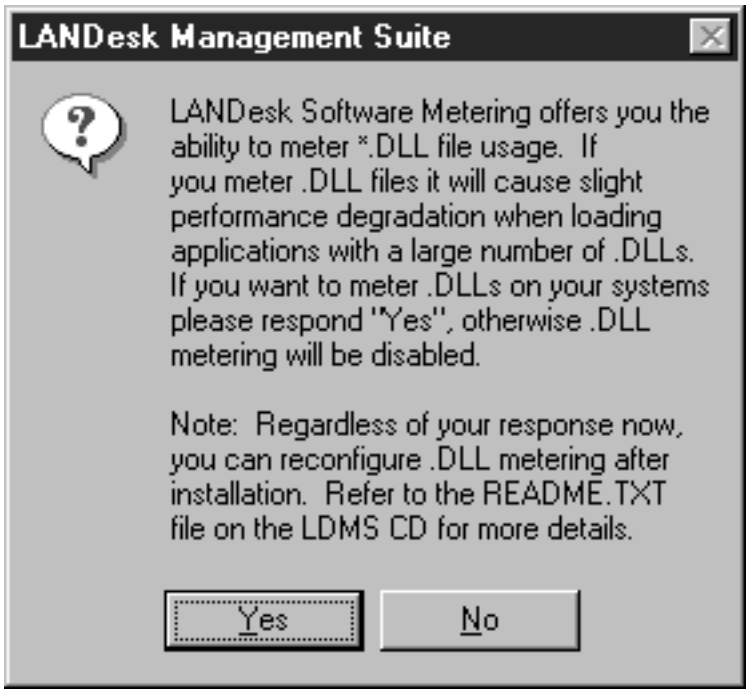


Figure 111. DLL Metering Confirmation

After selecting all of the tools in all of the categories to be installed, Figure 111 is displayed. After further investigation into metering DLLs we decided not to do software metering because of the performance degradation, and Tivoli LAN Access doesn't use this function of LANDesk.

2.5.3 System File Changes

Figure 112 on page 95 shows you how you can view the changes that LDMS will make to your system files. The check boxes must be selected to have changes made to a file. Select the **View** radio button to view the changes an option makes. These changes are listed in the Modifications window pane. Choose the **Edit** button to edit the modifications listed in the Modifications window.

Setup will place commands into the appropriate login script affecting client workstations at login if they are members of the group LANDESKGROUP.

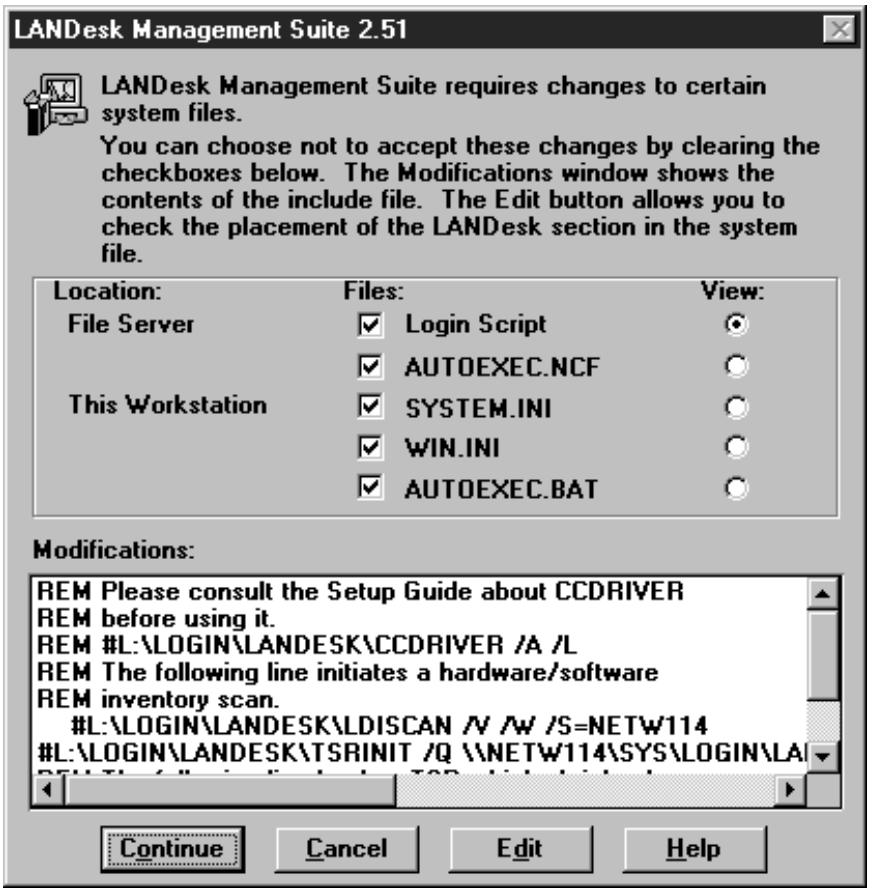


Figure 112. System File Changes

After clicking on **Continue** in Figure 112 LDMS builds your program groups and icons (see Figure 113 and Figure 114 on page 96).

Figure 113. LANDesk Management Suite Program Group

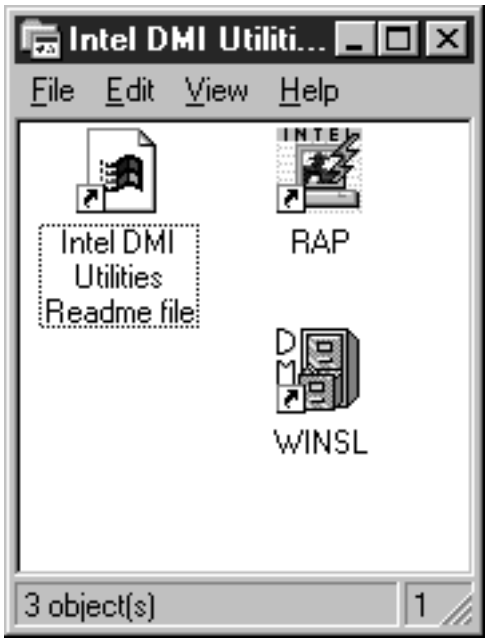


Figure 114. Intel DMI Utilities Program Group

As soon as the program groups are built, either Figure 115 or Figure 116 will pop up. The window you get depends on whether you were adding tools or re-installing, as shown in Figure 104 on page 88 or Figure 105 on page 89.

Figure 115. NLM Upgrade

Don't take the actions offered in Figure 115 or Figure 116 at this point in time; just write them down to perform later on.

Figure 116. Tool Addition

Attention

First make sure you have done the actions described in 2.4, “Installation and Configuration of Btrieve” on page 74. Do not skip the TO_DO.TXT file. Please click on the **To Do List** and follow the instructions.

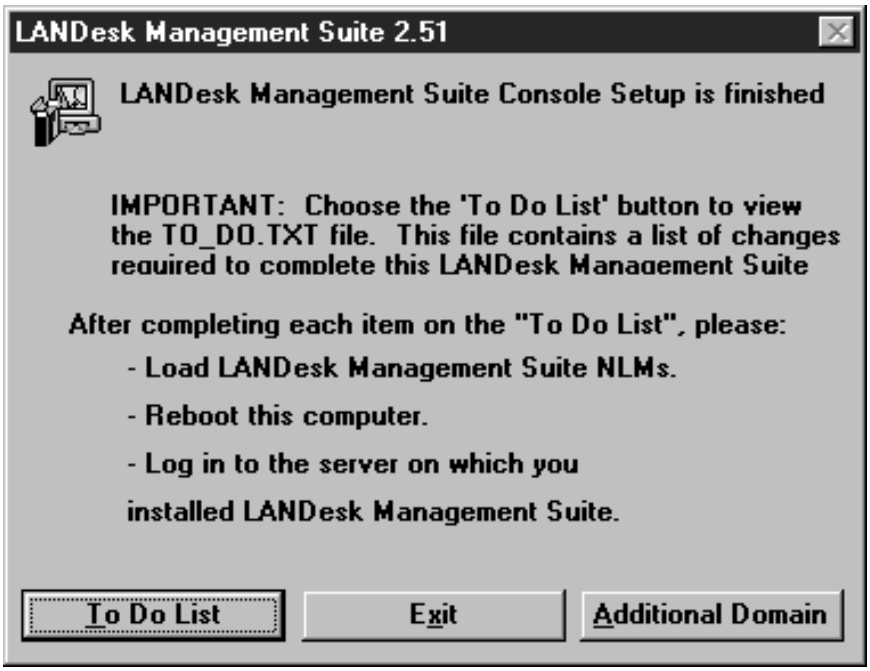


Figure 117. LANDesk Installation Completion

2.5.4 Things We Had to Do from the To Do List

After you have completed the items in the To Do List, use LD_AUTO.NCF to load the NLMs on your core server for future startups.

Since we used a Windows 95 management workstation we had to do the following:

1. Open the **Control Panel.**
2. Open the **Network** settings window.
3. Click on the **Configuration** tab.
4. Double-click on the **IPX/SPX Compatible Protocol** component.

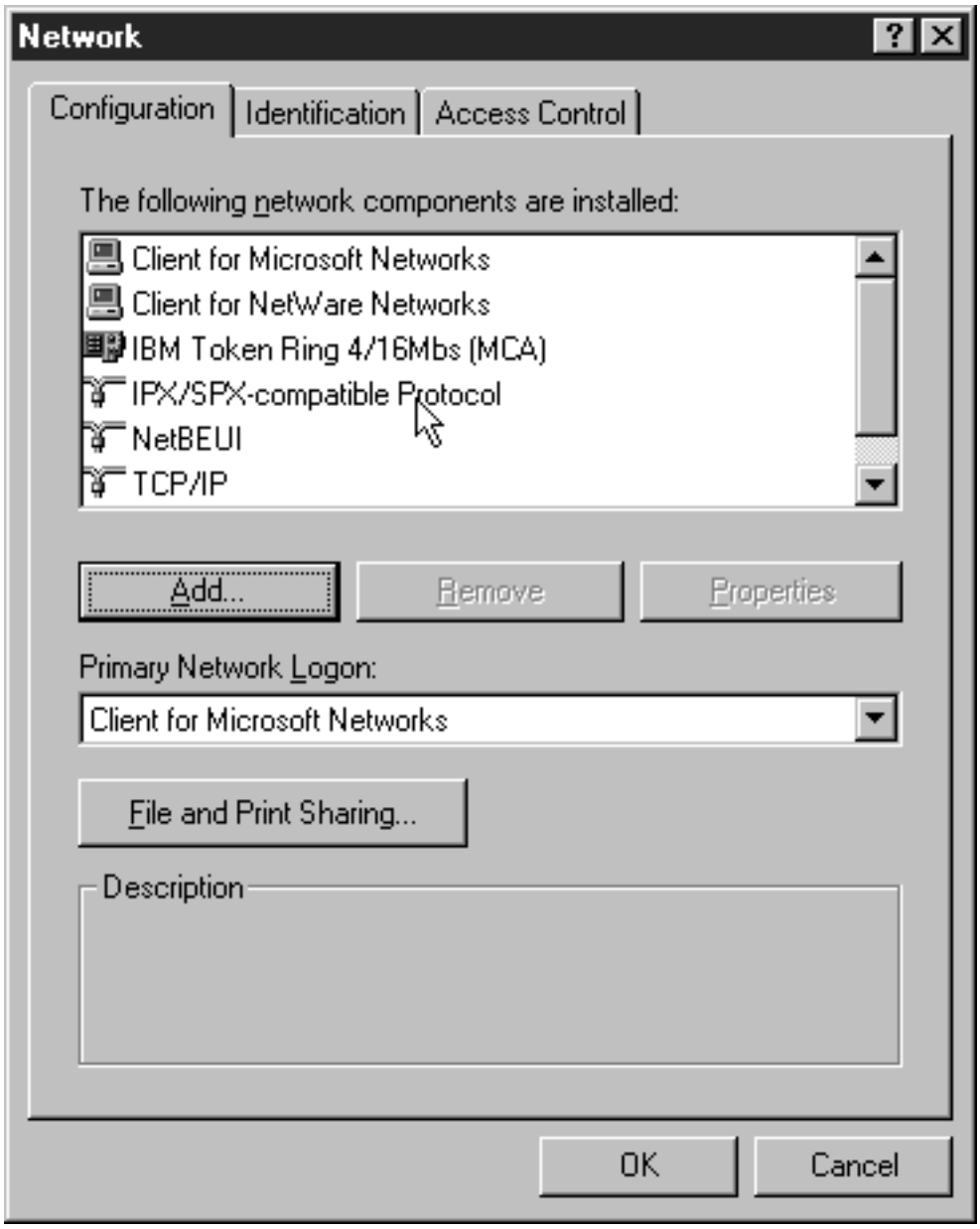


Figure 118. Network Configuration

5. Click on the **Advanced** tab.

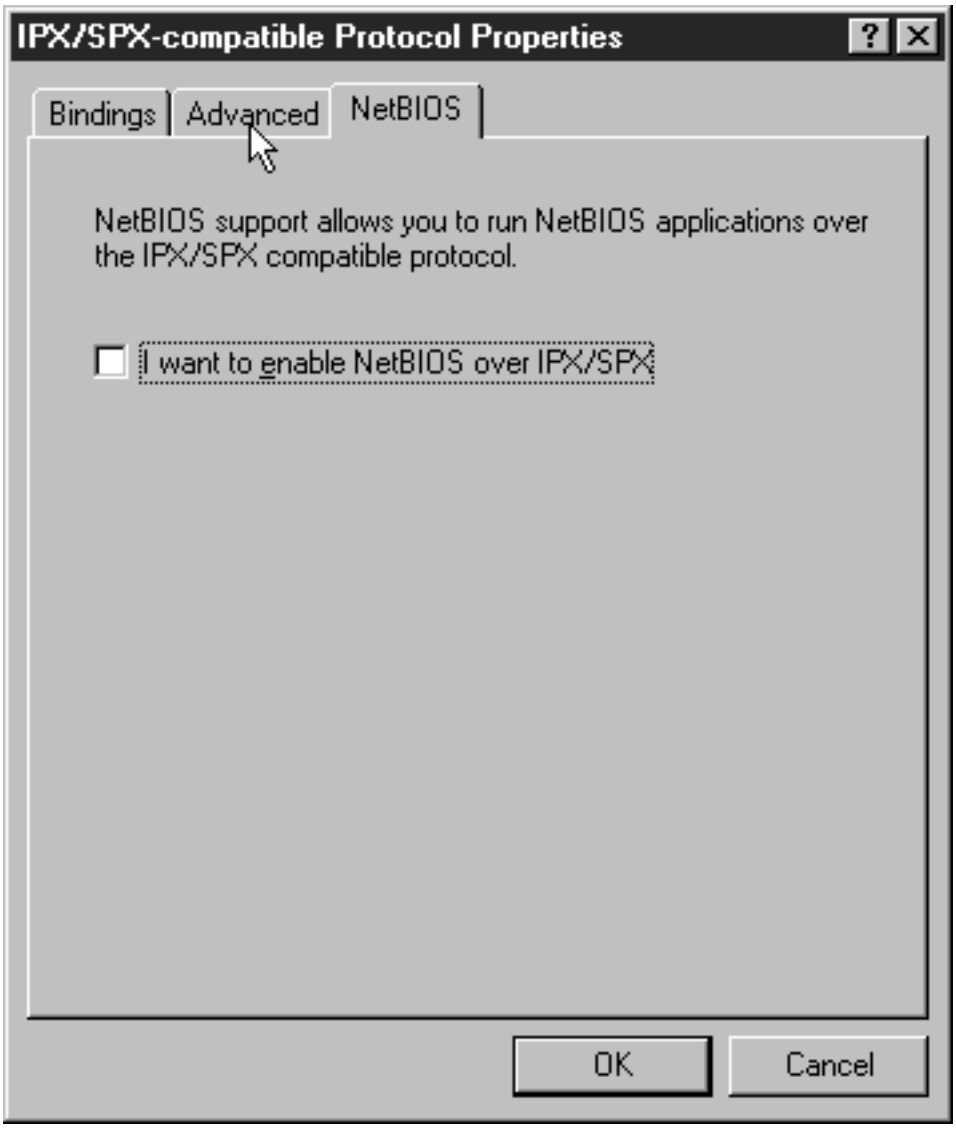


Figure 119. IPX/SPX-Compatible Protocol Properties

6. Select the **Maximum Connections** option.
7. Select the **Value** button.

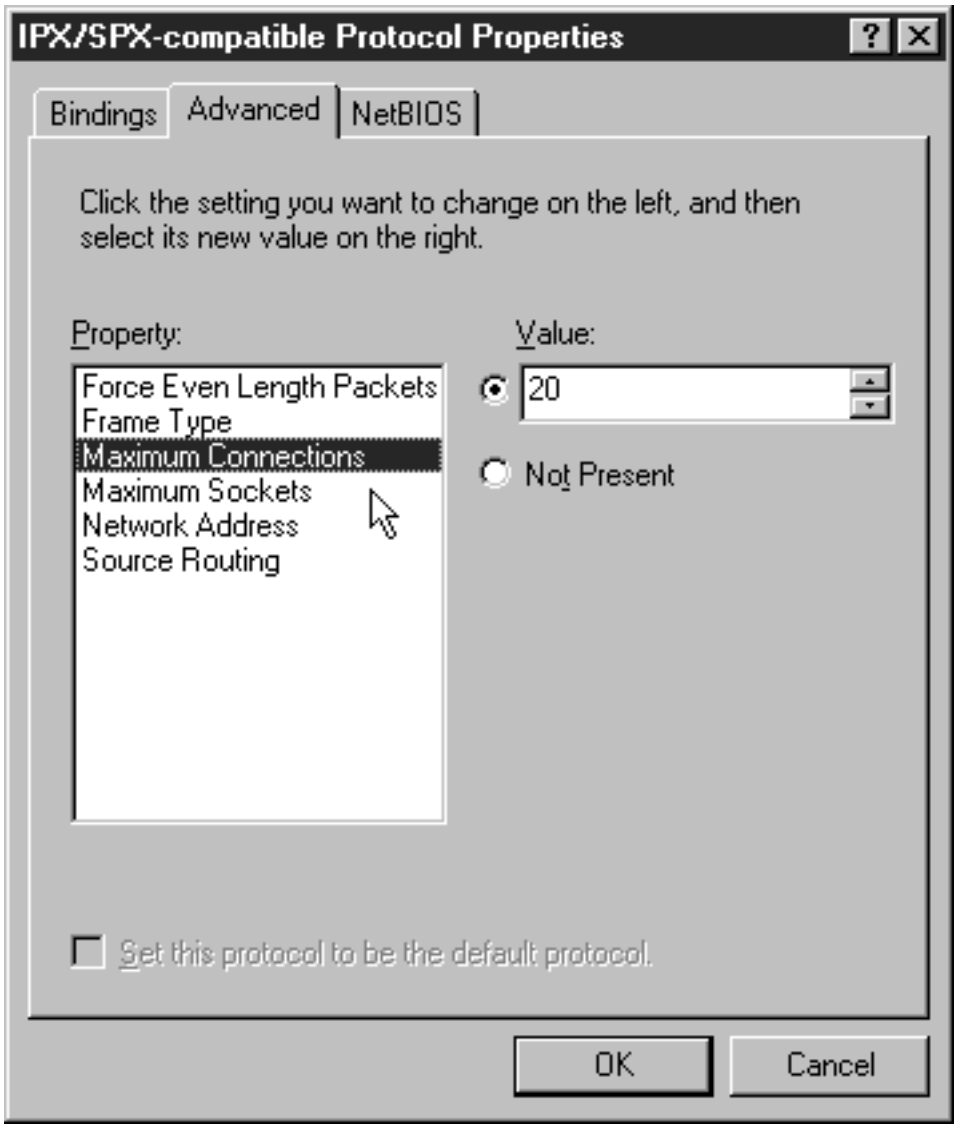


Figure 120. Advanced Maximum Connections Settings

a. Enter the Value as `20`.
b. Select the **Maximum Sockets** option.
c. Select the **Value** button.
d. Enter the Value as `30`.

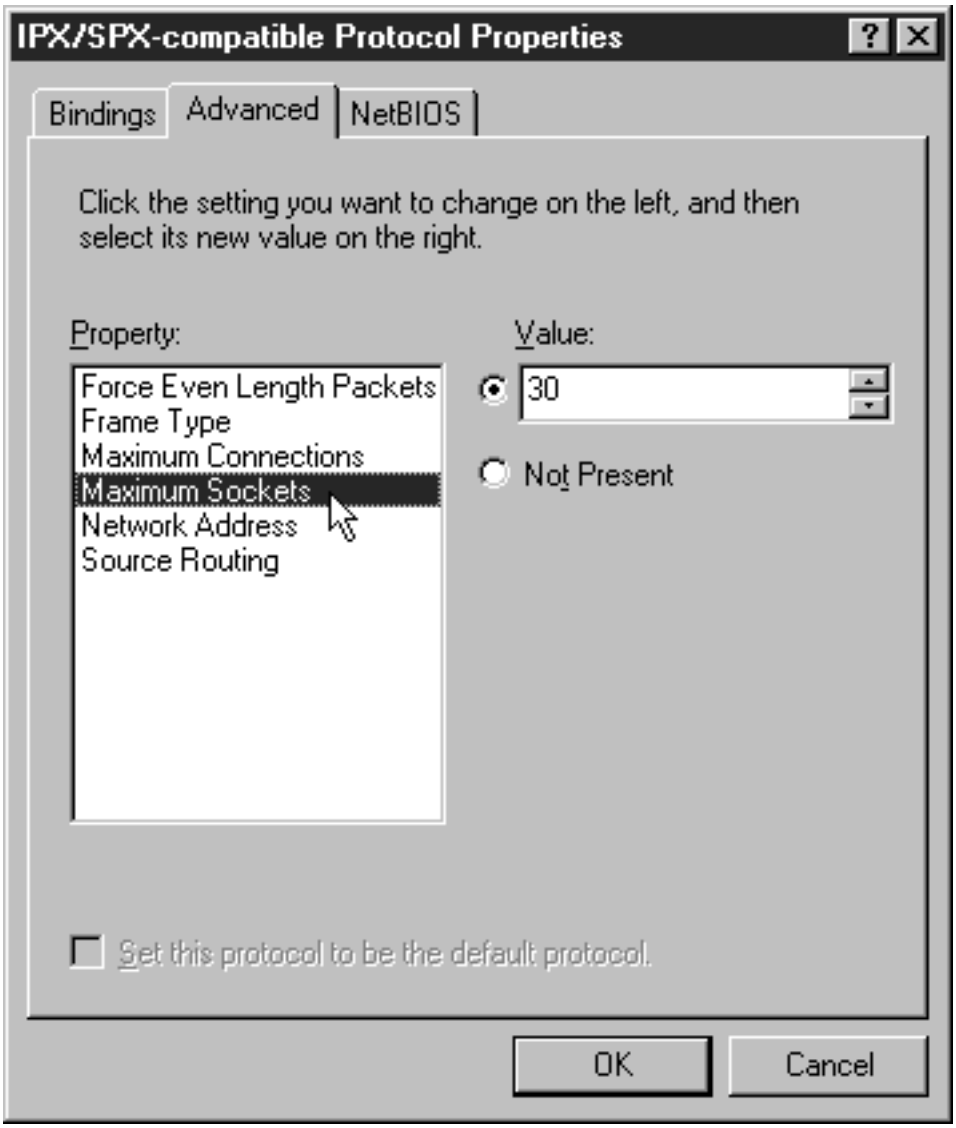


Figure 121. Advanced Maximum Sockets Settings

8. Click on **OK**. This will take you back to the Network panel.
9. Click on **OK** again and you will be prompted to reboot your system.
10. Click on **Yes** to reboot your system.

Note: For socket and connection values, the values suggested above on both the Windows 3.1x and Win95 systems are *minimum* values only. If you are using applications that make intensive use of sockets, you may need to increase these values.

Do not use EDIT.NLM to work with LDINIT.INI. LDINIT.INI contains some very long lines which EDIT.NLM will truncate, corrupting the file. You will have to use an editor on the NetWare client. All Windows 3.1 and 3.11 clients must have the *complete* WINUP9 fix (or later) installed. WINUP9.exe is an updated Windows client package for Novell NetWare. We got this file from Novell's Web page at http://support.novell.com.

Supervisor (NetWare 3.x) or Admin (NetWare 4.x) authority is required to administer the software distribution function. The default rights that are granted to the LANDESKADMINGROUP are not sufficient.

2.5.5 Check File Changes

Check the location of the following lines in your AUTOEXEC.NCF file on your LANDesk Management Server:

```
REM *** BEGIN LANDesk Management Suite 2.5 Section ***
REM LD_AUTO.NCF
REM *** END LANDesk Management Suite 2.5 Section ***
```

Make sure these lines do not conflict with your existing setup and NLM load commands. Uncomment the following line in your AUTOEXEC.NCF file:

```
LD_AUTO.NCF
```

After uncommenting the above line, either restart your file server, or at the server console, type the following command:

```
LD_AUTO.NCF
```

Check the location of the following lines in your SYSTEM LOGIN SCRIPT (on the LANDesk Management Server):

```
REM *** BEGIN LANDesk Management Suite 2.5 Section ***
IF MEMBER OF "LANDESKGROUP" THEN
#PUSHPOP CHKCONN=<servername>
include <UNC Path>LD_LOGIN.DAT
#PUSHPOP DELCONN=<servername>
END
REM *** END LANDesk Management Suite 2.5 Section ***
```

Make sure these lines come after you map search drives to the PUBLIC directory and any network Windows installations, but before the first EXIT statement.

Check the location of the following lines in your AUTOEXEC.BAT file:

```
REM *** BEGIN LANDesk Management Suite 2.5 Section ***
CALL C:\LD_AUTO.BAT
REM *** END LANDesk Management Suite 2.5 Section ***
```

Make sure these lines are executed after you have logged in to the network. If you do not log in using your AUTOEXEC.BAT file, you may need to place these lines in another file or manually load BREQUEST.EXE and set the DMIDIR environment variable after logging in. These changes *must* be made in your workstation configuration before you attempt to launch LDMS. If you do not load BREQUEST.EXE, LDMS will not work correctly. If you do not set the DMIDIR environment variable, you will get a DMI service layer error message when you launch Windows. The following lines should be in the [386Enh] section of your SYSTEM.INI file on your LANDesk management workstation:

```
device=VUSER.386
device=VMON.386
device=VDMID.386
device=VSHARE.386
VmonVirtualizeIRQs=no
VmonPacketHeap=5000
```

```
VmonFilterHeap=4096
TimerCriticalSection=10000
```

The following lines should be in your WIN.INI file on your LANDESK management workstation:

```
[CoreServices]
ClientDomain=<servername>
ClientName=<any unique name>    See:Note

[Traffic]
CSVInterval=10
CSVMaxDataEntries=65536

[ALCONV]
ShowMessages=1
ExecuteServices=2

[LDMS Metering]
RelayServer=<relay_server_name>
DLLMetering=<on or off>
```

Note: ClientName is assigned a unique name during the setup. This name can be changed after setup to any name unique to your domain, such as your user ID.

The LANDesk Management Suite Setup establishes a default domain depending on where you installed the software. If you installed it on a NetWare Server, the domain includes that server and any workstations that log in to that server. You can activate workstation management by including users in the LANDESKGROUP user group. Only users in this group are configured with CCDRIVER.EXE.

LANDesk Management Suite no longer requires LOGIN.COM and LOADTSR. Setup attempts to remove all copies of LOGIN.COM from your system. However, LANDesk Virus Protect still requires LOGIN.COM. If you are using LANDesk Virus Protect, you need to print the TO_DO.TXT and follow the directions on how to edit the login script to remove any dependency on LOGIN.COM.

CCDriver enables Client Configuration Utility to execute on the client workstations. It runs from the login script include file (LD_LOGIN.DAT).

To run CCDriver:

- Open LD_LOGIN.DAT in the PUBLIC directory of your management server.
- Remove the REM in front of CCDriver:

  ```
  REM #L:\LOGIN\LANDESK\CCDRIVER /A /L
  ```

- To configure Windows directories in your path, add the parameter /P.
- For network Windows installations, add a pointer to the root of the users directories using the /M command-line parameter. For example:

  ```
  Windows directory :   X:\WINDOWS
  Users directory   :   X:\USERS\USER1
                        X:\USERS\USER2
                        X:\USERS\...
  ```

  Use either:

  – The CCDriver command that searches only \USERS directories on drive X:

```
#L:\LOGIN\LANDESK\CCDRIVER /A /MX:\USERS
```

– The CCDriver command that searches \USERS directories on any drive:

```
#L:\LOGIN\LANDESK\CCDRIVER /A /M\USERS
```

For more information about CCDriver, see 2.6.3.1, “CCDRIVER” on page 105.

2.5.6 Client Configuration Utility

Before resetting the administrator's workstation, check to make sure that CLNTCFG.INI is configured correctly:

1. Open the CLNTCFG.INI in the shared LANDESK directory of your management server.
2. Check the [PRODUCTS] section. The products you installed should have Yes next to them. For example:

```
[Products]
DMI=YES   ; install DMI components
METERING=NO ; do not install Metering components
```

3. Check the [SERVER] section. It should be similar to the following:

```
[SERVER]
ServerName=<your server name here>
DomainName=<your Management Server name here>
ServerOSType=<NetWare3 or NetWare 4 or NT3>
SharedLANDeskDir=<path to SHARED LANDESK directory in UNC format>
```

That is all that we needed to do from the To_Do List.

2.6 Client Installation

This section discusses installation of Windows 95, Windows 3.1 and 3.11, Windows NT, and OS/2 clients.

2.6.1 Windows 95 and Windows 3.x Clients

Windows 95 and Windows 3.x clients are a scripted semi-automatic process.

The client configuration process is initiated and controlled by three utilities: CCDRIVER, CCLOADER, and CLNTCFG.

2.6.2 NetWare Clients

For NetWare clients, the system login script automatically launches the client configuration process when members of the LANDESKGROUP users group log in to the server.

You activate workstation management by including users in the LANDESKGROUP user group. Only users in this group are configured with CCDRIVER.EXE.

The LANDesk Management Suite no longer requires LOGIN.COM and LOADTSR. Setup attempts to remove all copies of LOGIN.COM from your system. However, LANDesk Virus Protect still requires LOGIN.COM. If you are using LANDesk Virus Protect, you need to print TO_DO.TXT and follow the directions on how to edit the login script to remove any dependency on LOGIN.COM.

2.6.3 Windows NT Clients

For Windows NT clients the client configuration process is launched when they log on to the Windows NT domain and their logon script or user profile is processed.

2.6.3.1 CCDRIVER

CCDRIVER is a DOS utility that executes from a NetWare system login script or Windows NT logon script. During setup and domain expansion, CCDRIVER.EXE is copied to the management server's or managed server's shared LANDESK directory. The following lines are placed in the server's LD_LOGIN.DAT file:

```
REM L:\\<SERVERNAME>\<shared_LANDESK_directory>\ccdriver /L /A
```

CCDRIVER does the following:

- Copies CCDRIVER.TXT to each workstation. This is a hidden file that contains the date you configured the workstation.
- Creates CCLOADER.INI and copies it to each Windows 3.x workstation's WINDOWS directory. This file contains information about launching the Client Configuration Utility, CLNTCFG.EXE.

  Note: Windows 95 does not need CCLOADER.
- Copies CCLOADER.EXE from the shared LANDESK directory to the workstation's WINDOWS directory.
- Modifies the WIN.INI file.

Attention

Do not delete CCDRIVER.EXE or CCDRIVER.INI.

2.6.3.2 CCDRIVER.EXE and Windows 3.x Workstations

On Windows 3.x workstations, CCDRIVER checks local hard drives and path directories for WIN.INI files. It places the following line into any WIN.INI file it finds:

```
load = ccloader
```

Windows 3.x is not compatible with UNC paths. Therefore, CLNTCFG.EXE, the Client Configuration Utility, can't execute directly from a Windows 3.x workstation's load line. Instead, CCLOADER must launch CLNTCFG.

2.6.3.3 CCDRIVER.EXE and Windows 95 Workstations

On Windows 95 workstations, CCDRIVER checks local hard drives and path directories for WIN.INI files. It places the following line into any WIN.INI file it finds:

```
load = \<SERVERNAME>\<shared_LANDESK_directory>\clntcfg
```

Note: CCLOADER.EXE is not needed for Windows 95 workstations.

2.6.3.4 CCLOADER

CCLOADER.EXE is a Windows utility that runs on Windows 3.x workstations. When a workstation launches Windows, CCLOADER.EXE does the following:

- Saves the workstation's current drive mapping for L: to the CCLOADER.INI file and then remaps L: for launching CLNTCFG.EXE, the Client Configuration Utility.
- Copies CCLOADER.INI into the Windows directory.

- Launches CLNTCFG.EXE.
- Maps L: back to its original drive mapping.

Attention

Do not delete CCLOADER.EXE or CCLOADER.INI.

2.6.3.5 CLNTCFG

The Client Configuration Utility (CLNTCFG.EXE) enables you to easily update your workstations. By modifying a date inside a .INI file, you can reconfigure your workstations automatically.

CLNTCFG.EXE is the Client Configuration Utility. This utility configures the desktop to use client utilities such as:

- Metering
- Distribute
- Desktop access

It does the following:

- Verifies that the workstation's Windows installation is correctly set.
- Copies files from the server's shared LANDESK directory to the workstation's directories.
- Modifies the workstation's WIN.INI file.
- Installs workstation components for Distribute, Software Metering, Desktop Manager, and DMI Control Panel.
- Uses the CLNTCFG.INI file to specify how Management Suite configures your workstations.

When a workstation launches Windows, CLNTCFG.EXE automatically runs. If no errors occur during the configuration process, the Client Configuration Utility automatically removes its load command from the workstation's WIN.INI. If errors occur, CLNTCFG's load command remains. After successfully configuring the workstation, CLNTCFG deletes CCLOADER.EXE and CCLOADER.INI, as they are no longer needed.

Attention

Do *not* delete CLNTCFG.EXE or CLNTCFG.INI.

From LANDesk Management Console, choose **Manage | Domain** to expand your domain.

2.6.4 OS/2 Client Install

The OS/2 version of the user agent, USEROS2.EXE, runs under the Novell NetWare Requester for OS/2 or utilizes the Novell OS/2 32-bit networking DLLs. If you use the Novell OS/2 32-bit networking DLLs, make sure those DLLs are in the workstation's path.

We chose to install the Novell Client32 for OS/2. This was difficult and we ended up replacing the Config.sys with a plain CONFIG.SYS with no networking in it. After rebooting, we installed Client32 for OS/2. After a reboot we copied the changes made to the plain CONFIG.SYS and pasted them at the end of the original CONFIG.SYS. We then removed the temporary CONFIG.SYS and rebooted with the original CONFIG.SYS (with the copied Client32 changes). We then ran MPTS and let it make the changes necessary to the new CONFIG.SYS (original with Client32 changes copied into it). We still had to go into the CONFIG.SYS and remove the REM from the routesys statement. After that everything worked fine and we were ready to install the OS/2 Client for LDMS.

To set up an OS/2 workstation at the workstation's OS/2 command line, run OS2SETUP.EXE (on the LDMS CD-ROM, in the OS/2 directory). Run this program for each OS/2 workstation you want to manage.

2.6.5 Starting the LANDesk Management Suite

From your management workstation click on **Start → Programs → LANDesk Management Suite** and then **Management Console** (see Figure 122). This will start the Management Console. Next, you have to start the Distribute Console, even if you will not be distributing software, because you must run Distribute before installing the MPM provider on LANDesk.

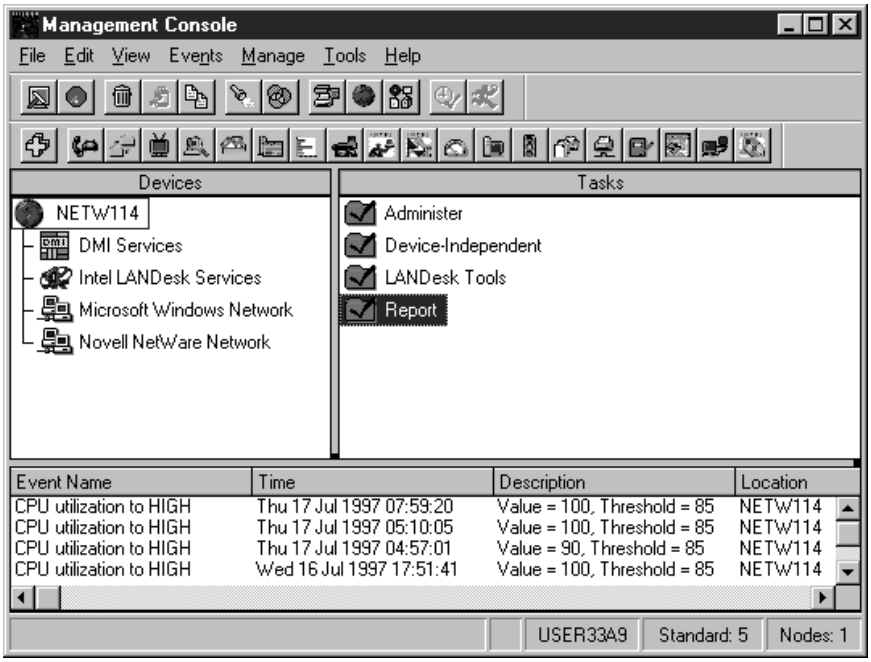


Figure 122. LANDesk Management Console

From the Management Console click on the **Distribute Console** icon in the tool bar (see Figure 123 on page 108).

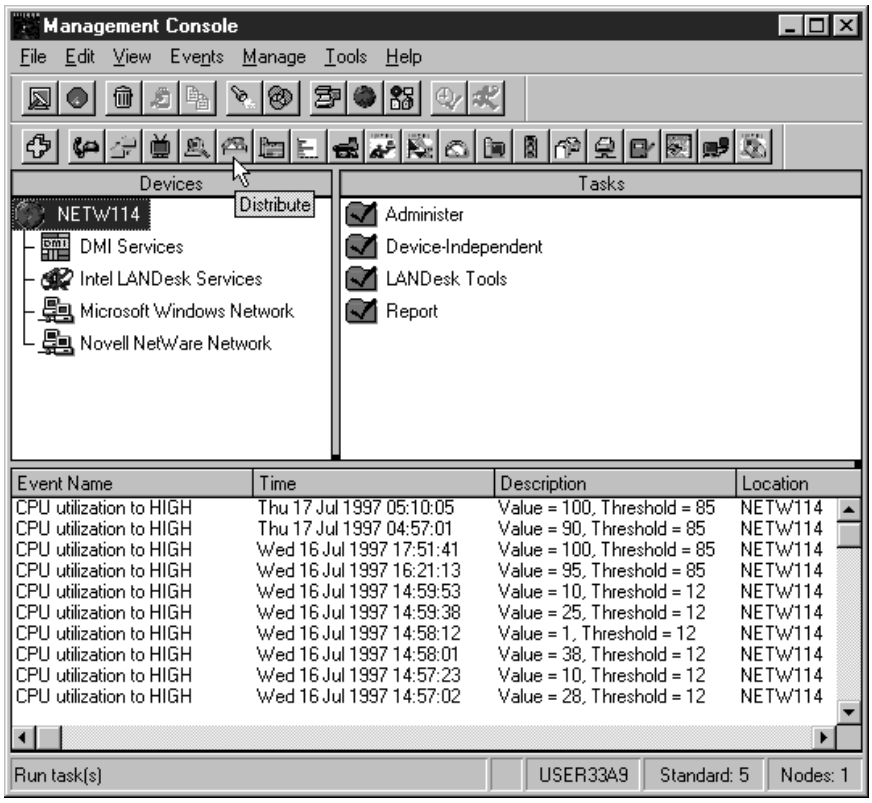


Figure 123. Distribute Console's Tool Bar Icon

This should bring you to a figure similar to Figure 124. If you get a warning with a return code of 86, you will need to make sure your Btrieve settings shown in Figure 95 on page 80 have been configured properly.

Figure 124. Configuration Panel for Distribute

Distribute uses a scanning technique to take pre-installation and post-installation snapshots of your hard drive or any network drives you choose. It uses the

differences between the two snapshots to create a distribution package for software applications. The process follows:

1. Distribute takes a pre-snapshot.
2. You install the software manually on your local workstation.
3. Distribute takes a post-snapshot.
4. Distribute then compares the snapshots and creates a package.

There are three basic types or personality files:

1. The administrator personality file tells the Distribute function the configuration of your workstation where you are creating the software distribution packages.
2. The base personality file contains the default configuration for target workstations and servers.
3. The target personality file tells the Distribute function a specific target workstation's configuration.
4. The target template personality file is used to create target personality files.

You do not need to configure the snapshot file or the personality files at this time. Tivoli LAN Access only requires Distribute to be started at least one time before the installation of the MPM provider. Once you close this panel you should get a panel similar to Figure 125.

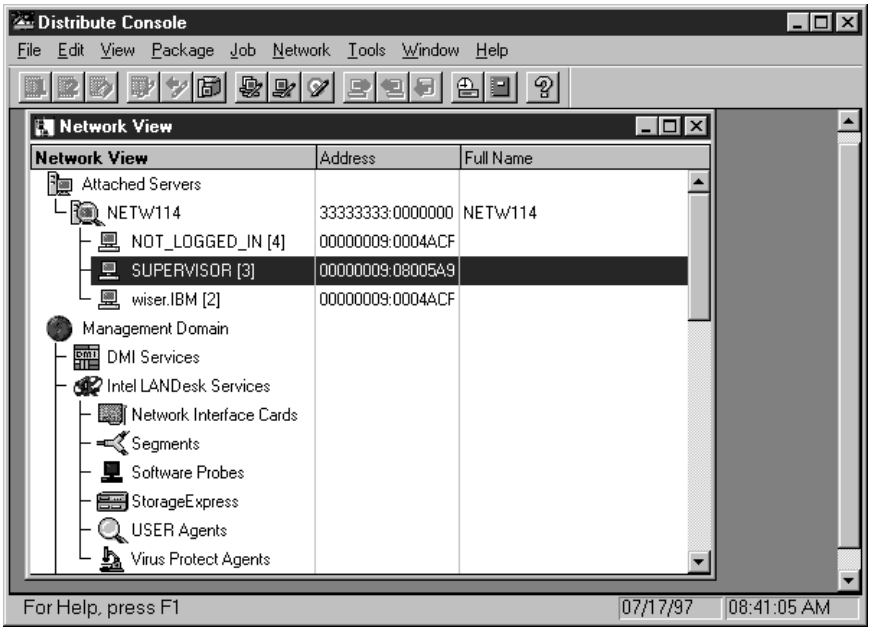


Figure 125. Distribute Console

Tivoli LAN Access will create an icon for every workstation and server attached or unattached, logged in or not. You can see by the addresses in Figure 125 it is going to make two icons for the workstation with the address 00000009:0004ACF. This is because this system is logged in to the NDS Tree not the server.

From the Desktop Manager (see Figure 126 on page 110) you do most of your workstation management.

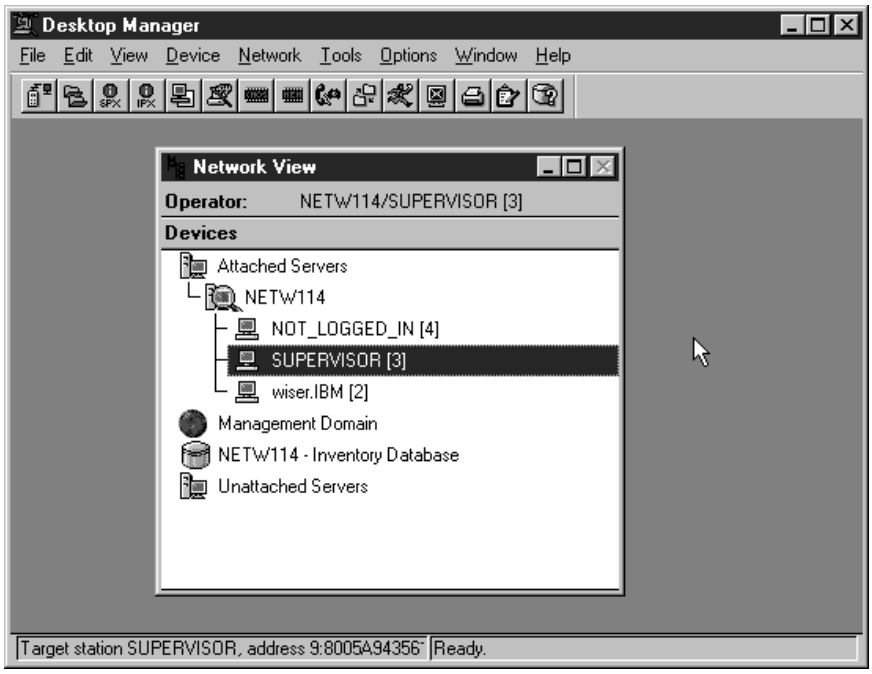


Figure 126. Desktop Manager

If you need to actively manage the work system your management workstation is installed on, click on the **WUser Agent** icon, located on the lower tool bar (see Figure 127 on page 111).

Note: We have found if you have more than one management console running in your environment, you may run into a discovery problem on the management workstation with the Tivoli LAN Access MPM provider installed (if you are running WUser). This is one reason why in 2.5, “Installation and Configuration of LANDesk” on page 84 we indicate that the management workstation with the MPM provider should not be used as an active LANDesk management workstation. The other is dependent on the size of your network. You don't want the MPM management workstation being busy when an alert happens and thus delaying the transfer of that alert to Tivoli Event Console.

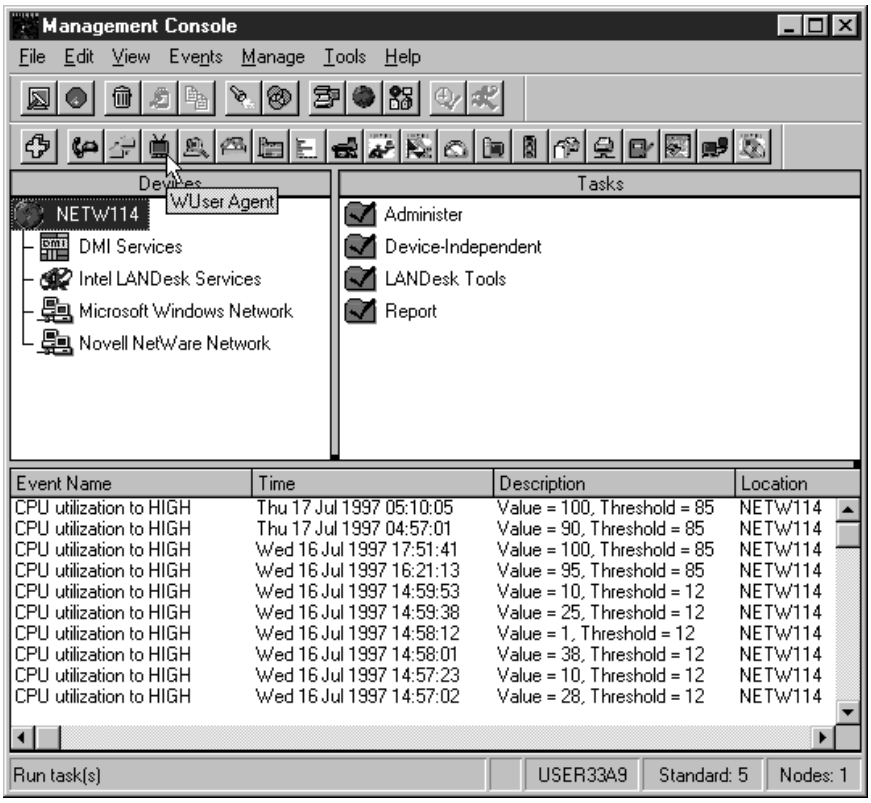


Figure 127. Management Console/WUser Icon

You can run WUser during the Tivoli LAN Access Site creation processes. This is a good way to check the processes. If you can hear the sound of your management workstation disk from your TMR desktop system, it is possible that the creation process is occurring. As the Tivoli LAN Access site is checking for systems it will make the same disk sounds as if you were accessing the system with the LANDesk Desktop Manager.

If you choose to start WUser, Figure 128 will pop up on your panel. If you close the pop-up window, WUser will still be running.

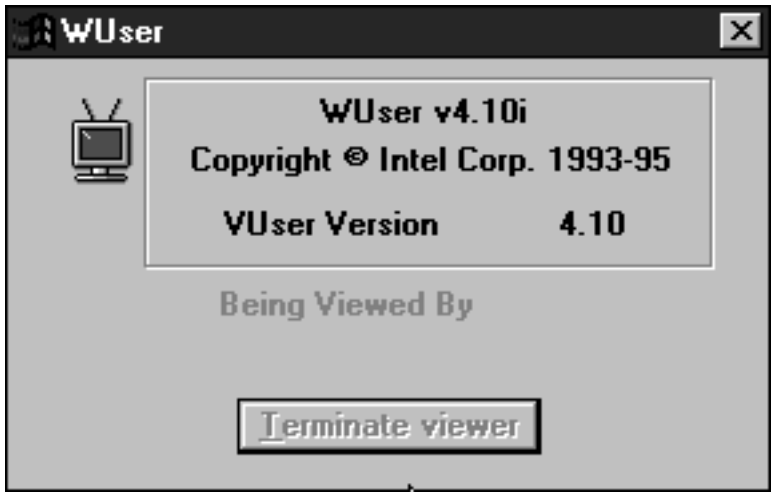


Figure 128. WUser Window

At this point you should have five things running in your task bar:

1. RAP II IPX

   In order for your computer to be DMI-enabled, RAP and WINSL must be running.

   Remote Access Protocol (RAP - the icon's name is RAP II IPX) is the agent that provides remote access to the local service layer Windows Service Layer (WINSL). Executing RAP automatically launches WINSL.

2. Alert Converter

   This converts and forwards alerts to AMS.

3. Management Console

   This is the main console. From here you can launch all other consoles, display Windows NT and NetWare domains and all attached devices.

4. Desktop Manager

   - Provides remote control, and displays current remote workstation software and hardware configurations.
   - Provides troubleshooting and diagnostic tools.
   - Collects and stores hardware and software configurations.
   - Creates an inventory database of workstations and components.

5. Distribute Console

   Distribute installs software packages created from before and after snapshots of a local installation.

We found that if you have these things running, the installation of the Tivoli LAN Access provider is much more reliable. You are now ready to install the Tivoli LAN Access provider on our management workstation.

2.7 MPM Provider Installation on the Management Workstation

This section explains the installation of the MPM provider for LANDesk. The prerequisites steps for installing the Tivoli LAN Access provider and the MPM APIs are:

- Make sure you have followed the steps in 2.4, “Installation and Configuration of Btrieve” on page 74.
- Perform the configuration changes shown in 2.4.4.1, “Configuring BSTART.NCF” on page 80.
- Make sure you have followed the steps in 2.5, “Installation and Configuration of LANDesk” on page 84.
- Make sure that the following five things are running on the LANDesk management workstation:

  1. RAP II IPX
  2. Alert Converter
  3. Management Console
  4. Desktop Manager

5. Distribute Console

From the management workstation, point to the code on the Tivoli LAN Access CD, or to the redirected drive that the code has been copied to. Within the W32 directory, run setup.exe. This will bring up the Welcome panel.

The Welcome panel gives you a brief description of LAN Access. After clicking on **Next** the Tivoli LAN Access Installation Location panel will pop-up, as shown in Figure 129.

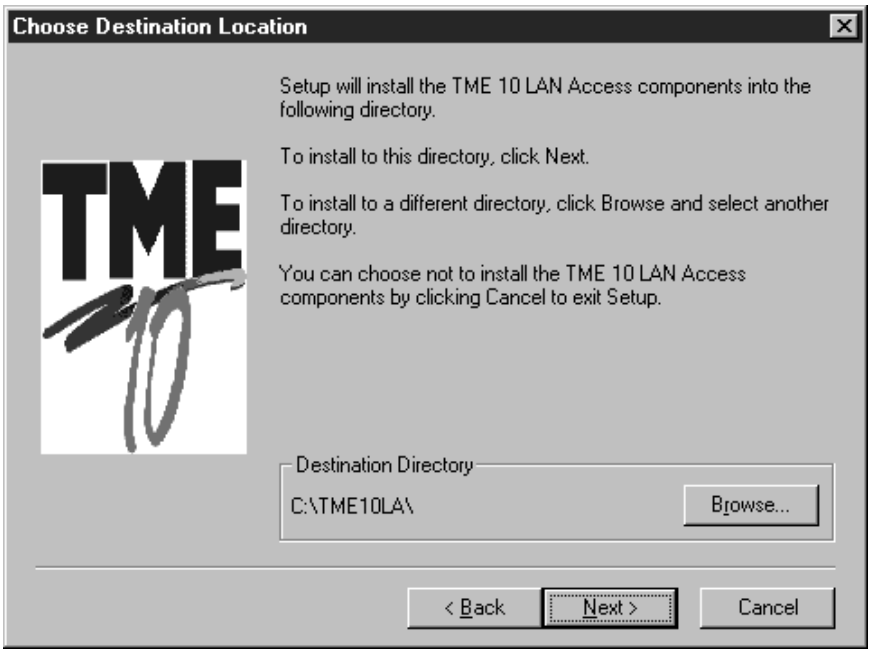


Figure 129. LAN Access Installation Location

After clicking on **Next** the Tivoli LAN Access Directory Target panel will bring you to a window similar to Figure 130 on page 114.

The target directories by default were filled in by a discovery process. Unless you know that the default is wrong, do not make any changes to the target paths.

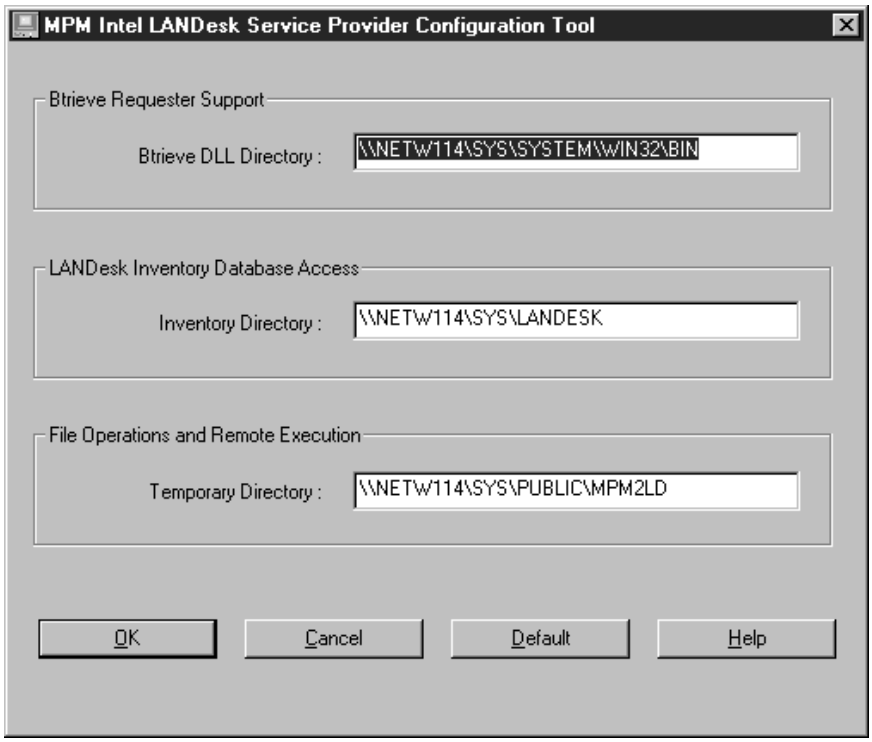


Figure 130. LAN Access Directory Targets

After clicking on **OK** a configuration completed message will show up asking you to click on **OK**. This is just the completion of the configuration of the target directories; it is not the end of the installation. After clicking on **OK** it took a few minutes before Figure 131 on page 115 popped up. The results will depend upon your network and system configuration.

This is where you choose the target directory for the Tivoli LAN Access Transport installation. If you have already installed IBM's Netfinity, the next few panels will be familiar. Tivoli LAN Access uses the Netfinity Transport for its communication from the MPM provider to the managed node.

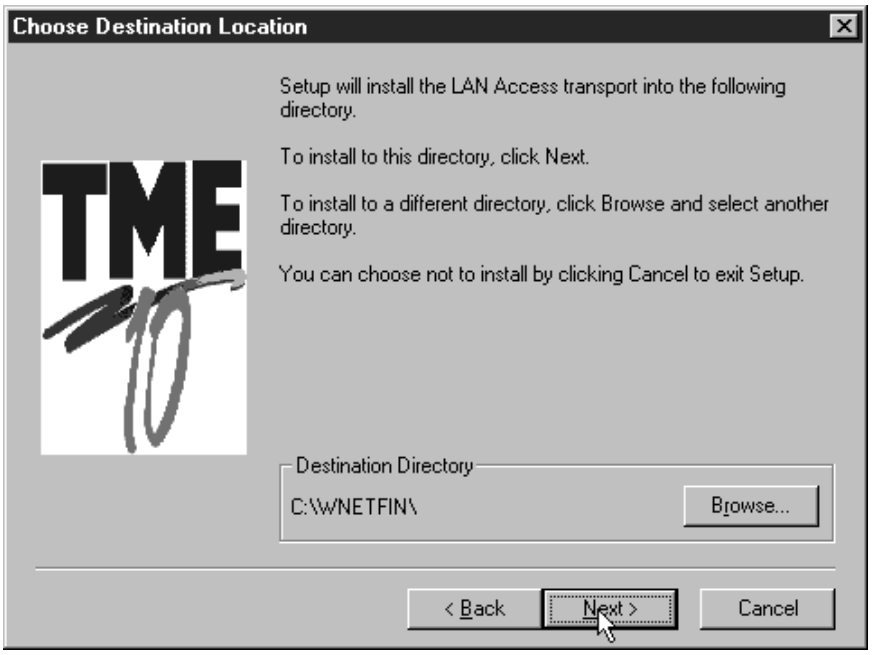


Figure 131. LAN Access Transport Target Directory

2.7.1 Driver Configuration

After choosing a target directory and clicking on **Next**, the Tivoli LAN Access files will be copied to their targeted directories. When the file transfer is almost done, the Network Driver Configuration panel will pop up, as shown in Figure 132 on page 116.

- The System Name is only related to Tivoli LAN Access and Netfinity systems. Make sure the name you select is unique to your Tivoli LAN Access or Netfinity environment.
- The network drivers that are listed in the window are dependent upon what you have installed on the system. The installation program checks to see what you have installed on your system before giving you the option. If you don't have IPX on your system, it will not show up in the list of possible drivers. To enable a protocol just click on the protocol to highlight it, then click on the **Driver Enabled** check box.
- The Network Time-Out is set to 15 seconds by default. We have found that if you have a slow network or any other section of your environment that barely meets the minimum requirements, you should increase this setting.

  Note: If you choose the default and later develop network timeout problems, you can click on the **Network Driver Configuration** menu from the Tivoli LAN Access list and make adjustments to this setting.

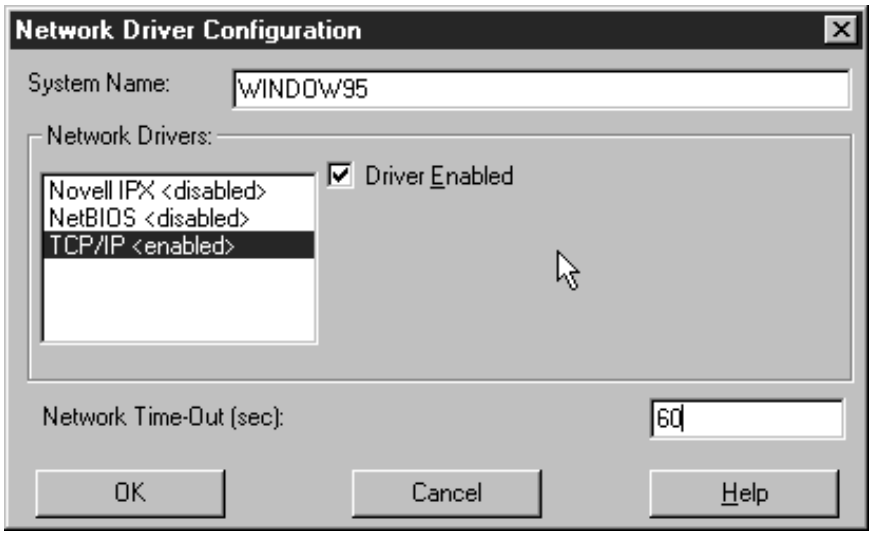


Figure 132. LAN Access Network Driver Configuration

We tested the IPX, NetBIOS and TCP/IP transport protocols. All three protocols worked fine. Remember this protocol is only for the connection between the managed node and the management workstation. If the managed node is remote from the management workstation, you have to consider routers and network traffic when choosing the protocol.

After completing the Tivoli LAN Access Network Driver Configuration, the file transfer will complete and will bring up the Setup Complete panel (see Figure 133). You should restart your system later, instead of immediately, as there are some other customization options you will need to perform.

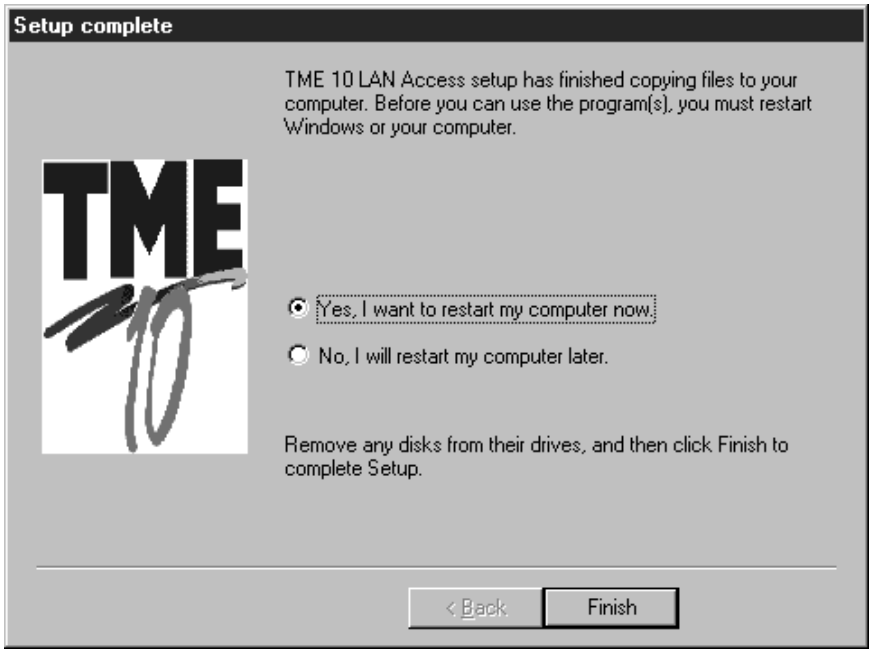


Figure 133. LAN Access Setup Complete

On our test system, we were unable to get a clean automatic shutdown by clicking **Yes**. We had to close down the LANDesk Management Suite in the following order:

1. Management Console
2. Distribute Console
3. Desktop Manager

After they have all successfully shut down, we could reboot our system.

2.8 LAN Access Provider Installation on the Managed Node

From the Windows NT managed node, point to the code on the Tivoli LAN Access CD or to the redirected drive that the code has been copied to. Open the W32 directory and run setup.exe. This will bring up the Welcome panel.

The Welcome panel gives you a brief description of Tivoli LAN Access. After clicking on **Next** the Tivoli LAN Access Destination Location panel shown in Figure 134 will appear.

Figure 134. LAN Access Installation Target Directory

This is where you select the target directory for the Tivoli LAN Access transport installation. If you have installed IBM's Netfinity, the next few panels will be familiar. Tivoli LAN Access uses Netfinity's Transport for its communication from the providers to the managed node.

Figure 135. LAN Access Transport Target Directory

After choosing a target directory and clicking on **Next**, the Tivoli LAN Access files will be copied to their targeted directories. When the file transfer is almost complete, the Network Driver Configuration panel (Figure 136) should appear. Review 2.7.1, “Driver Configuration” on page 115 for details on filling in the options.

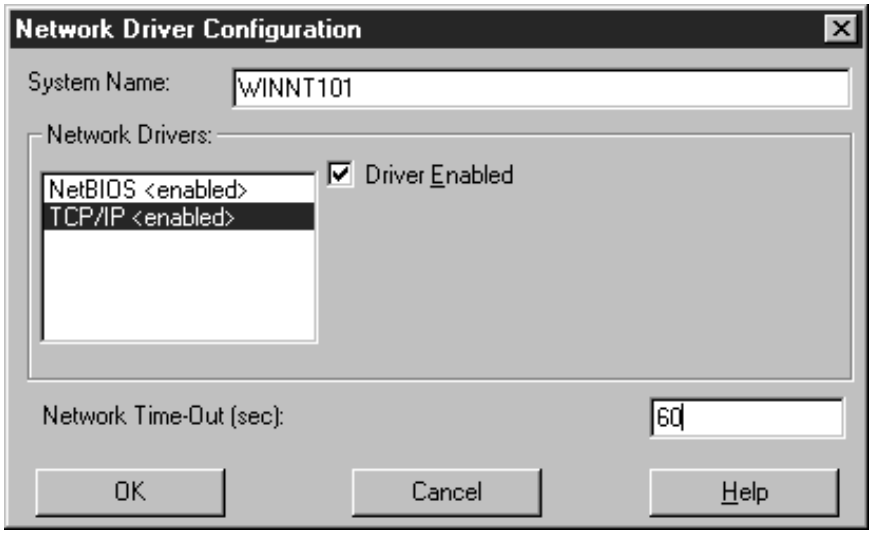


Figure 136. LAN Access Network Driver Configuration

After completing the Tivoli LAN Access Network Driver Configuration the file transfer will complete and the Setup Complete panel (Figure 137 on page 119) will pop up. You should select **Yes, I want to restart my computer now**.

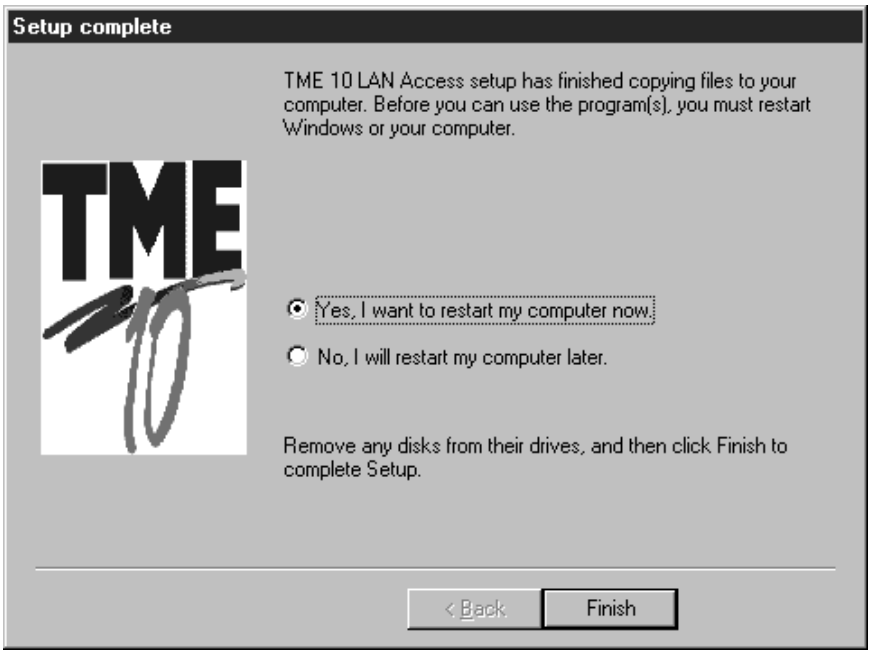


Figure 137. LAN Access Setup Complete

2.9 Uninstall the Tivoli LAN Access Providers

This section discusses the uninstall procedures of the LAN Access provider on the Windows NT 4.0 Tivoli managed node and on the Windows 95 LANDesk management workstation.

On the Windows NT 4.0 Tivoli managed node and on the Windows 95 LANDesk management workstation, there are two ways to uninstall the LAN Access provider.

Note: On the LANDesk management workstation make sure that the following five things are running:

1. RAP II IPX
2. Alert Converter
3. Management Console
4. Desktop Manager
5. Distribute Console

1. Click on Windows **Start → Programs → Tivoli LAN Access → Uninstall LAN Access**.
   - Both Windows NT and Windows 95 will ask you to confirm your decision to uninstall by popping up Figure 138 on page 120.

Figure 138. Uninstall Confirmation

- On the Windows 95 LANDesk management workstation, after most or the code is removed, Figure 139 pops up and shows you the MPM APIs that will be removed.

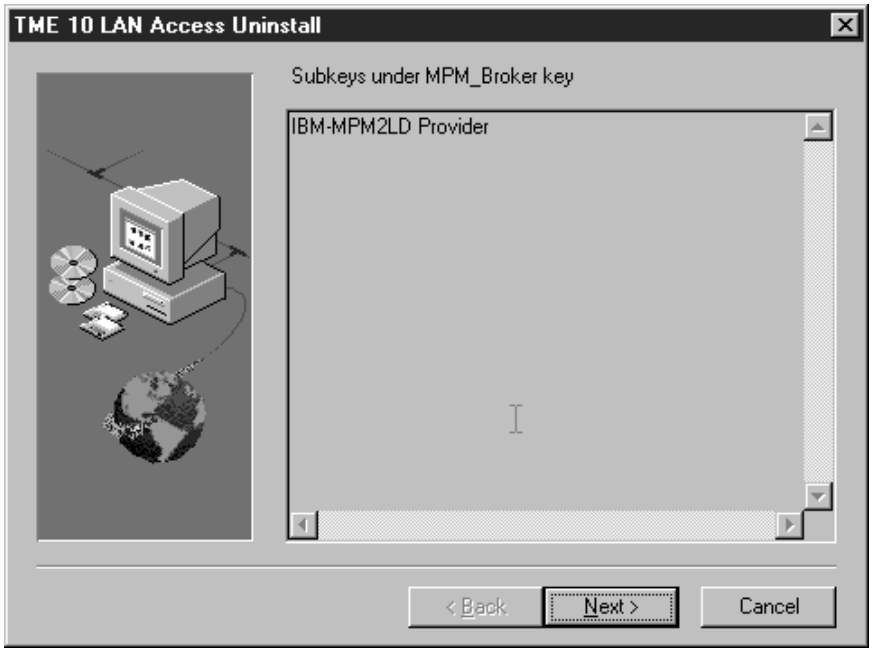


Figure 139. MPM Provider List

- You may have more than one entry in Figure 139. This depends on what providers you installed.
  - Microsoft SMS IBM-MPM2SMS provider
  - Intel LANDesk IBM-MPM2LD provider
  - IBM Netfinity provider
- After all the code is uninstalled and the registry changes have been made you will get a pop-up window indicating that the LAN Access transport is being removed followed by a message indicating that the uninstall log is being processed.
- After the provider has been removed, you will need to restart your system.

The second way to uninstall it is to:

2. Click on Windows **Start** → **Settings** → **Control Panel** → **Add/Remove Programs** → **Install/Uninstall**. Highlight **Tivoli LAN Access** and click on the **Add/Remove** button.

Note: This method of uninstalling the code works better if the LANDesk Management Suite is not running. You should only have two things running in your task bar:

- RAP II IPX
- Alert Converter

Both ways of uninstalling the code remove almost all the registry entries. The only things left are two or three entries on the Windows NT managed node system in the *legacy* area.

2.10 Alert Management

This section shows how to set up alerts in LANDesk that will get detected and handled by Tivoli Enterprise Console (TEC). Tivoli LAN Access will pass filtered events up to TEC. This can be on any platform that Tivoli TEC is supported on.

In order to show an example of how the flow would work, we set up a CPU usage alert for our LANDesk's NetWare Server. Setting up a server alert in LANDesk is done from the Management Console as shown in Figure 140. Click on the **Server Manager Console** tool bar icon as indicated with an arrow pointer in the following window:

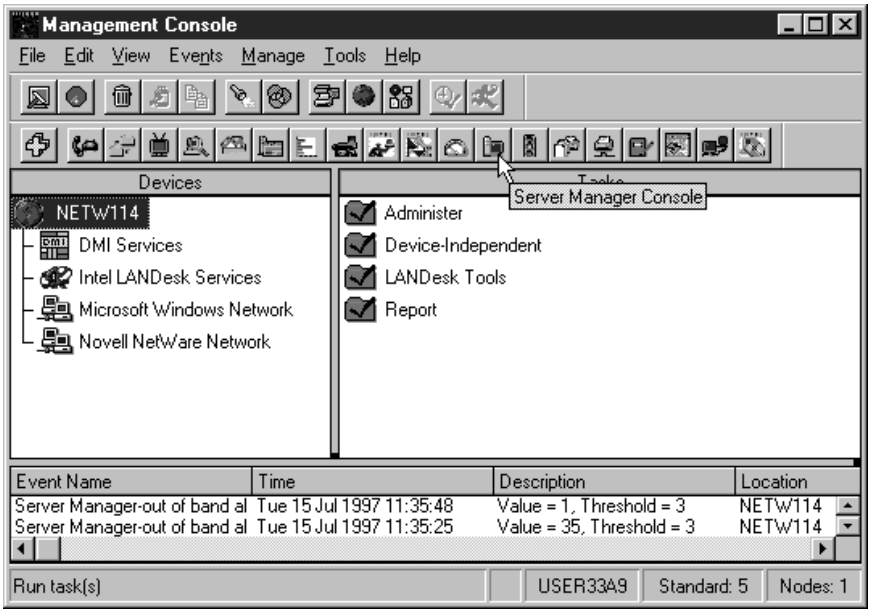


Figure 140. LAN Access Server Manager Tool Bar Icon

This tool monitors and manages your attached servers.

Click on the server you want to manage. Then click on **Server Status** and **CPU Utilization** (see Figure 141 on page 122). This will bring up Figure 142 on page 122.

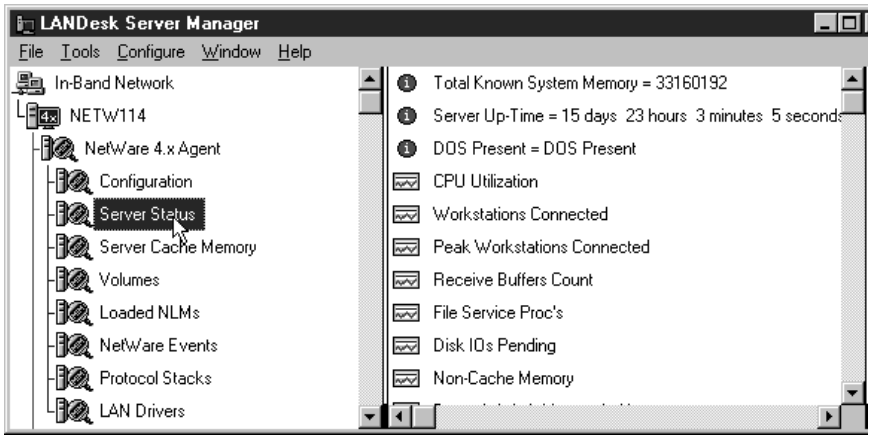


Figure 141. Server Status

You must click on the **CPU Utilization** panel so that it is highlighted.

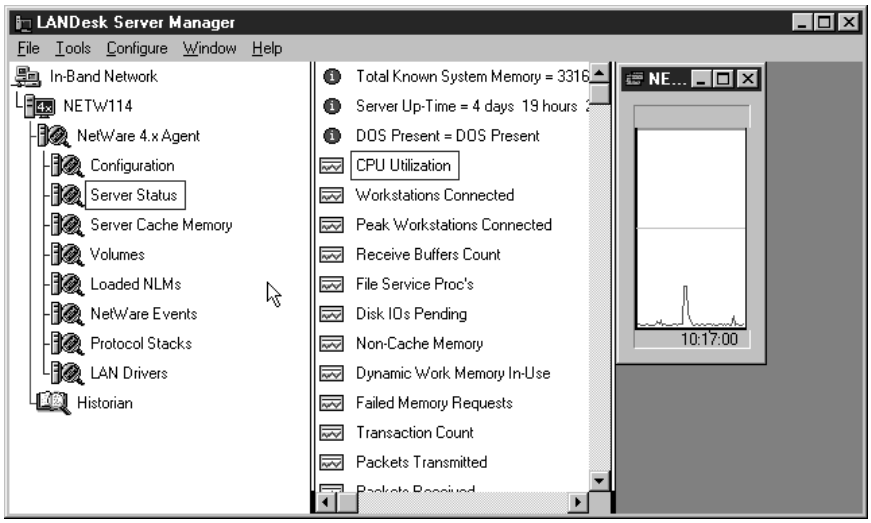


Figure 142. CPU Utilization Graph

On the task bar click on **Configure**, then **Events** as shown in Figure 143 on page 123. This will bring you to Figure 144 on page 123.

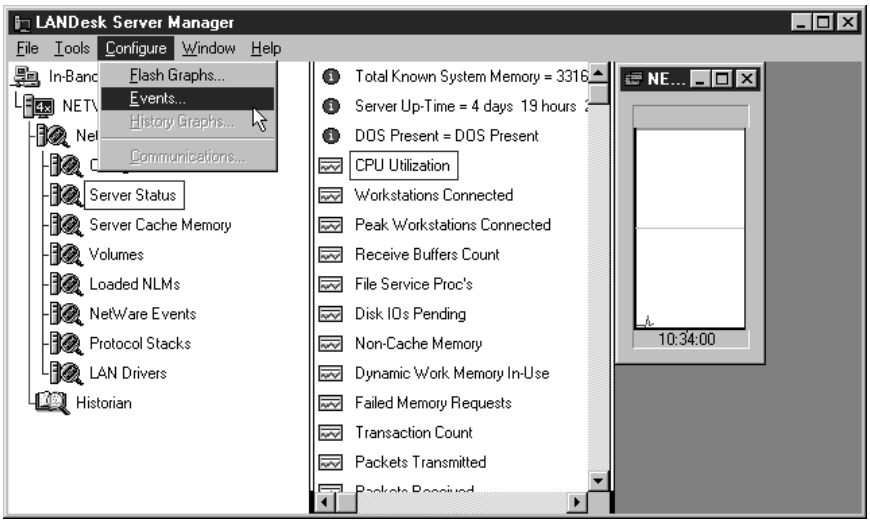


Figure 143. Setting a CPU Threshold

We chose to make this a warning by clicking on **Warning** to highlight it. We first set the CPU Utilization to 85% (by typing 85 in the Actual field) and the duration was set by typing a 2 in the Duration field. This means that the CPU Utilization must stay above 85% for more than two seconds in order to hit that threshold. Setting the polling interval to 2 will make the CPU check the value every two seconds. From this panel we could set up different threshold types:

- Informational
- Warning
- Critical

Each one of these can take a different action if the threshold conditions are met.

You can now select an event to occur once the threshold has been reached. This is done by clicking on the **Select** box in Figure 144 in the AMS Settings section.

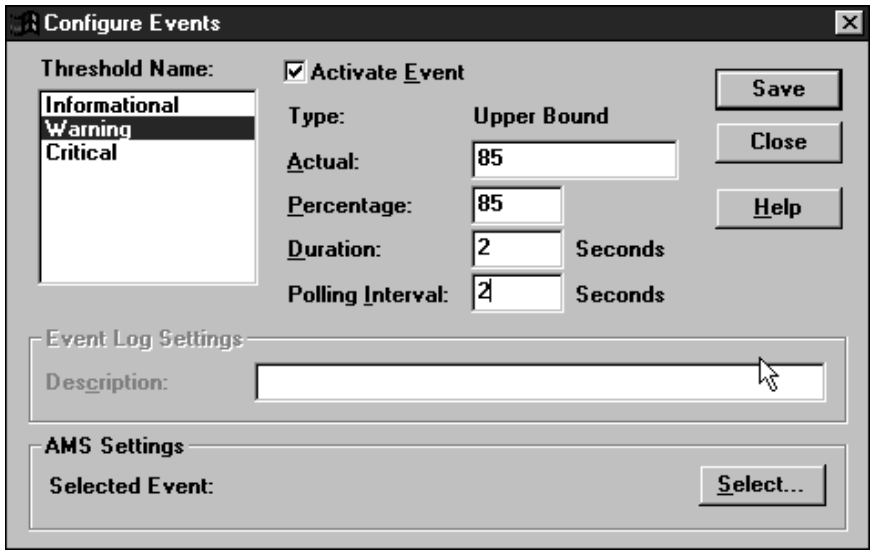


Figure 144. Event Configuration

Clicking on that field will bring up the window shown in Figure 145 on page 124. The two events listed in Figure 145 on page 124 are the default events:

- Server Manager-AMS alert failure
- Server Manager-out of band alert

We chose to create a new event called CPU Utilization Warning, by clicking on the **Create** button. This brings up the window shown in Figure 146.

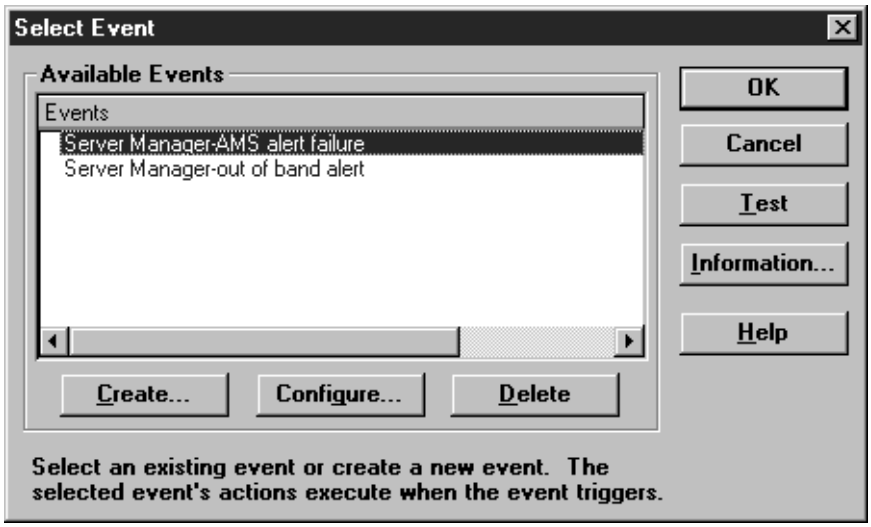


Figure 145. Event Selection

After filling in the name and description, click on **OK**. This will bring you to Figure 147 on page 125.

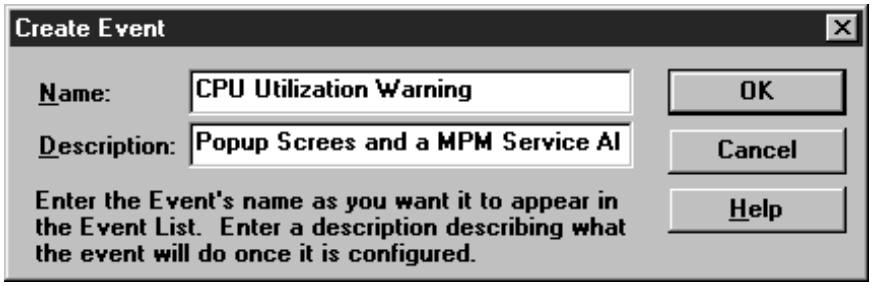


Figure 146. Event Creation

At this point we have only made an event called CPU Utilization Warning that will be kicked off by the CPU Utilization exceeding 85% for more than two seconds. Next we configure the tool (action) we want to be started when our threshold is exceeded. By clicking on the **Configure** button, the window shown in Figure 148 on page 125 is brought up.

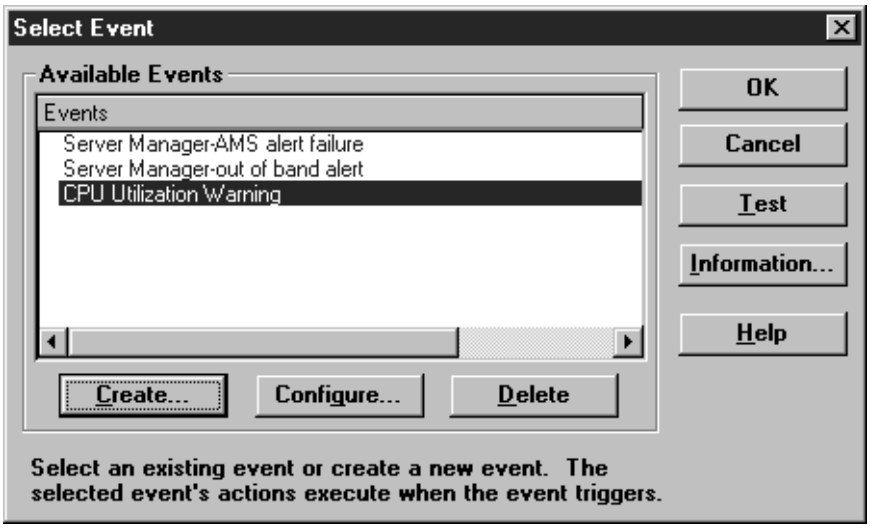


Figure 147. Event Selection and Configuration

Select a tool from the Available Tools box and click on the **>>** button to move them to the Selected Tools box. Once you have selected all the tools (actions) you want this threshold to start, click on the **Configure** button. This will bring you to a window similar to Figure 149 on page 126.

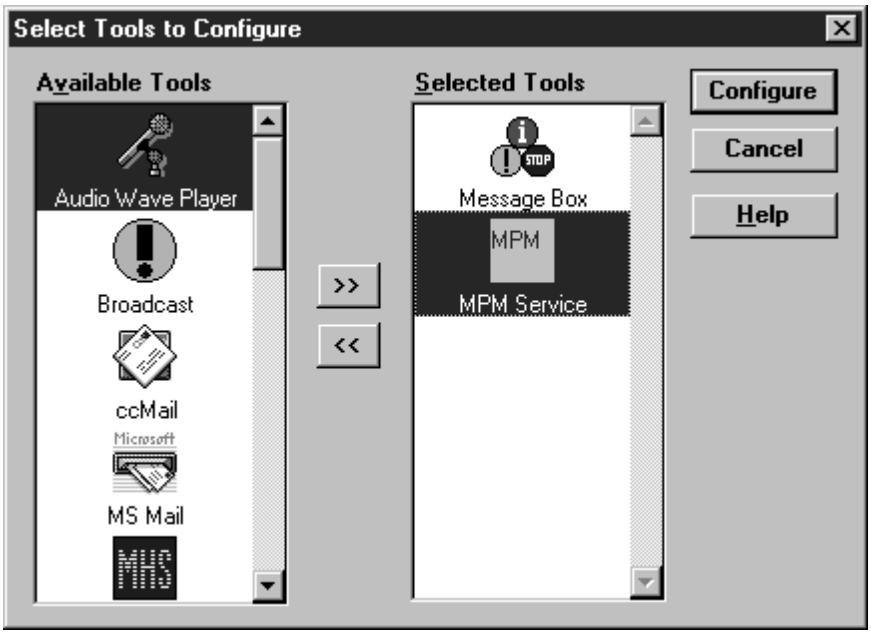


Figure 148. Tool (Action) Selection

Figure 148 shows the selected tools. They will get executed in alphabetical order. Since we selected two tools (actions) to be started for this alert we have to configure each one of them separately.

The first action that we customized was the Message Box. Click on the **Message Box** icon and then click on **Configure**. This will bring you to Figure 149 on page 126. You must fill in the Current Action Name or if you have already created an action, you can click on the **Retrieve** button. This will bring up a drop box that will list all previously configured actions for the Message Box tool. We created a

new Action called CPU usage exceeded 85%. In the Message section of Figure 149 on page 126 you can type any message you want to show up in the pop-up panel. By clicking on one or more of the push buttons in the Arguments area you can add:

- The parameters set for this alert
- The description you gave the alert
- The name of the server that generated the alert
- The date of the alert
- The time the alert was generated
- The severity of the alert

All that is shown in Figure 150 on page 127.

In the Message Box type area you can choose to have an error beep by placing a check in the check box.

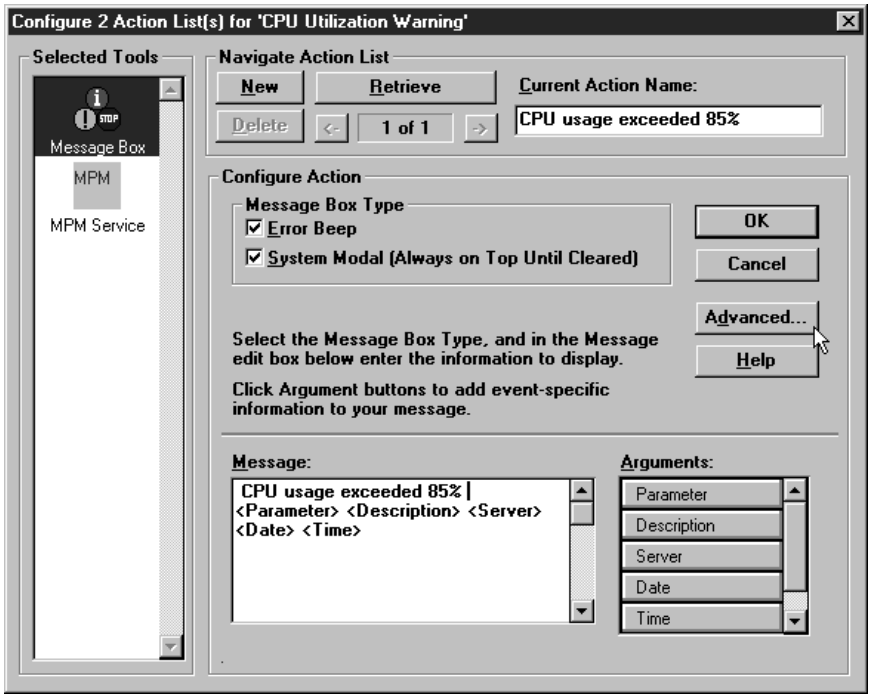


Figure 149. Message Box Tool (Action) Configuration

If you check the System Modal check box and the alert is generated, the user interface will not function until you clear the alert by clicking on **OK** (see Figure 150 on page 127).

Note: To make the event happen we set the upper limit down to 6% so we could force the alert shown in Figure 150 on page 127.

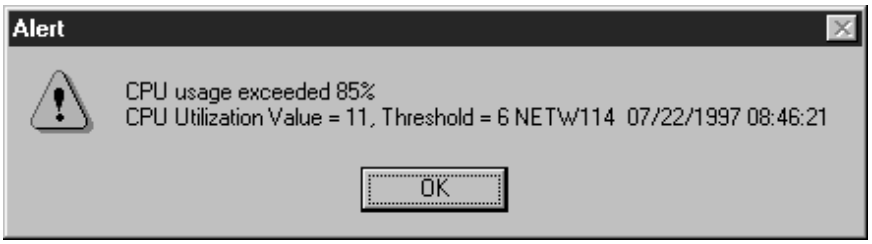


Figure 150. Alert Message Box

Next click on the **Advanced** button in Figure 149 on page 126, which will bring up the window shown in Figure 151 on page 128. Using the Advanced Tool Configuration you can place some limits on when actions (also called tools) will occur:

- Limit by time of day.
- Limit by location of the alert.
  - This is how you tell LANDesk what systems or groups of systems you want this alert to pop up on.
- Bypass running this tool if you have the same event multiple times.

For example, on one alert you may want a pop-up panel only from 8:00AM until 5:00 p.m. and from 5:00 p.m. until 11:00 p.m. contact a pager. Then from 11:00 p.m. until 8:00 a.m. just log the alert in a file. You can also set what system or systems the alert is executed on. In the Two-Stage Event Options you can choose if the alert will be generated at the beginning or end of an event.

Another example might be if you wanted to know as soon as you were running short of memory, or you might want to get notified when a backup has finished.

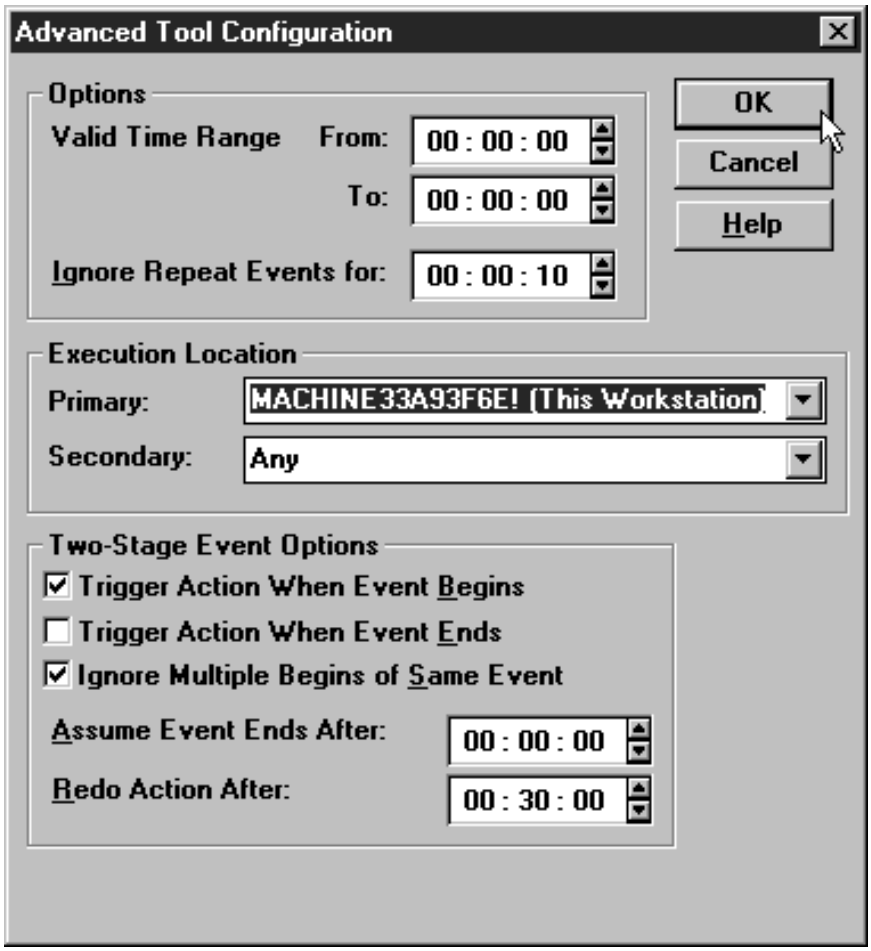


Figure 151. Advanced Tool Configuration

By clicking on **OK** in the Advanced Tool Configuration panel shown in Figure 151, it will bring you back to Figure 149 on page 126.

To configure the other tool we clicked on it in the Selected Tools box. This will bring up Figure 152 on page 129. There is not much to configure in this panel. We clicked on the **Retrieve** button and selected the Default MPM configuration. Then we clicked on the **Advanced** button and got the window shown in Figure 151.

Clicking on **OK** on the Advanced tool configuration panel and on the MPM Tool (action) Configuration panel shown in Figure 152 on page 129 will bring up Figure 153 on page 129.

Note: The MPM tool is not related to the MPM-API. It is related to the toolbox provided with Intel LANDesk. They also use the term MPM.

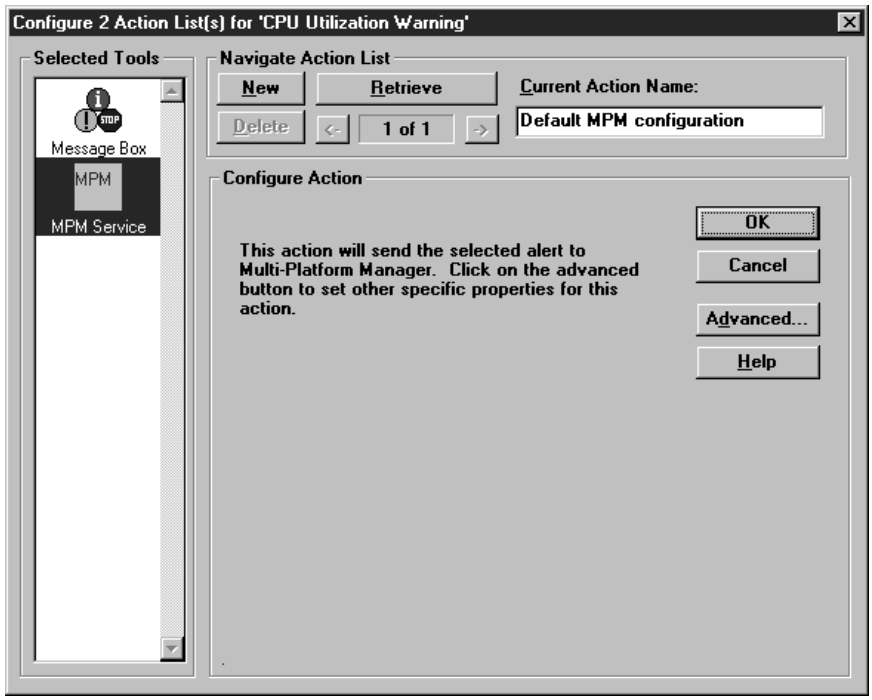


Figure 152. MPM Tool (Action) Configuration

As you can see, we have two tools (actions) that are configured to run when this event occurs. After selecting **CPU Utilization Warning**, click on **OK**. This will bring you to Figure 154 on page 130 with Selected Event: CPU Utilization Warning put into the AMS Settings box.

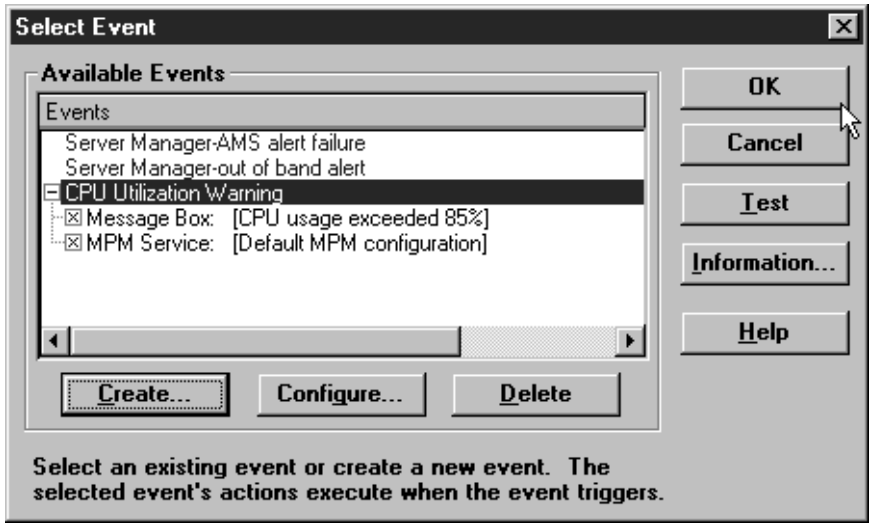


Figure 153. Event Selection

You have now configured the CPU Utilization Warning event to start when the threshold and other parameters have been exceeded. When the event is started it will now pop up an alert panel on the selected system or systems. It will also generate a alert and send it to the MPM.

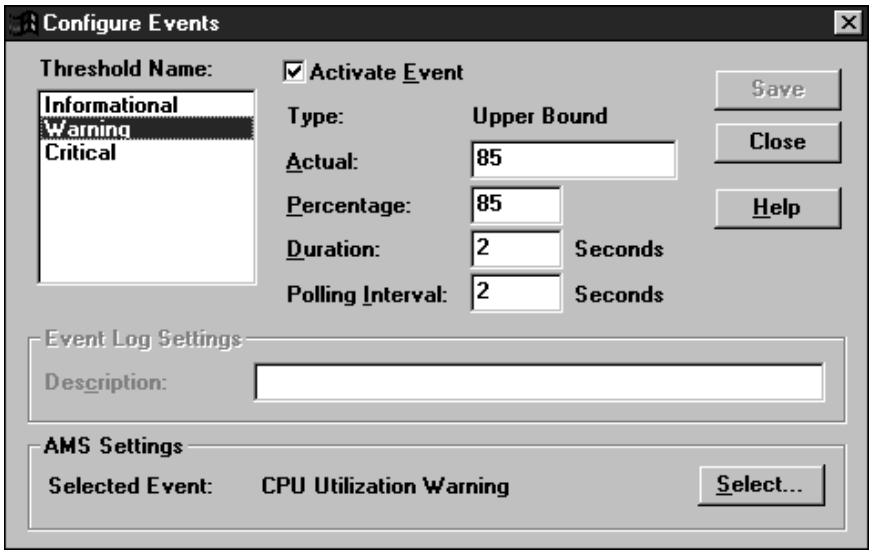


Figure 154. Event Selection Completed

Chapter 3. Netfinity 5.0

This chapter documents the installation and customization of Netfinity 5.0 as it relates to Tivoli LAN Access. For specific details on Netfinity see the following publications:

- *Netfinity V5.0 Database Support*, SG24-4808
- *Netfinity V5.0 Command Line and LMU Support*, SG24-4925
- *Systems Management from an NT Server Point of View*, SG24-4723

3.1 Netfinity

The Netfinity provider must be installed on an Intel-based machine running one of the following products:

- Windows NT Version 3.51 or 4.0, or OS/2 Version 3.0 or 4.0
- Netfinity Manager Version 4.0 or 5.0

To enable remote command execution, you must install the supplied patch on all clients running Netfinity Version 4.x under Windows 3.1x and Windows 95. This patch ships with the Netfinity provider and can be distributed using TME.

If the Netfinity provider is installed on Netfinity Manager Version 5.0, a required patch is automatically installed if the Netfinity file, netfbase.exe, is dated 4/10/97.

Netfinity Version 4.X Manager and Services systems running Windows 3.x or Windows 95 require a patch for the file RCSHD.EXE. This patch can be found in the \W32\NF40FIX directory on the LAN Access CD.

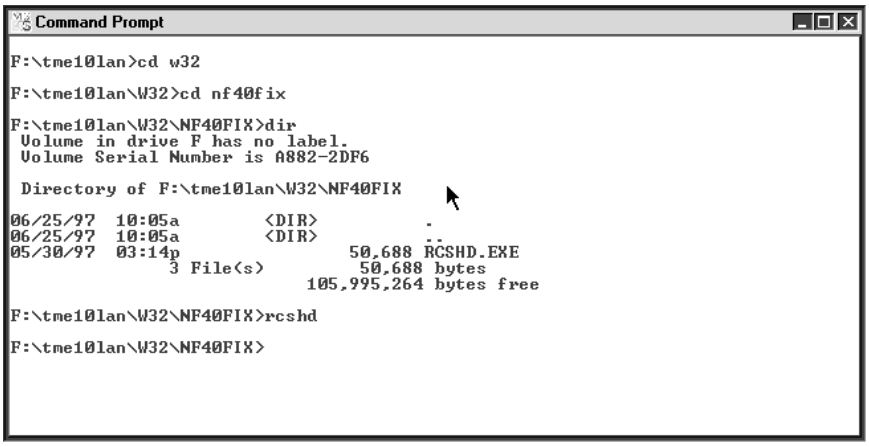


Figure 155. Install Fix for Netfinity 4.0

The following restrictions apply to performing file operations on nodes configured with Netfinity Services:

- Universal times are not supported; time zones are ignored.
- File transfers using Netfinity Version 4.0 do not support multiple concurrent Netfinity Managers. If two or more Netfinity Managers attempt to perform a file transfer operation concurrently, the first subscription is accepted and all

subsequent attempts fail while the original subscription is being executed. A file transfer operation that fails should be retried at a later time. This restriction does not apply to Netfinity Version 5.0.

Two or more Netfinity Managers can access the same Netfinity client. If multiple providers are operating on multiple Netfinity Managers and feed information to a single NT managed node running LAN Access, many of the client machines can appear multiple times (once through each manager). If multiple transports are used for communication between a Netfinity Manager and a Netfinity client, the client machine can appear multiple times (once for each type of transport). These scenarios could cause problems with software distribution and the collection of inventory.

A manager-of-managers concept using several levels of Netfinity managers is not supported. This means that if you have a Netfinity Manager managing another Netfinity Manager you will see this managed manager as a LAN Access client but you will not see the clients managed by the second manager. You have to make the managed manager an MPM provider in order to see its clients.

3.2 Installing on Windows NT

Before you begin installation, make sure that Netfinity is running on the node on which the files will be installed.

To install the Netfinity provider and transport on Windows NT, run `\w32\setup.exe` from the LAN Access CD-ROM.

Please read the README.TXT file on the LAN Access CD. The information on it is very helpful. Some specific things that we would like to point out are:

- Installation of Tivoli LAN Access
  - When the final dialog box appears for configuring the network driver (LAN Access Transport Layer) on the Windows NT managed node, a timeout setting is required. The dialog box defaults to 15 seconds. You will probably want to increase that value in most interconnected LANs.
  - By default the LAN Access Transport Layer is not configured with a user ID or password on the Target Remote MPM Systems (systems where the provider for SMS, LANDesk, or Netfinity is installed). This is *not* required. However, if you desire a user ID and password on these systems, open the **LAN Access** folder and use the Security Manager to set this user ID and password. Once the Security Manager application is started, select **Edit/Display Incoming Passwords**. Now enter a user ID, password, and select **MSB Client** from the Services list box. At this point click on **Set** and then **Exit**. Now you can exit the Security Manager.

    If security is set on the Target MPM Location, you will be prompted when using the Tivoli Desktop to create a LAN Access site. Enter the same user ID and password here that you set in the Security Manager.
- Known Problems/Limitations
  - If you use BARC programs for software distribution and these programs are batch files that use the command line interface (CLI) utilities, modify the statements that invoke the CLI utilities to include the location of the utilities. The CLI utilities are located in the C:\TMELACLI directory. For example, if

your batch file uses wdskspc c: to interrogate the available disk space on drive C prior to a distribution, change the command to c:\tmelacli\wdskspc c:.

- Do not specify a destination directory path deeper than one level as part of the platform-specific options; c:/foo currently works, but c:/foo/foo2 does not.
- Do not specify individual Tivoli LAN Access nodes as subscribers. Also, do not specify multiple LAN Access collection or site objects as subscribers for a file package. If you do, results will be unpredictable. Specify a single LAN Access site or a single LAN Access collection.

- Unable to register the MPM alert action message during install

  Note: If this message is received during installation, execute the following command from the directory where Netfinity is installed:

  ```
  MPMACTIN INSTALL
  ```

  Note that the Netfinity Network Interface must be running.

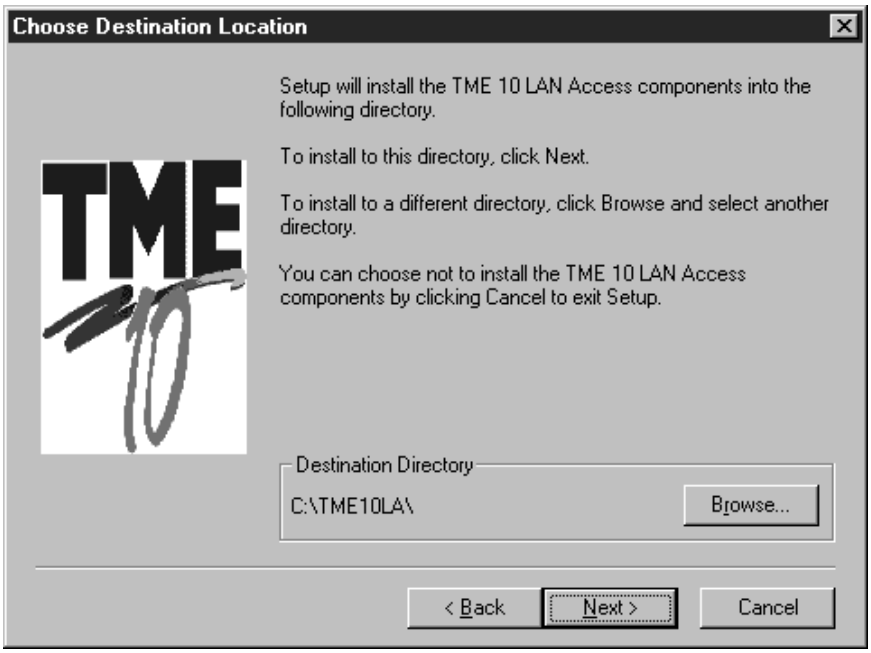


Figure 156. Netfinity Provider - Choose Destination Location

Choose the destination path where the LAN Access code will get installed. If you are not sure about the path, you can click on the **Browse** button to select the required path.

There are no restrictions concerning the file system you are installing on. It can be NTFS or FAT. In our case all of our drives were NTFS.

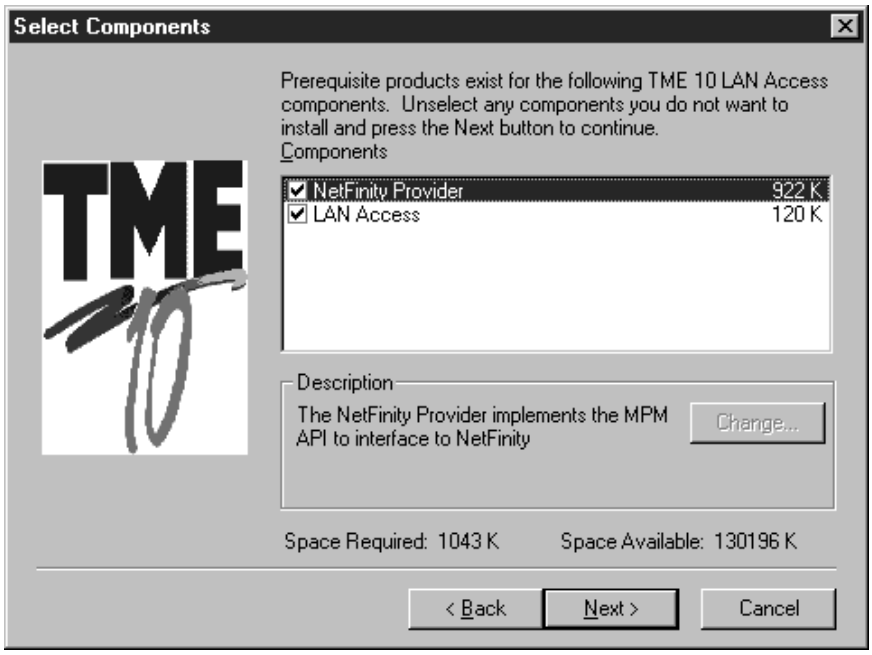


Figure 157. Netfinity Provider - Select Components (Part 1 of 2)

The option to install either Netfinity provider or LAN Access will depend upon what software is already installed on your system. In our case, the machine on which we installed the code is the provider and LAN Access site; therefore, we will get both choices. If you are installing on a machine that is not a TME managed node, you won't see this panel. Only the Netfinity provider will get installed by default.

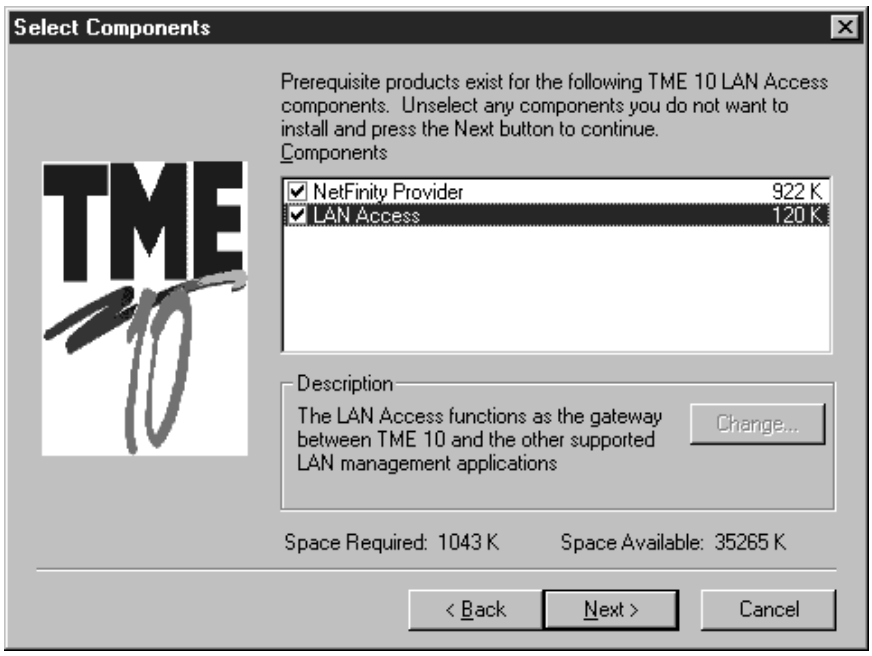


Figure 158. Netfinity Provider - Select Components (Part 2 of 2)

3.2.1 Installing on Windows 95

Installing on a Windows 95 machine is exactly the same as installing on Windows NT. You will see the same panels with the same options. Also, the environment variables are the same. We did not test out the beta code for Windows 98 nor did we use the 32-bit Windows 95 OEM code.

3.3 Installing on OS/2

Before you begin installation, make sure that Netfinity is running on the node on which the files will be installed.

To install the Netfinity provider and transport on OS/2, run \os2\install.exe from the LAN Access CD-ROM and you will get the following window:

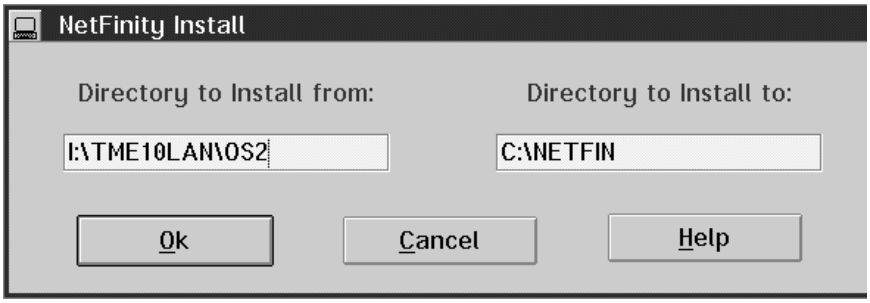


Figure 159. Netfinity Provider - Install Panel

Select the directory to install the code in. The default is to install it on the Netfinity directory.

If you don't use the default, the new directory will get created for you and the path variable will get updated for that directory.

In this case we were not presented with an option to install the LAN Access site because our OS/2 machine is not a managed node. In the future when OS/2 is able to run the framework, this option will be added.

3.3.1 Configuring the Netfinity Provider

After making your selections in the installation section, you will be asked to enter some configuration information. This procedure applies to all operating system platforms on which the Netfinity provider is installed. The Configuration program can be started manually after the installation process by running the nfprvcfg.exe program. This file is located in the directory that was chosen during the installation process (for example, C:\TME10LA\).

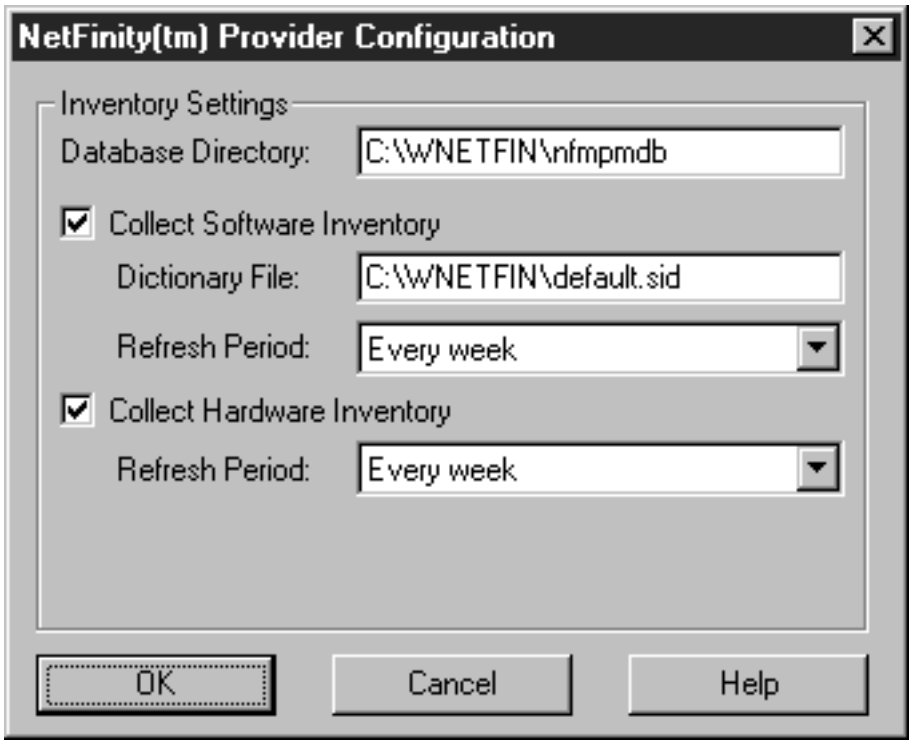


Figure 160. Configuring Netfinity Provider

The values in Figure 160 are the default values established during the initial installation. When you look at the configuration on a later date the values you select will be displayed.

- Database Directory

  If **Collect Software Inventory** is selected, this field specifies the directory used to hold the collected hardware and software inventory data (typically 50 KB per client system). This field defaults to the nfmpmdg subdirectory of the Netfinity directory (typically c:\wnetfin\nfmpmdb). Accept the default or change the subdirectory to where you want the data stored.

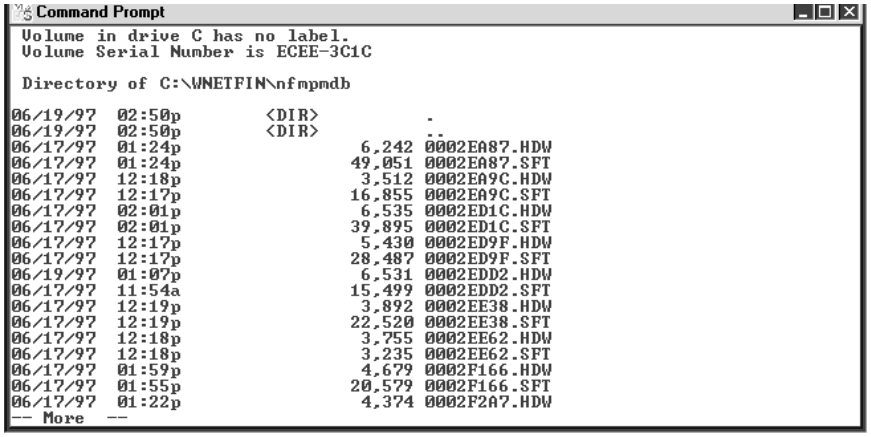


Figure 161. Database Directory

- Collect Software Inventory

Specifies whether software inventory is collected by the Netfinity provider. Select this check box to enable the collection of software inventory data. If it isn't selected, software inventory information won't get collected from Netfinity clients and therefore, it won't be available to Tivoli Inventory.

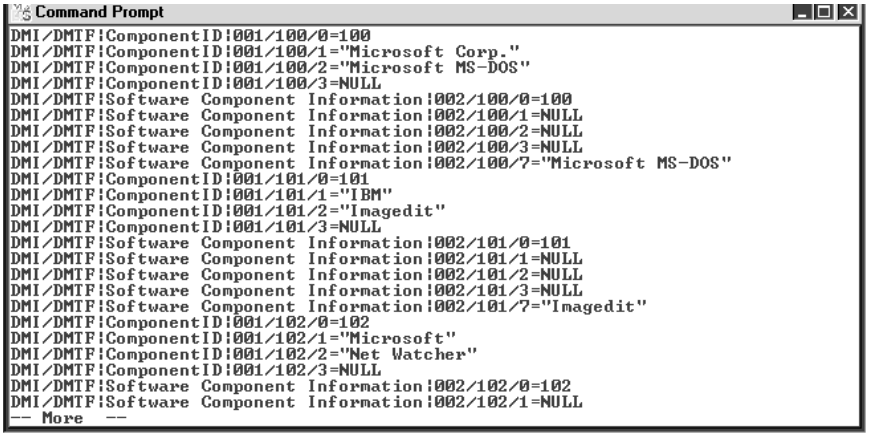


Figure 162. Part of Software Inventory

- Dictionary File

  If Collect Software Inventory is selected, this field specifies the name of the dictionary file to use when scanning systems for software. This field defaults to the software inventory dictionary provided with Netfinity. If you have defined a custom dictionary you want to apply, use this field to specify the name of the custom dictionary.

- Refresh Period

  If Collect Software Inventory is selected, this field specifies the period between re-scans of the software inventory of Netfinity clients. The following values can be selected by clicking on the list box:

  – Every hour, 4 hours, 8 hours, 12 hours

  – Every day, 2 days, 4 days

  – Every week, 2 weeks, 4 weeks, 8 weeks, 16 weeks

  Every week is the default provided by the system.

- Collect Hardware Inventory

  Specifies whether hardware inventory is collected by the Netfinity provider. Select this check box to enable the collection of hardware inventory data. If it is not selected, hardware inventory information is not collected from Netfinity clients and therefore, not available to Tivoli Inventory.

Figure 163. Part of Hardware Inventory

- Refresh Period

  If Collect Hardware Inventory is enabled, this field specifies the period between re-scans of the hardware inventory of the Netfinity clients. The following values can be selected by clicking on the list box:

  – Every hour, 4 hours, 8 hours, 12 hours

  – Every day, 2 days, 4 days

  – Every week, 2 weeks, 4 weeks, 8 weeks, 16 weeks

  Every week is the default provided by the system.

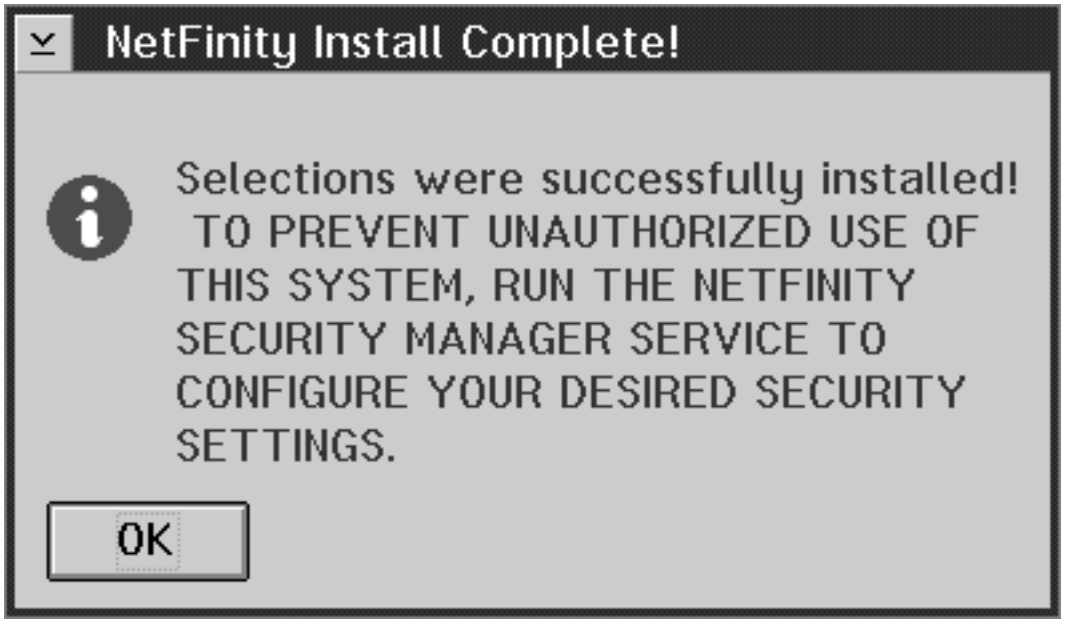


Figure 164. Configuring Netfinity Provider Finished

To make the changes take effect the system has to be restarted.

3.4 Installing the LAN Access Transport and Event Adapters

There is nothing special required to install the LAN Access Transport and event adapters. Execute the file \W32\SETUP.EXE from the LAN Access CD-ROM, and it will install all of the required files:

- tecad_msb.exe in \wnetin
- tecad_msb.map in \usr\local\Tivoli\bin\w32-ix86\TME\TEC\ADAPTERS\ETC
- tecad_msb.log in \var\spool\Tivoli\host_name.db\tmp

Also the files needed for the TME Enterprise Console are copied:

- lanacc.baroc

  Note: In the user manual this file is called lanaccess.baroc. (baroc stands for Basic Recorder of Objects in C.)
- la_netf.baroc for Netfinity
- la_ldms.baroc for Intel LANDesk
- la_sms.baroc for Microsoft SMS

You will find them in \usr\local\Tivoli\bin\w32-ix86\TME\TEC\ADAPTERS\ETC.

For more details on TEC and its interactions, see 5.1.3.1, “Example of Using the Tivoli Enterprise Console” on page 200.

Chapter 4. SMS 1.2

Microsoft Systems Management Server consists of many different components. These components can be physically spread out across different systems. The components are:

- Site server
- Logon server
- Helper server
- Distribution server
- Client

The site server is the main part of SMS. It is the location where SMS services run. It also communicates with other sites. There are two types of sites: primary sites and secondary sites. A primary site has its own database where it stores its inventory data. A secondary site sends its inventory data to its parent primary site. The site server has a folder c:\sms\site.srv.

Communication between SMS and its clients is implemented through the Windows NT logon process. When clients log on to the Windows NT domain, the SMS client pulls information from the logon server. That is why, by default, all domain controllers act as SMS logon servers. We can specify a list of servers that should act as logon servers. In our case NTSRV48 was our primary domain controller, site server and logon server. SMS also automatically detects all member servers and uses them as logon servers. As all clients logged on to our domain, no validation took place other than on NTSRV48, so in fact, NTSRV48 was the only active logon server. We can tell that it's a logon server since it has the folder c:\sms\logon.srv.

Some of the site server services may run on another computer. That system is known as a helper server. An example is the Sender service, which is responsible for communication with other sites. You can install Sender on systems that are running the RAS service, in order to off-load site server.

The SMS client can be installed on different platforms:

- MS -DOS 5.0 and higher
- OS/2 2.0
- OS/2 3.0
- Windows 3.x
- Windows NT 3.51 SP4
- Windows NT 4.0
- Macintosh

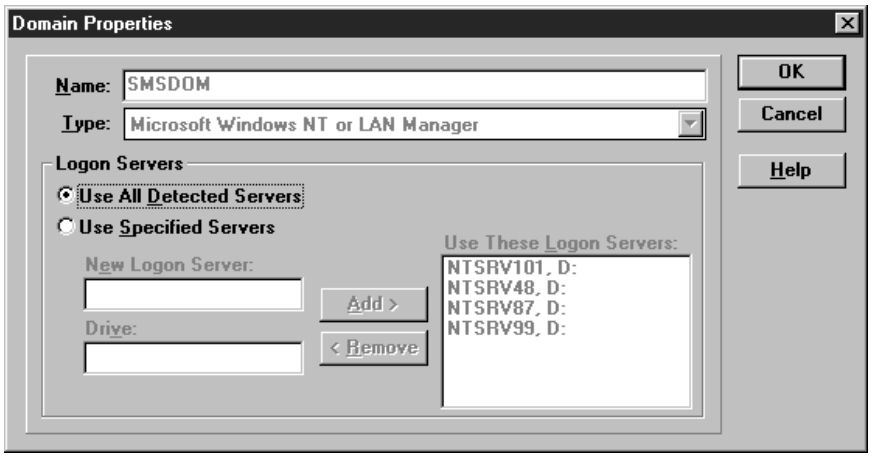


Figure 165. Servers Used As Logon Servers

4.1 Installation of the SMS Environment

For this part of the project, our environment was set up as follows:

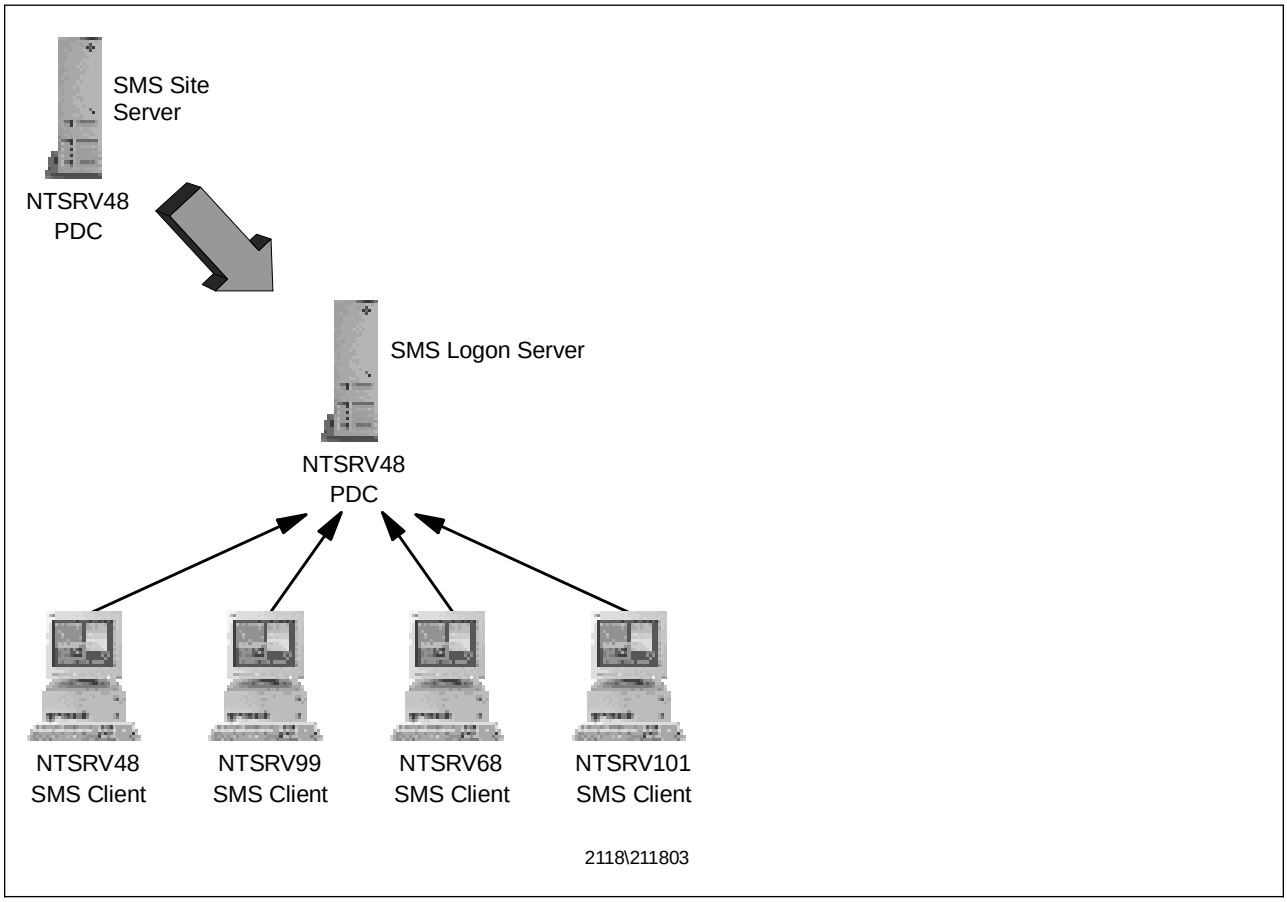


Figure 166. SMS Environment

A prerequisite for SMS installations is Microsoft SQL Server Version 6.0 or 6.5. Both SMS and SQL servers require a special user account. During each installation we had to specify those accounts. Because they both require the same privileges

we created just one ID and used it for both system applications as shown in Figure 167 on page 143. We used SQL 6.5 with Service Pack 4 in this environment and SMS with Service Pack 3.

The SMS server relies on Windows NT services directory replication and domain logon process. That is why we had to set up directory replication and install SMS server on the domain controller. Directory replication also needs a special account.

To create a database, SMS needs two database devices: one for the data and one for a transaction log. We can create these devices with SQL Enterprise Manager or they can be created automatically by the SMS server installation. A disadvantage of using the automated creation process is that you don't see any SQL server error messages, which is why we created the database devices ourselves.

4.1.1 Installation of Microsoft SQL Server

Before installing SQL server we created a user account for SQL services. We put the account into the Domain Admin group. We set its password to never expire and the user cannot change the password. This is because if somebody changes the password for this account, the SQL services will fail to start.

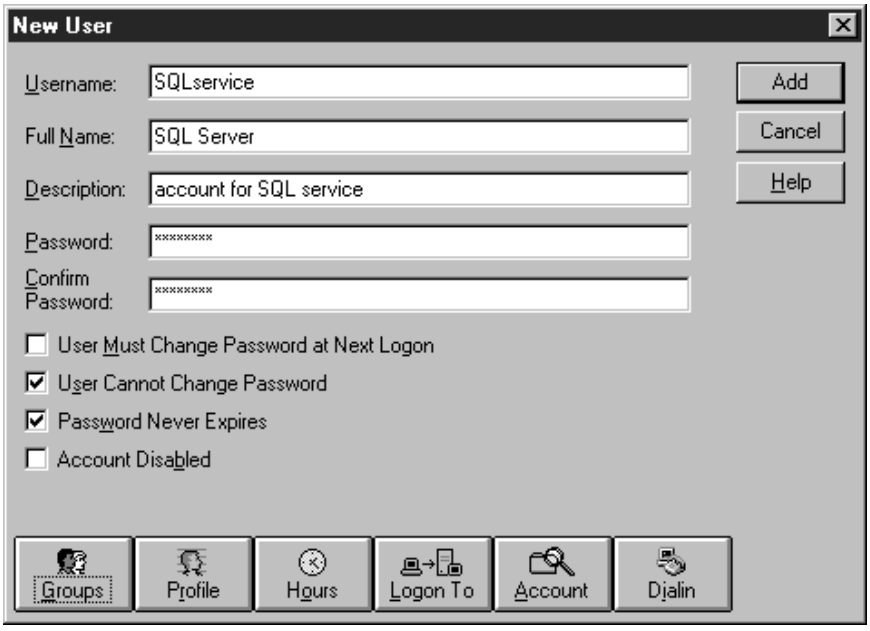


Figure 167. NT 4.0 User Manager Options or SQL User ID

We installed SQL server by executing setup.exe from the V6.5 CD. The first thing we needed to do was to specify the size of the master device. This is the device where all system tables will be located. The minimum size is 25 MB but it is good idea to set it higher because it can't be increased without reinstalling. We set it to 35 MB.

Note: If you are installing SQL 6.5 and SMS 1.2 from the Windows NT Backoffice 4.0 CD, most of the processes in this section are done automatically for you. The installation of the code, the set up of the user IDs and the installation of the service packs are all integrated into the Backoffice CD installation process.

On the next menu we set Character set and Sort order. All databases that are created on the SQL server have the same setting. You can choose a default. The sort order has an impact on queries you will perform with SMS. If you say that the sort order is case-sensitive, then the result of queries will also be case-sensitive. We also chose to start the SQL Server service and SQL Executive service at boot time. If you change your mind, you can easily modify the startup from the Windows NT Services window.

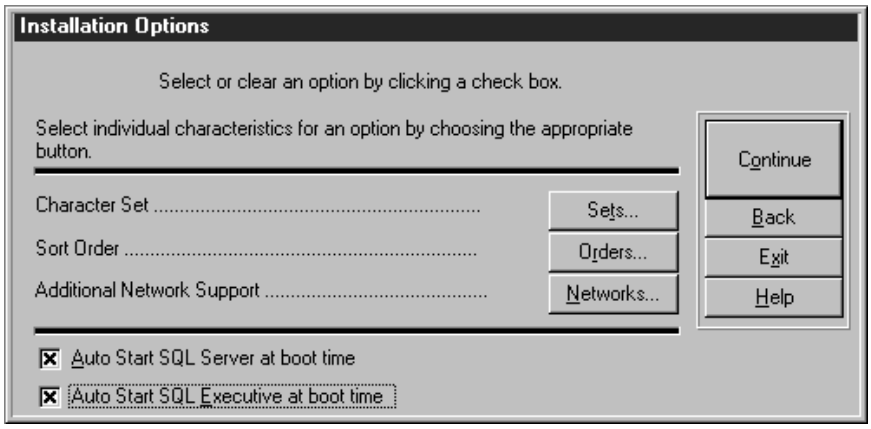


Figure 168. SQL 6.5 Sort Order

For the installation path we accepted the default path.

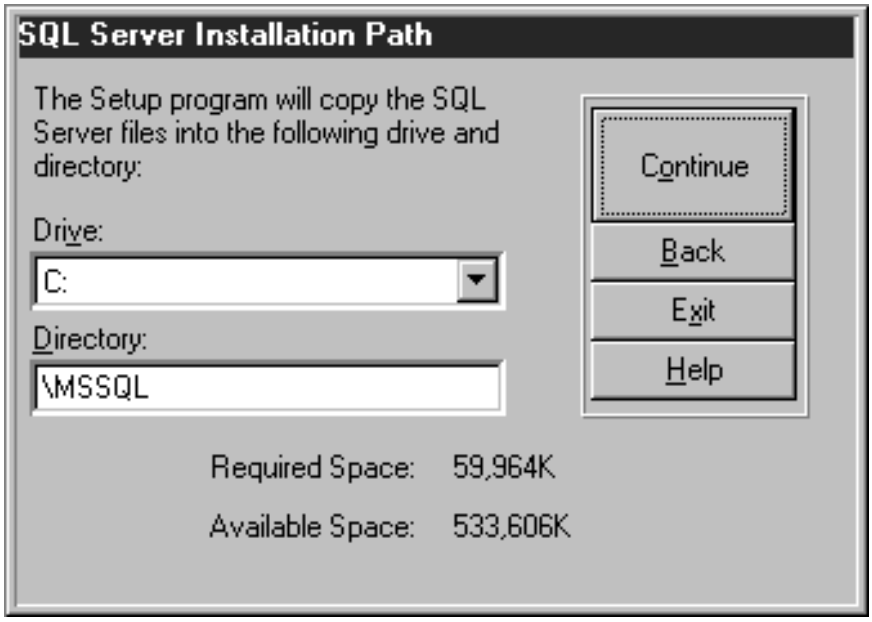


Figure 169. SQL Installation Path

The message in the following window indicates that the installation of SQL server is complete.

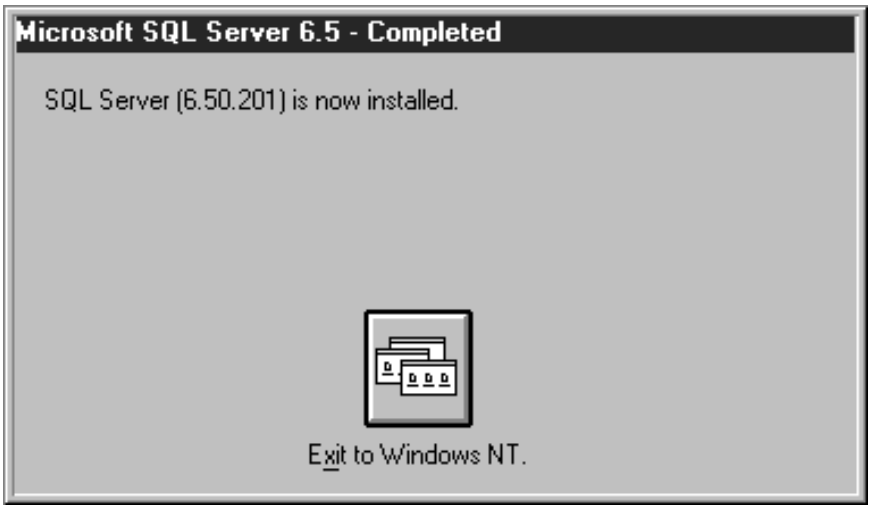


Figure 170. SQL Installation Complete

After rebooting you should apply the maintenance and then continue on with your customization.

4.2 Configuration of SQL Server

Before we can use the SMS server we have to modify these SQL server parameters:

- User connections
- Open objects
- Memory
- Size of temporary database (tempdb)

Note: See Appendix B, “Microsoft Information” on page 275 for a useful tuning article from the Microsoft Knowledgebase.

During installation the SMS server requires up to 20 connections. You need 5 connections per administrator. The default value is 15. We changed it to 30 for our installation. The connections are used by the SMS Services and the SMS administrator. If you need more information on connections, you can look at the online documentation that is installed with SMS.

The number of open objects determines how many tables, views or stored procedures can be opened at the same time. We left the default value of 500 objects since we did not have a big site to manage.

You can specify how much memory should be allocated to the SQL server. The unit size is 2K and the default value is 4096 units (8 MB). We changed it to 16384 units (32 MB).

The size of the temporary database should be at least 20 percent of the size of the SMS database. A larger temporary database improves performance. We set the size of tempdb to 20 MB.

To configure the SQL server you should start SQL Enterprise Manager. The first time you start it, it will ask you to register the SQL server. The default name of the

SQL server is the NetBIOS name of the server running SQL server. The default name of the SQL administrator is sa and there is no password. You should add a password as part of your normal security process.

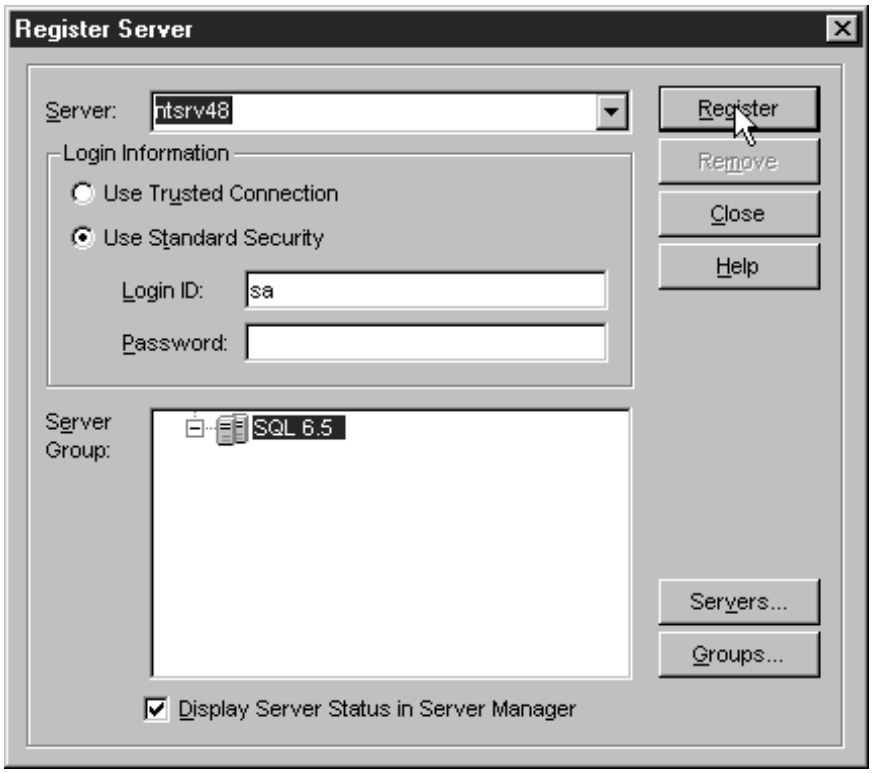


Figure 171. Security for the System Administrator User ID

You should right-click on the SQL server and click on **Configure**. The Tab key lets you choose configuration values.

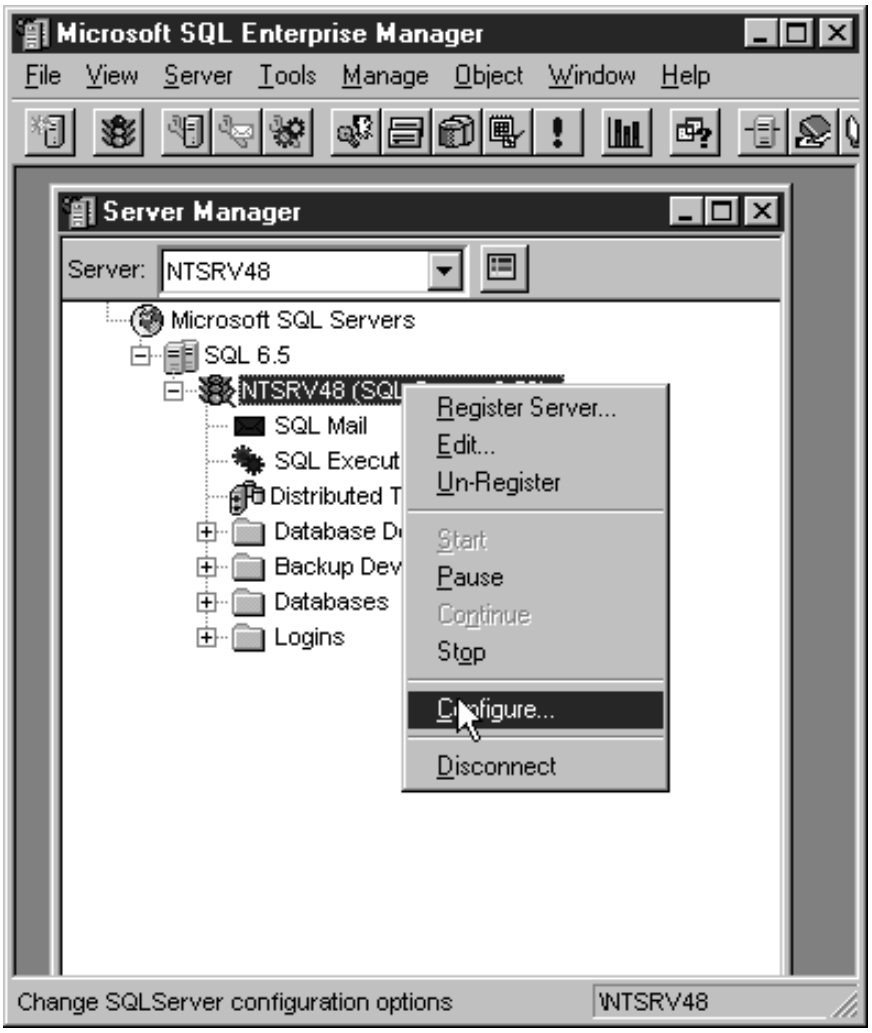


Figure 172. Configure the SQL Server

As you can see in Figure 173 on page 148 we changed a few of the values.

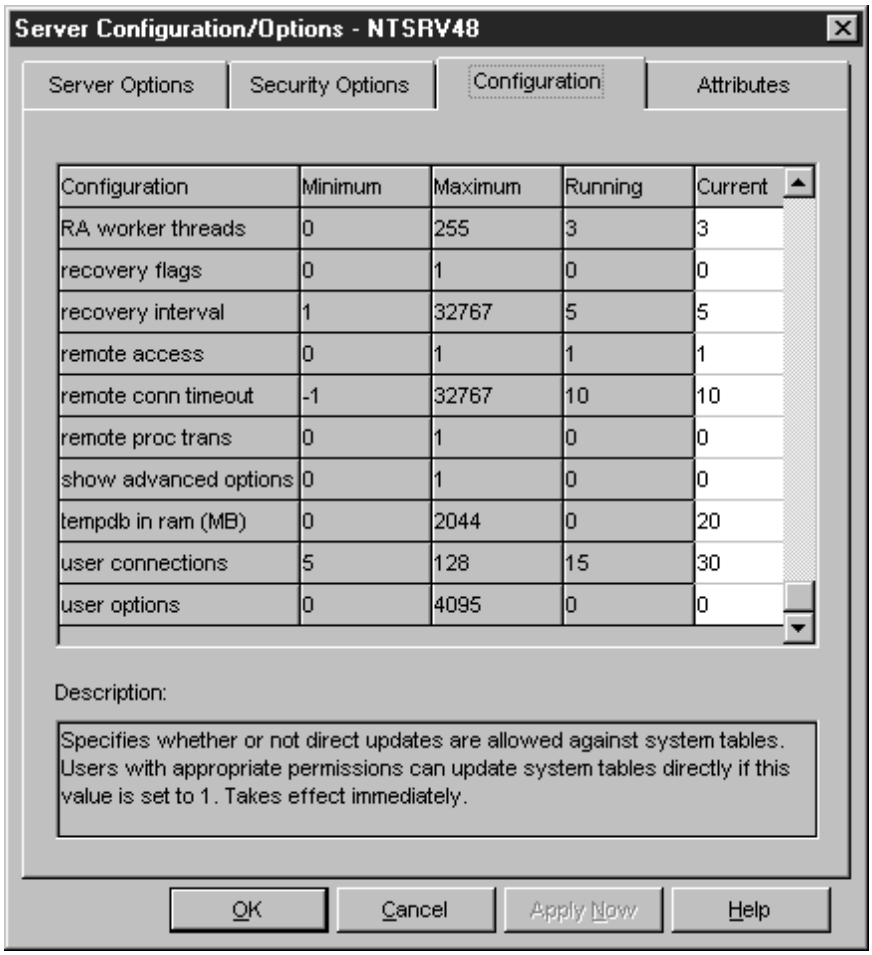


Figure 173. SQL Server Configuration

4.3 Setting Directory Replication

Before you start installing SMS server you should set up the directory replication service. We suggest you use Service Pack 3 for Windows NT since the base release replication service has problems accessing export and import folders.

You should create a user account for the replication service and put it into the backup operators and replicator local groups.

The SMS server creates all user logon scripts on the site server in the directory winnt\system32\repl\export\scripts. We had to replicate this directory to all logon servers in winnt\system32\repl\import\scripts. In our case NTSRV48 was acting as the PDC, SMS site server and SMS logon server. We had to replicate the c:\winnt\system32\repl\export\scripts folder to the c:\winnt\system32\repl\import\scripts folder. You should create one file in the c:\winnt\system32\repl\export\scripts folder. If it is replicated to the c:\winnt\system32\repl\import\scripts folder, then you can proceed with the SMS installation.

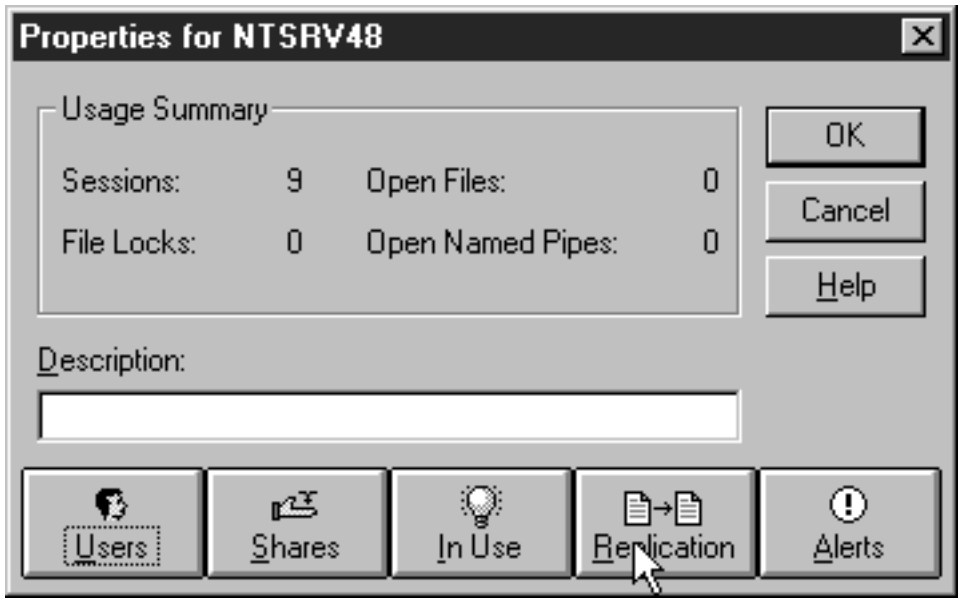


Figure 174. Configure Directory Replication

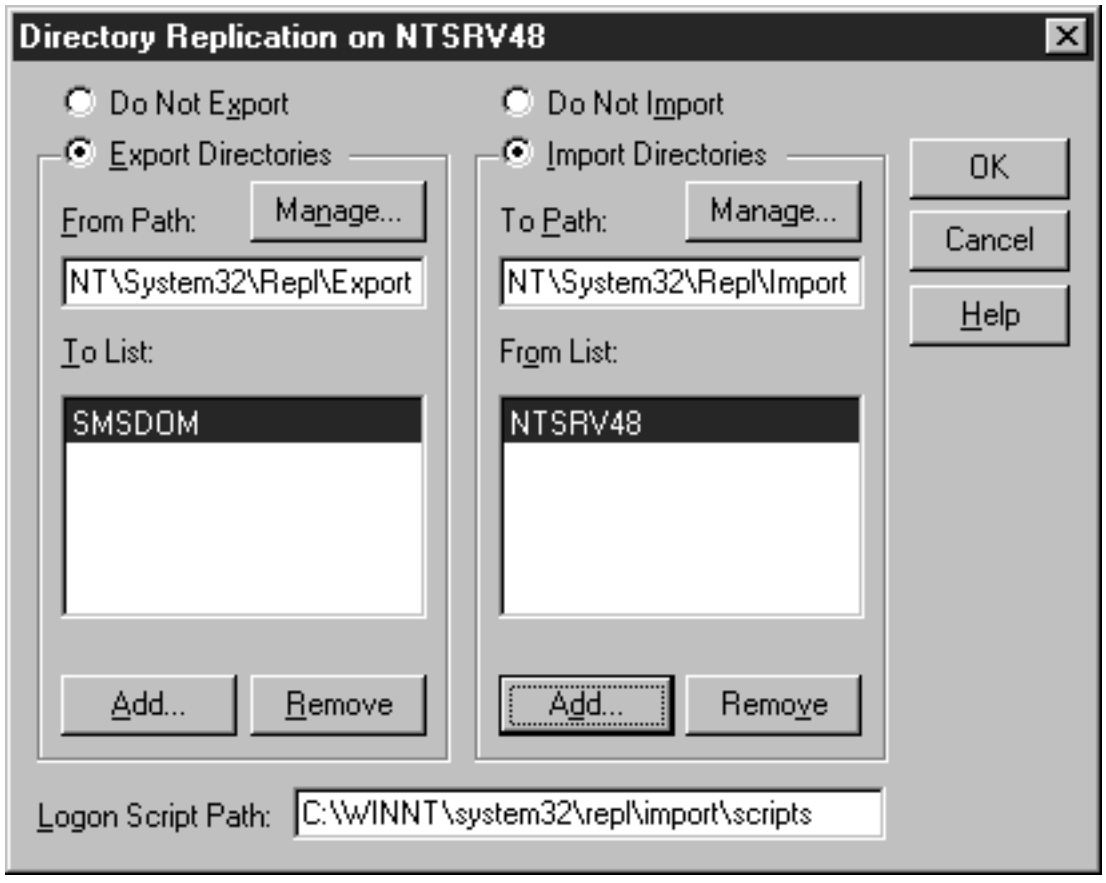


Figure 175. Directory Replication

4.4 Installation of Microsoft Systems Manager Server V1.2

To install Systems Management Server we had to create a user account on Windows NT that is used by SMS services. Since we are using the SQL server exclusively for SMS, we used the same account. Otherwise, we would have created separate accounts. It makes sense in a production environment to have them as separate accounts.

From the product CD we ran setup.exe and chose **Install a Primary Site**.

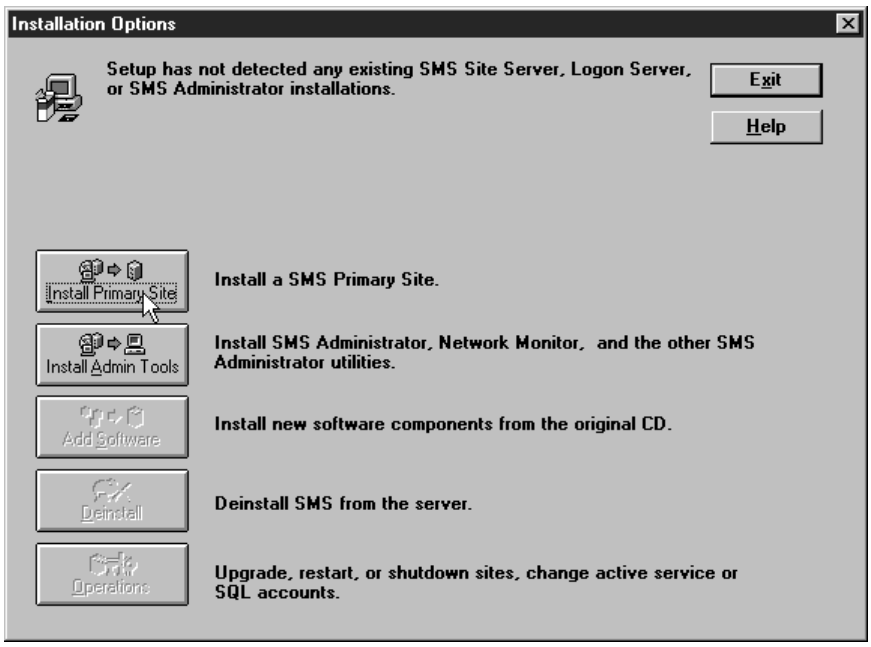


Figure 176. Install the SMS Primary Site

We accepted the default SMS components. As none of our clients were PowerPC or Digital Alpha we chose to install only code for Intel processors.

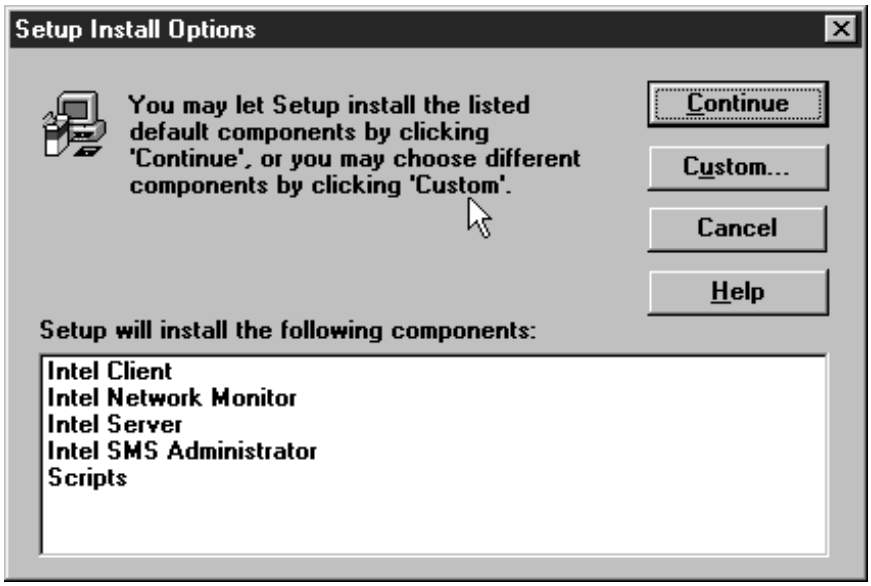


Figure 177. Setup Install Options

Next we needed to enter information that the SMS server needs to access the SQL server. The SQL Server name is the name of server where SQL is running. In our case it was ntsrv48.

SQL Login is an account defined inside SQL server. The default SQL account created at SQL server installation is sa with no password. This account has access to all SQL data so you should immediately change its password. Also you might create another SQL account for SMS. It needs the following rights:

- Create database
- Dump database
- Dump transaction log

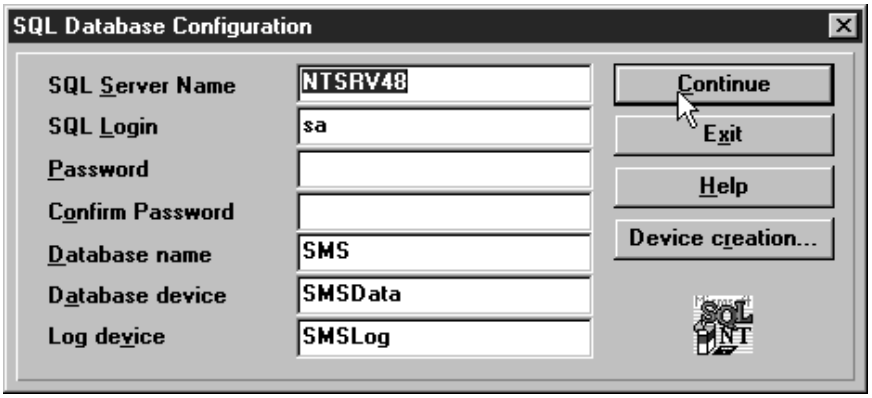


Figure 178. To Connect to the SQL Database

Next we needed to enter SMS site information. The Site Code is three characters that must be unique within the SMS hierarchy. The Site Name field is just a description field. The Site Server is the name of the computer where we want to install a primary site (the main part of the SMS server). The Site Server Domain is the NT domain name of the site server. For example, if we want to create a primary site on computer NTSRV48 and computer NTSRV48 is a member of domain SMSDOM, then we need to enter SMSDOM.

Note: Be careful of the Automatically detect all logon servers check box. If it is checked, SMS will automatically detect all logon servers and will install logon servers on them. If you don't want all logon servers to participate in SMS, then don't check that box.

The Service account (SQLservice) is an account that will be used by SMS services. It needs to be a member of the Domain Admin global group or the administrators local group. If all SMS servers and NT clients are members of one domain, then it is enough to put this account in the Domain Admin global group. Otherwise, we need to put it in the administrators local group.

Since we used the SQL server exclusively for the SMS server we used the same account as for SQL server, which is why its name in Figure 179 on page 152 is SQLservice. As was mentioned earlier, for a production environment you should consider using separate IDs.

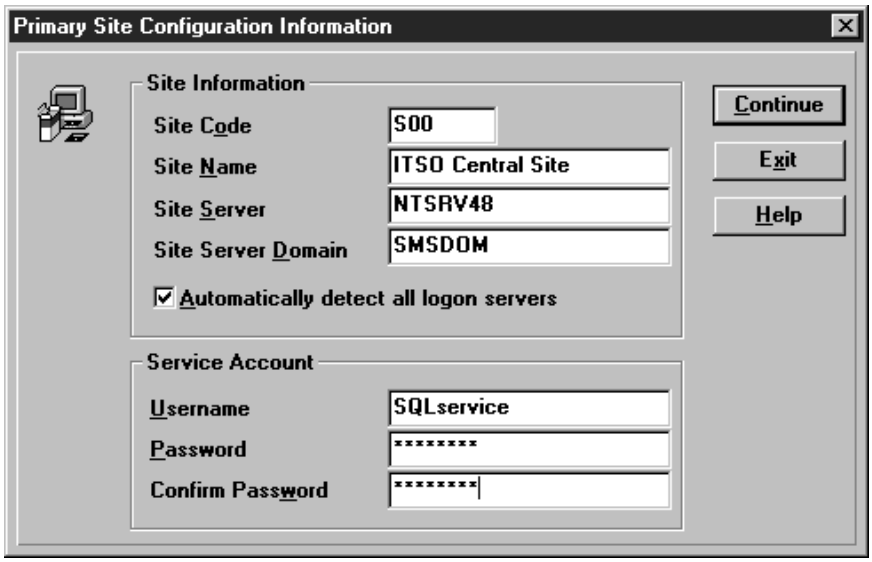


Figure 179. Site Information

4.5 Configuring SMS for LAN Access Integration

For LAN Access to work with SMS, several things must be done on the SMS server.

4.5.1 Enabling Software Distribution

To enable software distribution to SMS clients from the Tivoli desktop, you need to specify a directory on the SMS site accessible to all LAN clients. It will be used by LAN Access to create the packages for distribution. SMS also creates a directory used for distribution, named Sms_Pkgd on all distribution servers (in our case ntsrv48). The directory specified for LAN Access cannot be the same one. We created a directory called Tme_Pkgd and shared it, but this directory can have any name. The only important fact is that all LAN clients have at least read access to it. This directory must be created prior to the installation of LAN Access components, during which, as is shown in 4.7, “Installation of LAN Access Components on the SMS Site” on page 171, you will be prompted for it.

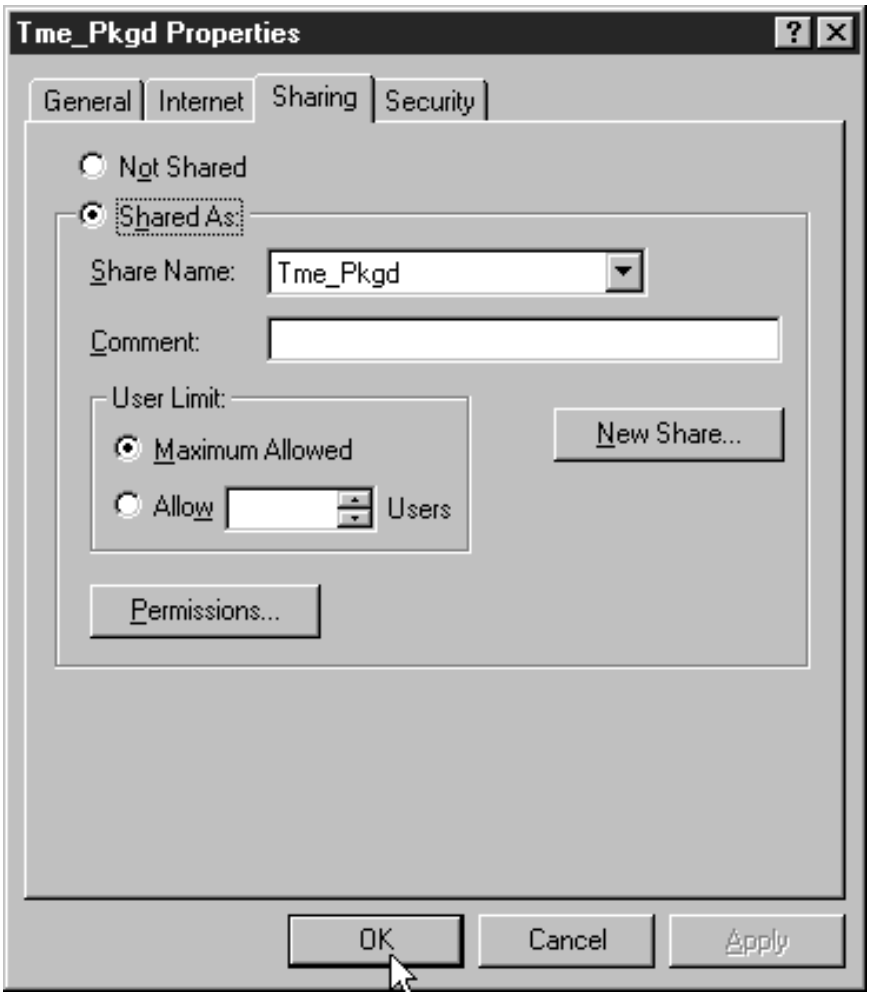


Figure 180. Creation of a Shared Folder

4.5.2 Enabling Inventory

LAN Access collects software inventory information about SMS clients from the SMS database under the audited_software group. This means that to be able to retrieve software inventory data on LAN clients from the Tivoli desktop, the SMS administrator must run an SMS software audit on the LAN clients.

To run the SMS software audit, SMS has to scan its clients for software inventory information using a software signatures file, called audit.rul. You can edit this file if you want additional signatures added.

Note: Installing new SMS service packs replaces AUDIT.RUL, so to make sure you don't loose your changes if you install service packs, you should save the file with a different name.

To perform a software audit you need to compile the audit.rul file and then prepare a software package to distribute to the SMS clients with the software signature file and the executing instructions for the scan.

Following is a piece of the AUDIT.RUL file:

```
package 0 "1-2-3 5.0 English (International) Win16, Lotus Development"
    file "L14CLS.DLL" size 312368 crc 62473 187422 64595
    file "C1WUIMGR.DLL" size 179888 crc 35977 107934 33668
    file "LGALLERY.BMP" size 151670 crc 30334 91003 60360
```

First you have to compile audit.rul by running the rul2cfg.bat batch file.

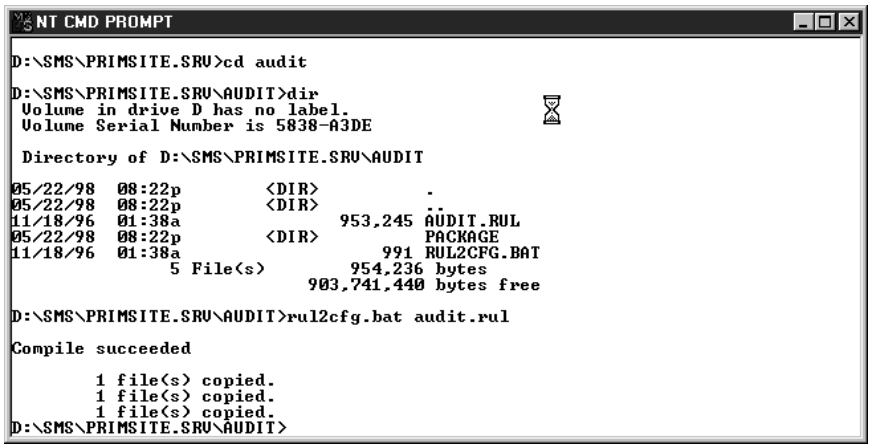


Figure 181. Compilation of audit.rul

The output file name will always be audit.cfg.

Next you need to define a software package. Since software auditing is a very common procedure, Microsoft has already defined a package for you, called audit.pdf (package definition file). You will find it in the SMS\Primsite.srv\Import.src\Enu folder.

```
[PDF]
Version=1.0

[Audit Setup]
CommandLine=audit.bat
CommandName=Audit Software
UserInputRequired=FALSE
SupportedPlatforms=MS-DOS 5.0, MS-DOS 6.0, MS-DOS 6.2, Windows 3.1,
               Windows95, Windows NT 3.1 (Alpha), Windows NT 3.1 (MIPS),
Windows NT 3.1 (x86)

[Package Definition]
Product=Audit
Version=1.00
Comment=Audit 1.00
SetupVariations=Audit
```

Figure 182. audit.PDF Contents

In the SMS Administrator application you should click on **File, Open** and select **Packages**.

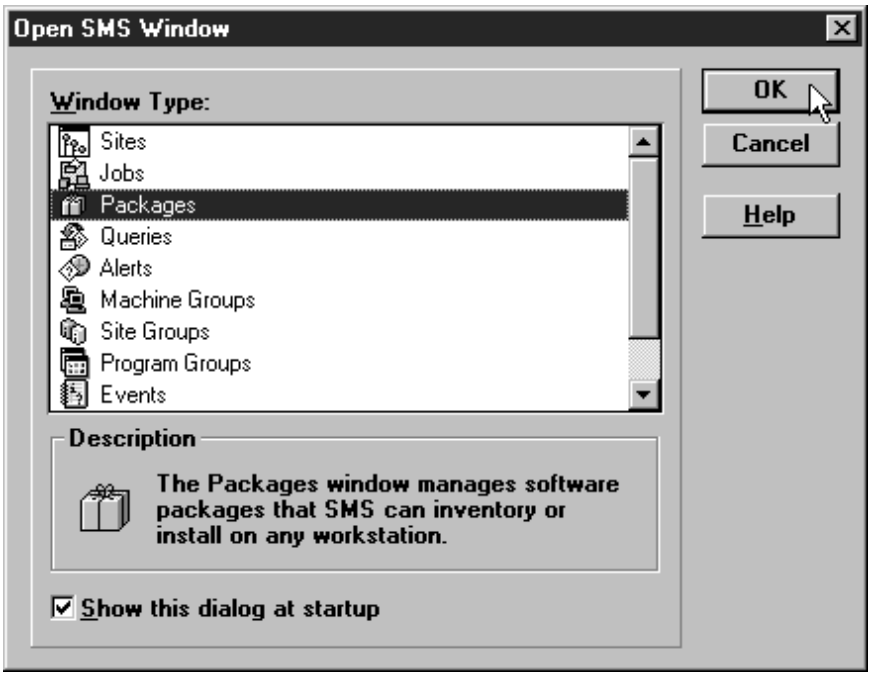


Figure 183. Open SMS Window

With the Packages window active in the SMS Administrator console select from the menu bar **File->New** to create a new package. In the Package Properties window click on the **Import...** button.

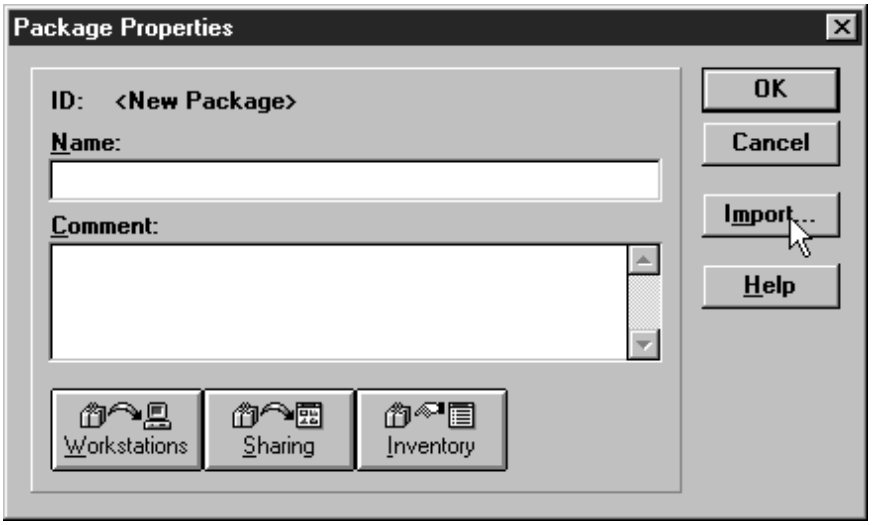


Figure 184. Package Properties

Select **audit.pdf** as the import file from the SMS\Primsite.srv\Import.src\Enu folder and click **OK**.

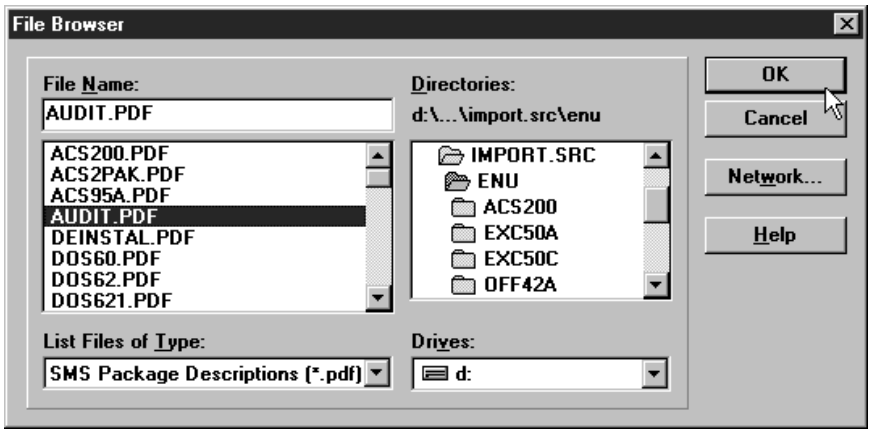


Figure 185. Importing a Package Definition File

Next you should click on the **Workstations** button shown in Figure 184 on page 155 to specify the source folder and the command that will be run on the clients. Since you have imported a package, the executing instructions are already defined and you only need to specify the source folder.

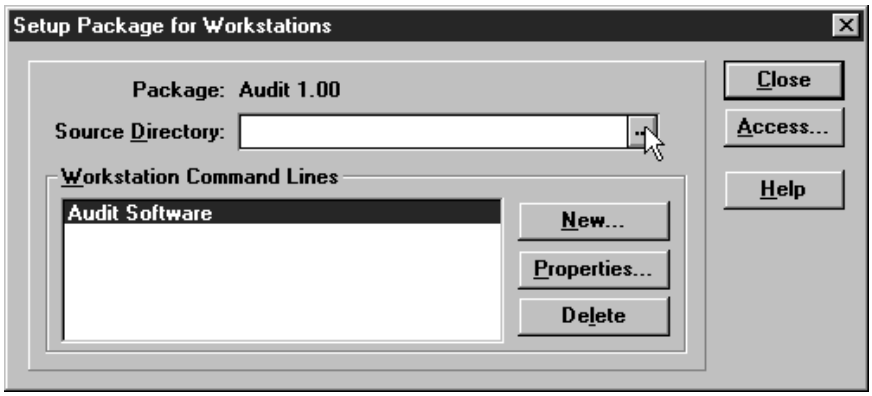


Figure 186. Specifying Source Folder

You can click on the button next to the Source Directory field to display the Directory Browser to look for the source directory.

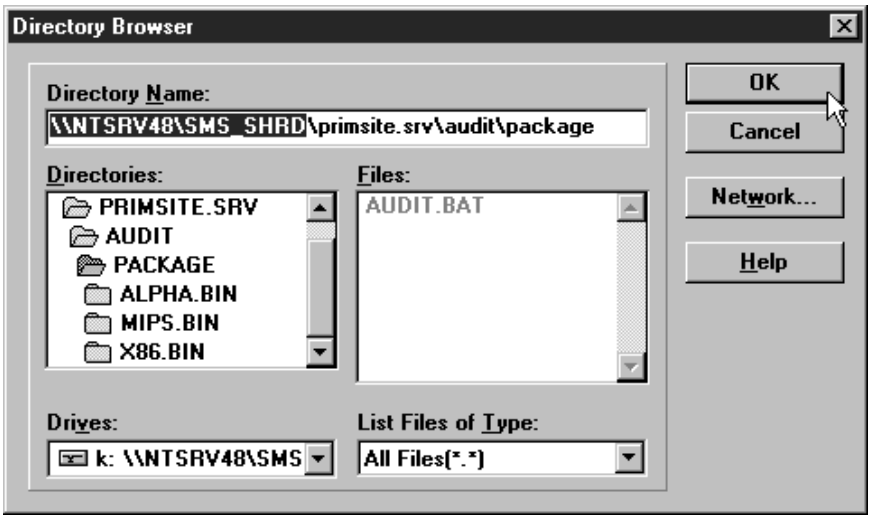


Figure 187. Directory Browser

In the Directory Name field enter `\\servername\SMS_SHRD\primsite.srv\audit\package` where servername is the name of your SMS site server. Click on **OK** to go back to the Setup Package for Workstations window. A piece of the audit.bat file follows:

```
@echo OFF
REM Copyright (c) 1993, 1994 Microsoft Corporation
echo Microsoft Systems Management Server (SMS)
echo Software Auditor
if "%OS%" == "Windows_NT" goto NT_PLAT
X86.BIN\audit16.exe
goto end
:NT_PLAT
if "%PROCESSOR_ARCHITECTURE%" == "ALPHA" goto AUD_ALPHA
if "%PROCESSOR_ARCHITECTURE%" == "MIPS" goto AUD_MIPS
if "%PROCESSOR_ARCHITECTURE%" == "x86" goto AUD_X86
echo Unable to determine operating system or processor architecture.
echo Consult your network administrator.
pause
goto END
:AUD_ALPHA
ALPHA.bin\audit32.exe
GOTO END
:AUD_MIPS
MIPS.bin\audit32.exe
GOTO END
:AUD_X86
X86.bin\audit32.exe
:end
```

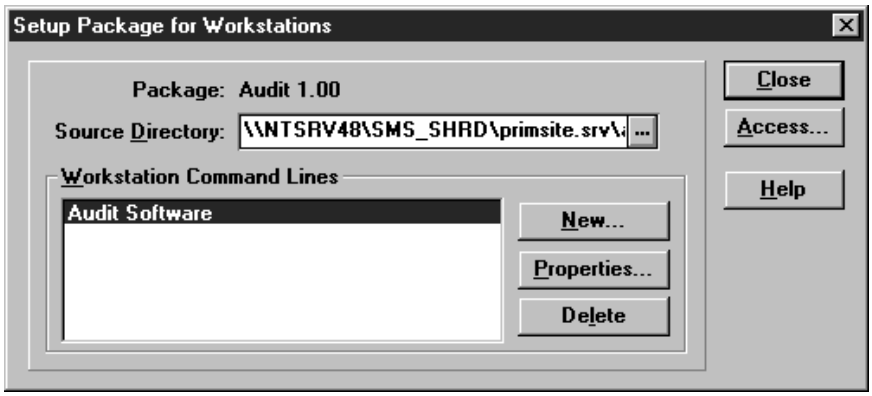


Figure 188. Specifying Source Folder

Click on **Close** and in the Package Properties window, click on **OK**. The SMS server will ask you if it is OK to update all sites with this package. You should click **OK**.

Now that you have created the package, you must distribute it. To do so, start by selecting from the menu bar **File, Open** and from the Open SMS Window select **Jobs**. Click on **File** and **New** to create a new job.

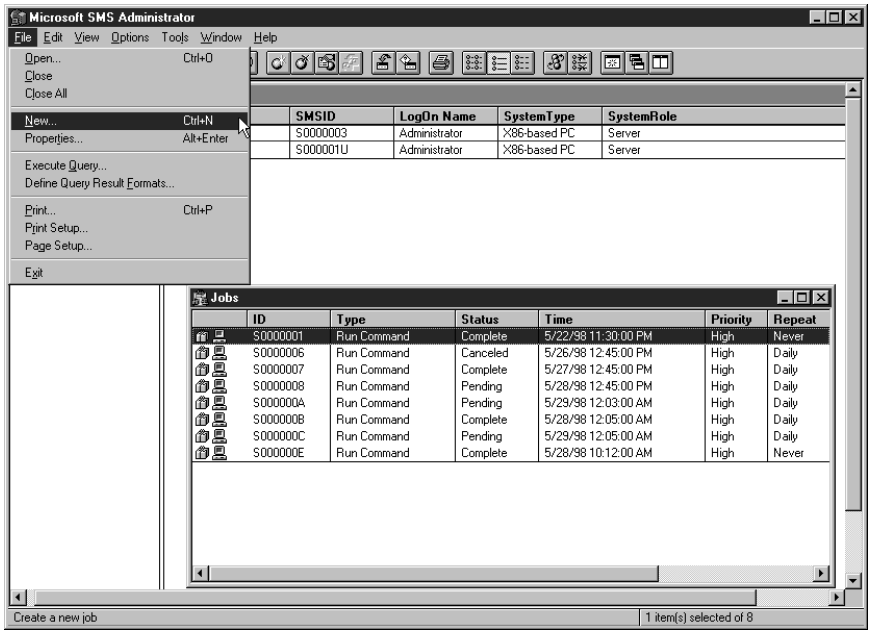


Figure 189. Creating a New Job

You can enter a comment. Make sure that in the Job Type field, **Run Command on Workstation** is selected. SMS software distribution is merely just a distribution of files and the execution of a command.

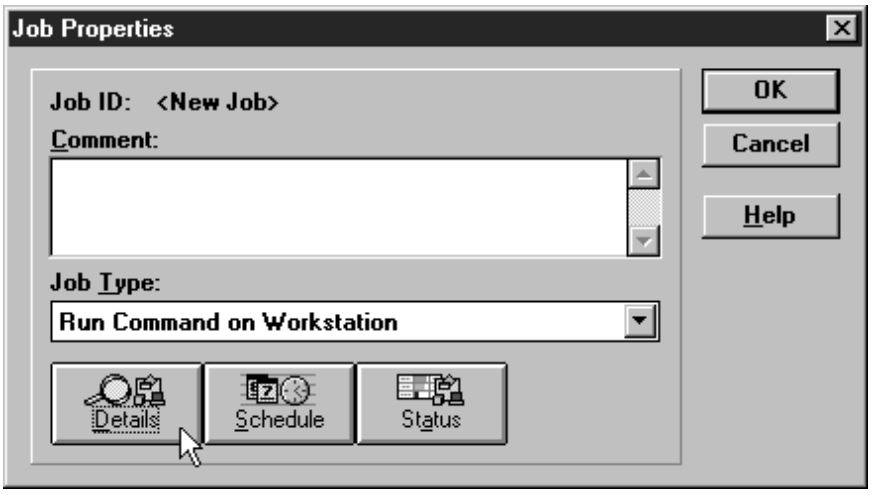


Figure 190. Job Properties

Click on the **Details** button to display the window where you can specify details about the job. The results are in Figure 191 on page 160. The description of the fields in that window follows:

- Make sure that in the Package field, the name of the package you just created (Audit 1.0 in our case) appears.
- In the Job Target fields you can leave the default values (*|*|* stands for all computers) or you may change it if you do not want all computers to receive the package.
- In the Send Phase we chose the **Even if Previously Sent** radio button, which means even if the targets already got the package, it will be sent again.
- In the Distribute Phase, we selected both check boxes.

  The package will be put on distribution servers. (In our case only ntsrv48 is a member of the default servers group.) Even if the distribution servers have the package they will receive the new version.
- In the Run phase you should check the **Run Workstation Command** check box.

  Make sure that the Audit Software command is selected. (You did not need to define the command since you had imported the package.) You can select Offer, Mandatory or Expires time.

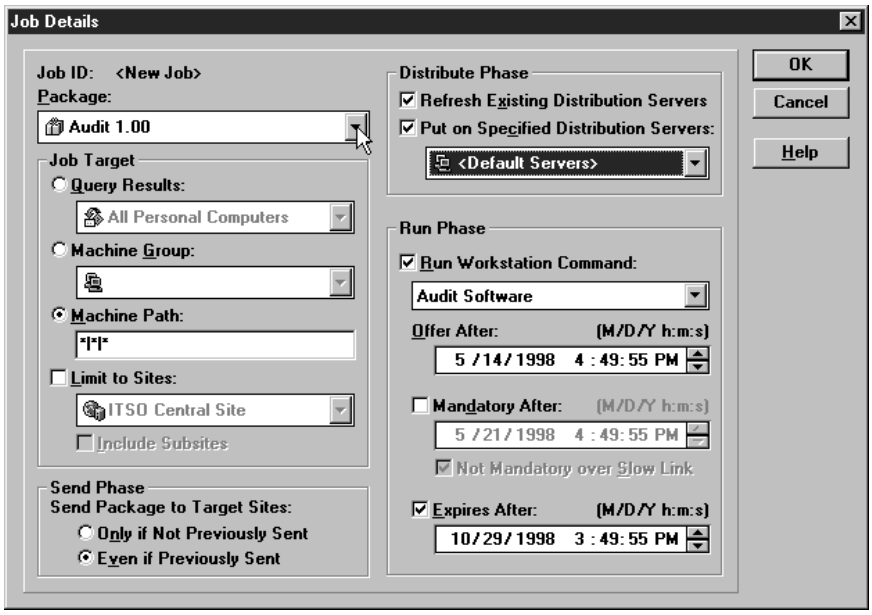


Figure 191. Job Details

After updating all the fields in Figure 191 click on **OK**. When SMS asks you if it is OK to update all sites with this job you should click on **OK**.

Note: You can monitor the status of the job in the Jobs window.

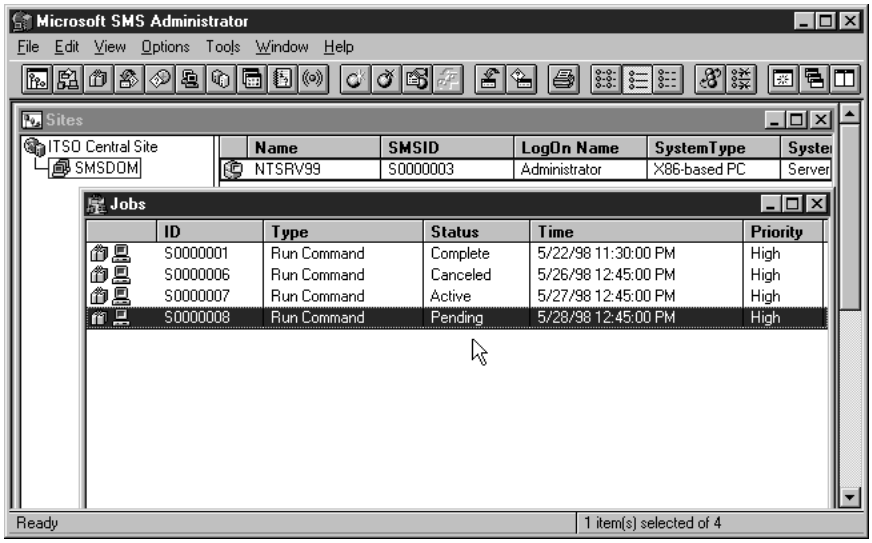


Figure 192. Jobs Window

The initial status of the job will show as pending. That means that the job has not been picked yet by the SMS Scheduler. If you see this status for more than half a day, you should check if all computers have clocks synchronized with the SQL server.

When the status changes from Pending to Active, the Scheduler starts to distribute the package.

If the package was successfully distributed and a client has selected it, the Package Command Manager will pop up in the client's monitor to show the new package in the Pending Commands folder.

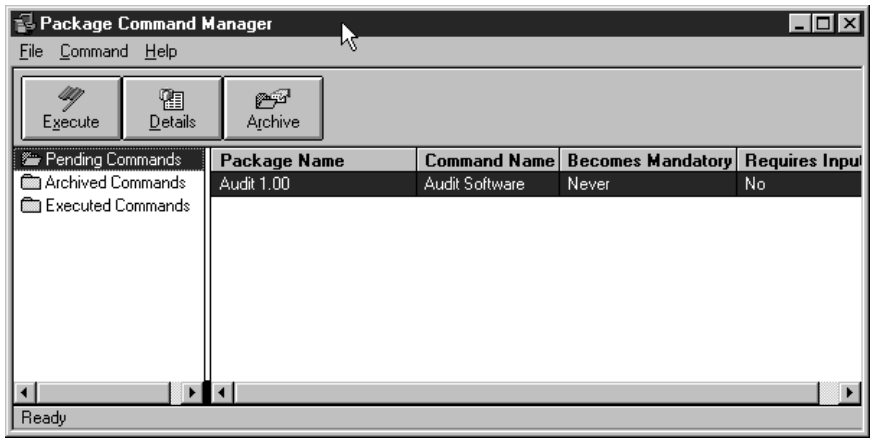


Figure 193. Package Command Manager - Audit Software

You can set how frequently the Package Command Manager that is installed on the SMS client checks for new packages in the distribution server. By default this value is 60 minutes. To change the frequency of this polling interval select from the menu bar of the Package Command Manager **Command->Options**.

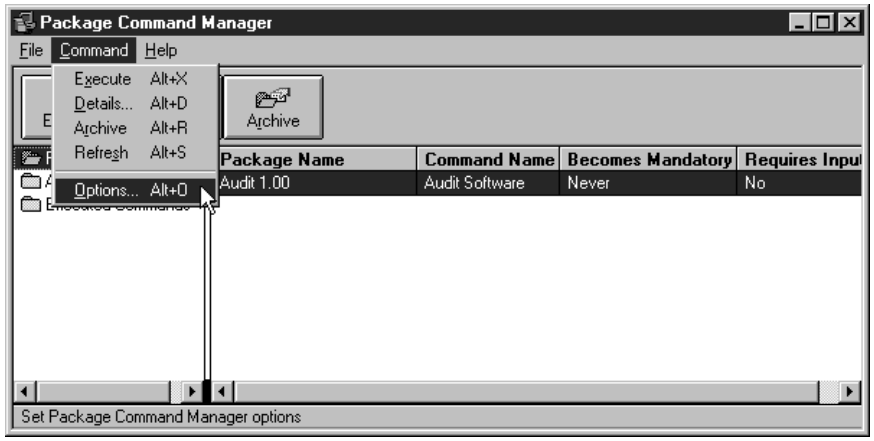


Figure 194. Modifying the Polling Interval

Update the value in the field provided. In this case we changed it to every 10 minutes.

Figure 195. Package Command Manager Options

If you did not modify any of the fields in the Jobs Details Window (see Figure 191 on page 160), by default new jobs are not executed, so you will need to select the **Execute** button on the Package Command Manager to execute the Audit 1.0 package and start the auditing process.

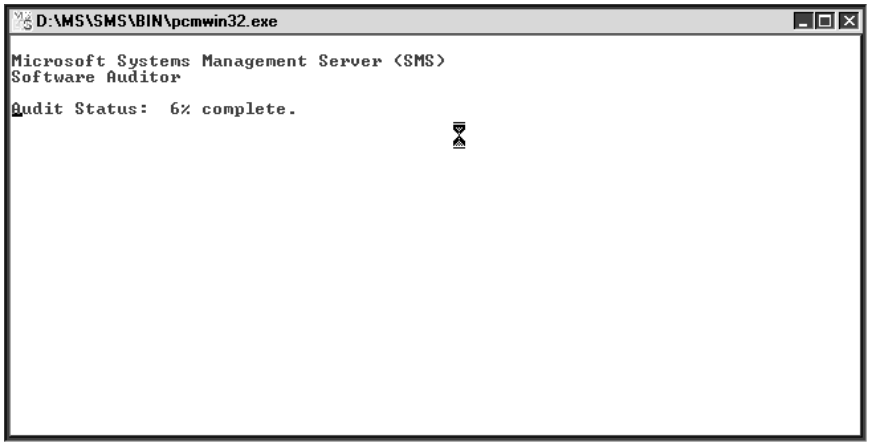


Figure 196. Audit Status

The auditing results will be reported to the SMS site server (through the login server) the next time an inventory scan is performed. By default, inventory is performed every 7 days but we show you how you can change this value.

Select **File->Open** from the menu bar in the SMS Administrator console. Choose **Sites** in the Open SMS Window. Highlight your site and select **File->Properties...** from the pull-down menus to display the Site Properties window.

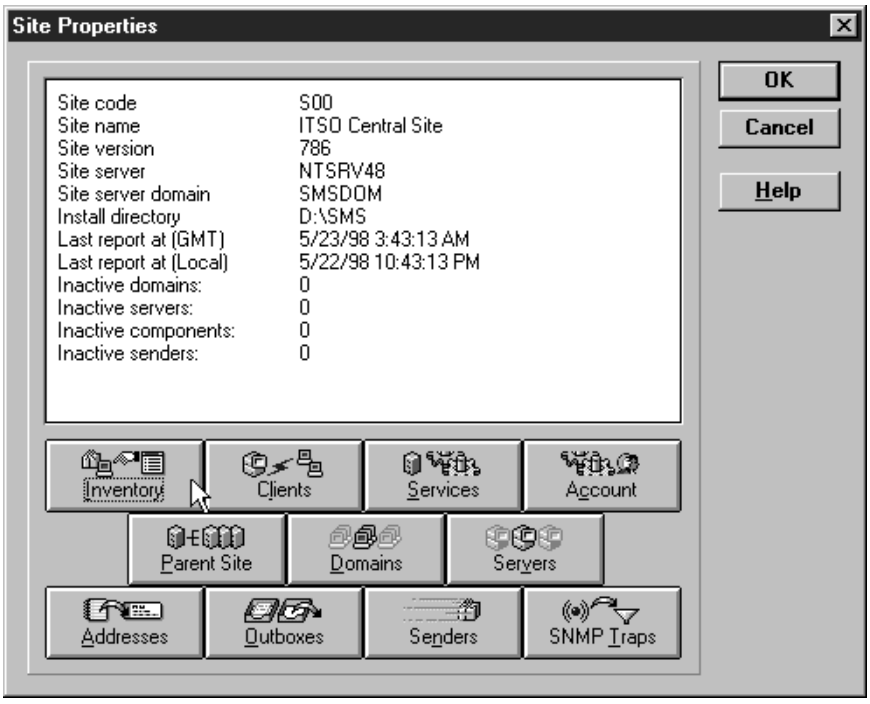


Figure 197. Site Properties

Click on the **Inventory** button. The following window will appear:

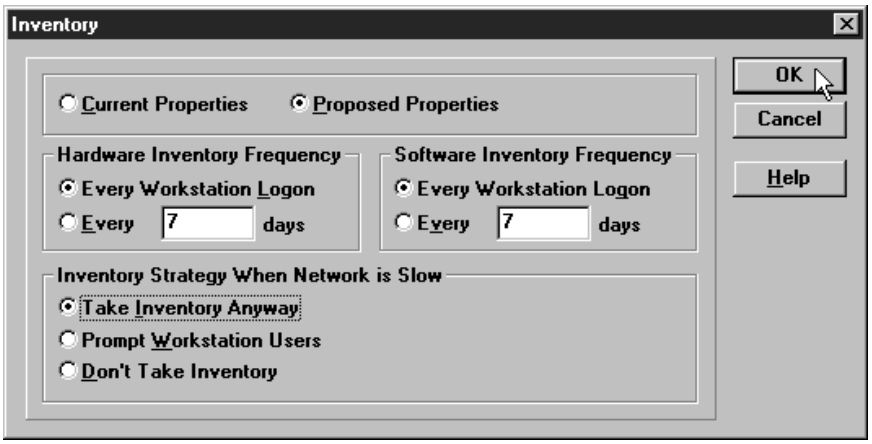


Figure 198. Inventory Window

Clicking on **Proposed Properties** enables the fields to be changed. We changed this interval to Every Workstation Logon. Click **OK** to exit.

To see the results of the software audit immediately, you can log off and log on to the Windows session.

In the SMS Administrator window click on **File** and **Open** and then choose sites. Double-click on the icon for your domain (ours was SMSDOM) found in the left pane of the Sites Window. On the right pane of this window are all the systems in that domain.

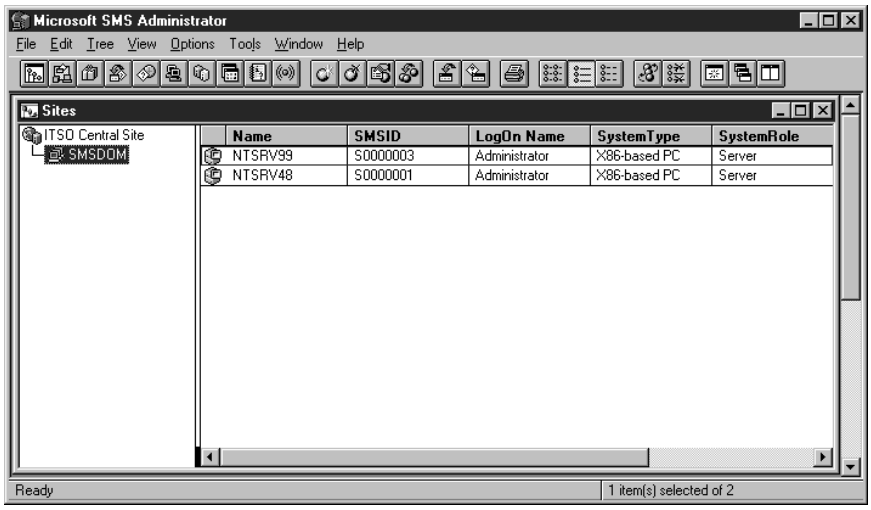


Figure 199. Sites Window - Systems in Domain SMSDOM

Double-click on a system to get the Personal Computer Properties. Scroll down the panel on the left to look for the **Audited Software** icon. Double-click on this icon to see the results of the software audit.

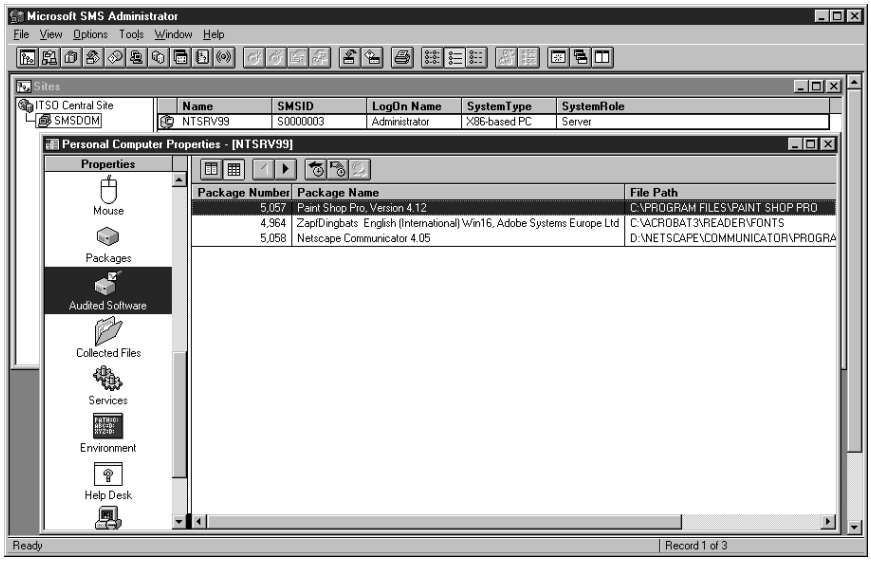


Figure 200. Results of Software Auditing

Now the software inventory information for the clients is in the SMS database under the audited_software group and the SMS provider will look there for it. With this done, we will be able to retrieve the LAN clients software inventory data from the Tivoli desktop.

4.5.3 Enabling SMS Alerts

The LAN Access event adapter can track SMS events and pass them to the Tivoli Enterprise Console. SMS does not receive dynamic alerts from the clients. It checks the SMS database and compares the client status with the conditions defined to trigger the alert. The client status is located in the information received from an inventory scan that was performed on the client and is written to the SMS database. That means if the inventory scan was performed seven days ago, the

client status is seven days old. In reality, a typical inventory frequency is seven days for software inventory and 14 days for hardware inventory (since you do not install new hardware very often).

To create an alert you will have to define two things. The query that triggers the alert, and the action to be performed as a result. So, the first thing to do is to define a query. To open the query dialog, select **Queries** from Open SMS Window.

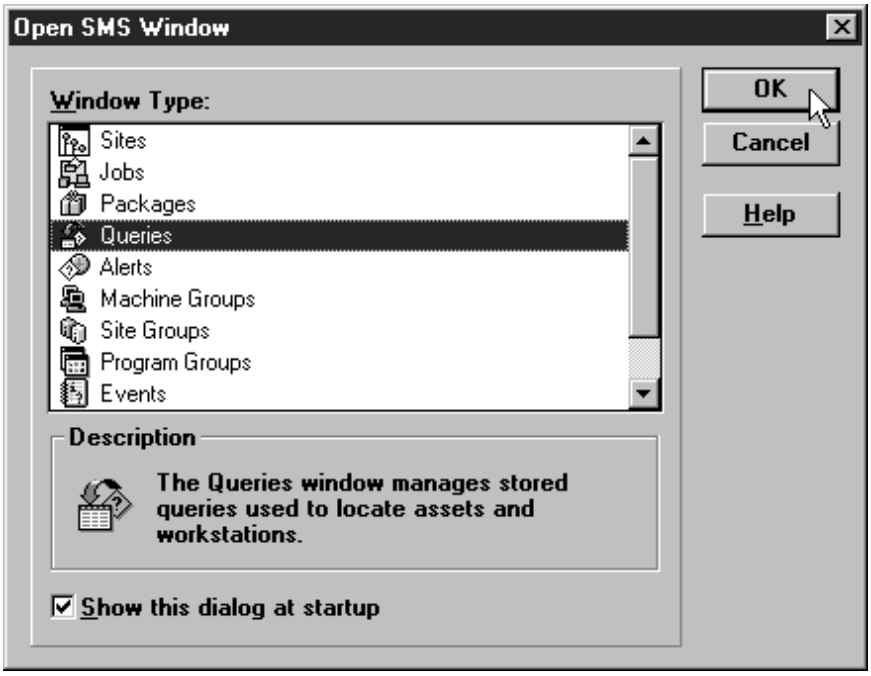


Figure 201. Open SMS Window

A typical example that people use to get familiar with the process is to query the disk space that is in use. This query is already defined in SMS and we used it without making any changes to it, but you can modify this query or create new ones from the query dialog. The query's name is Computers with Nearly Full Disks....

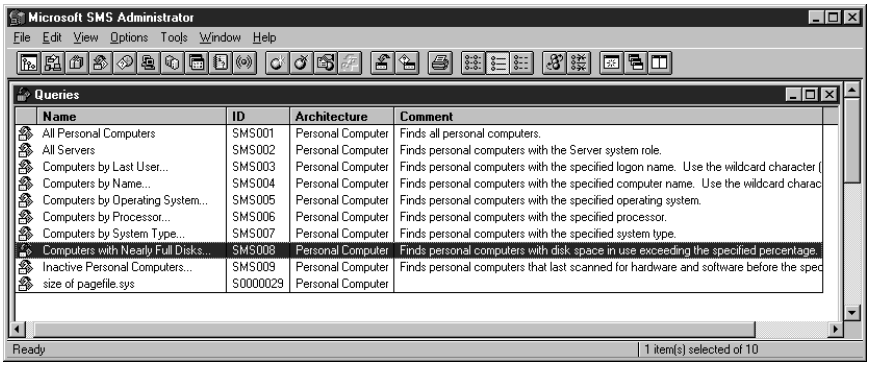


Figure 202. Queries

To display the Query Properties dialog for any query, double-click on the query. To create a new query, select **File->New...** from the menu bar.

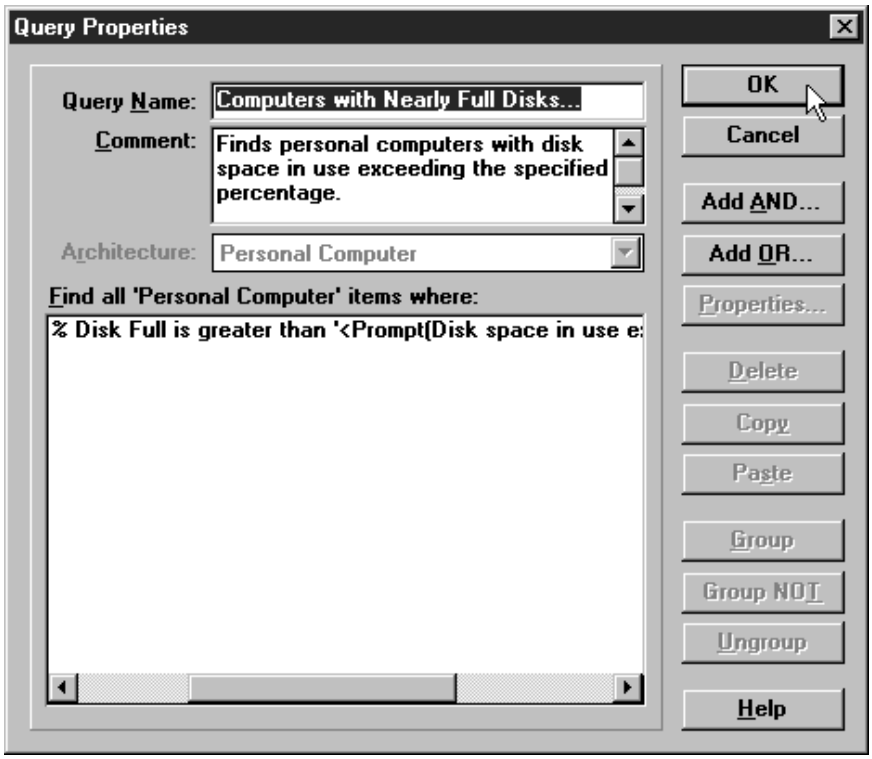


Figure 203. Query Properties

The query Computers with Nearly Full Disks... looks for computers that are using more disk space than a threshold amount that we specify when creating the alert.

To create an alert from the SMS Administrator click on **File** and **Open** and select **Alerts** to display the alert's dialog. Then click on **File->New**. In the Alert Properties window that appears enter the name you wish it to be known by.

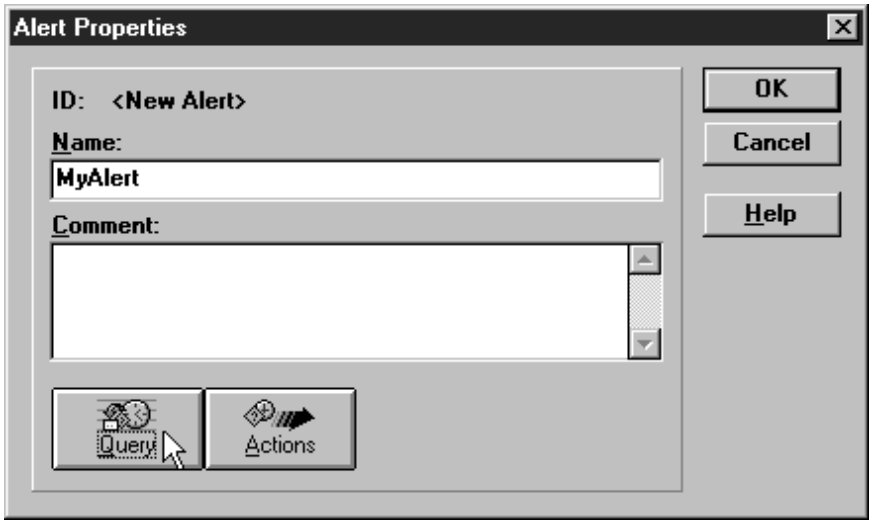


Figure 204. Alert's Properties

Then click on the **Query** button to bring you to the Alert Query window:

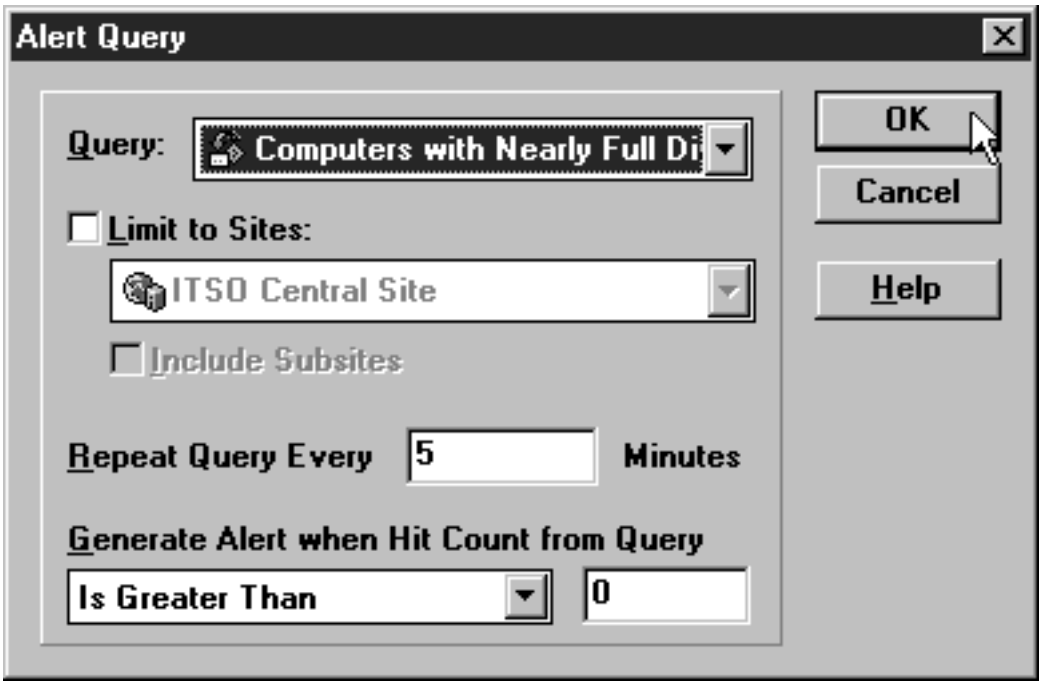


Figure 205. Queries

Click on the Query list and choose the query **Computers with Nearly Full Disks**. We also changed the default value in the Repeat Query field to 5. In a production environment there is no point in performing an alert query every 5 minutes against old data. We did it here for test purposes. The field, Generate Alert when Hit Count from Query, determines how many computers (objects) have to satisfy the query condition to trigger an alert. Click on **OK**.

Since the query we used included a value for us to input, SMS will prompt you for a value as follows:

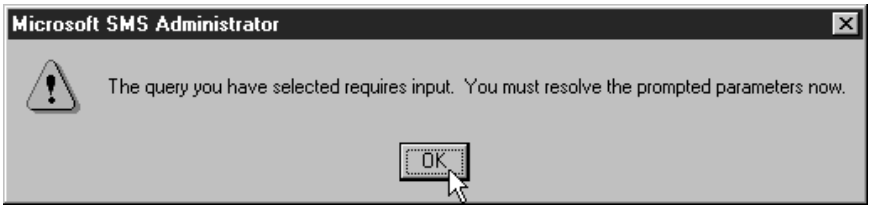


Figure 206. Value Required

The SMS alerter service will compare this value with the information for the drives in the SMS database.

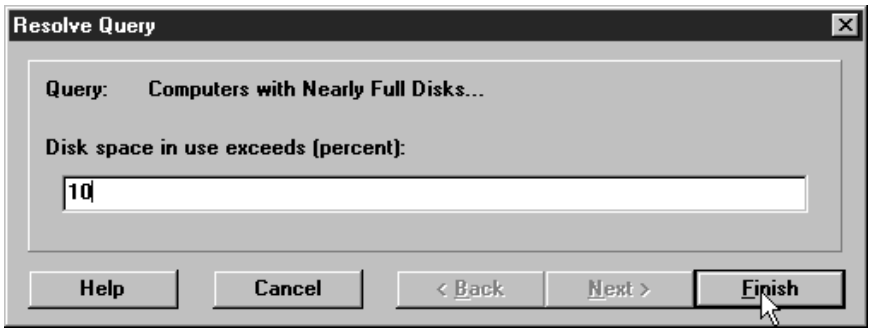


Figure 207. Value to Enter

Click on **Finish** to return to the Alert Properties.

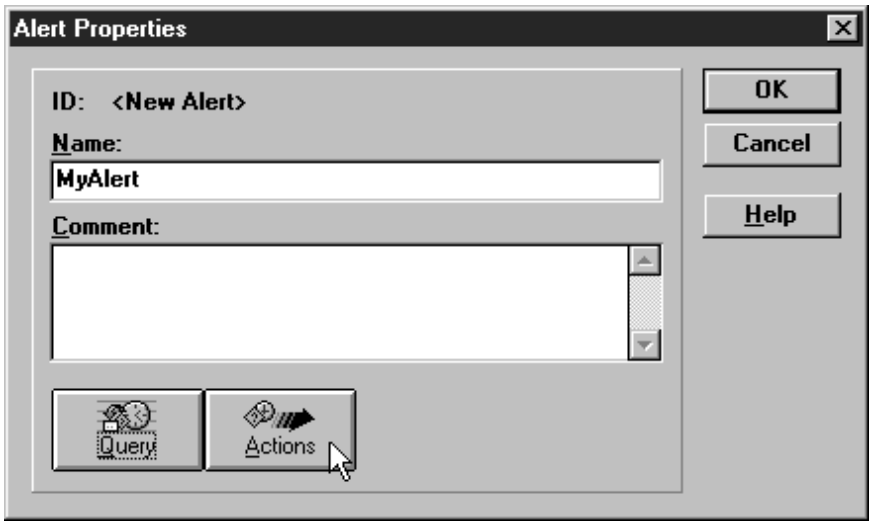


Figure 208. Defining the Actions

We then need to define the actions that will be triggered as a result of the alert conditions being met. Click on the **Action** button. Set the **Log an Event** check box. This option creates an event in the SMS event database if the condition specified in the alert's query is satisfied. The event will then be processed and forwarded to the LAN Access event adapter, which in turn, will forward it to TEC.

You can also execute any command or notify an administrator, but those choices are not helpful in showing the integration that can occur between LAN Access and SMS.

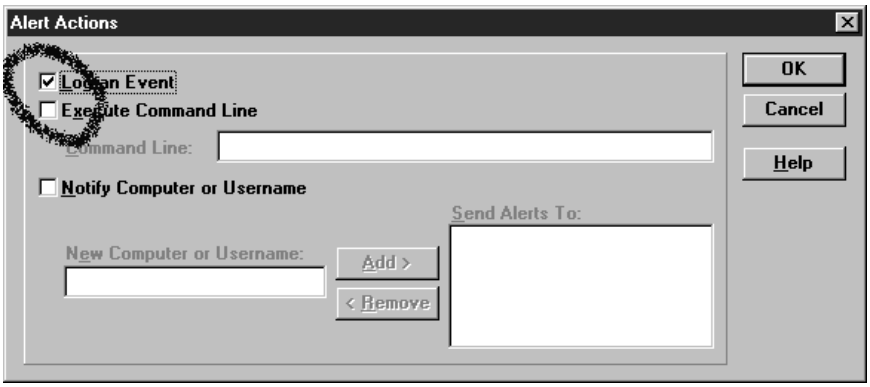


Figure 209. Alert Action

Click **OK** to go back to the Alert Properties window and click on **OK** again to activate the alerts query. The alert is now created and placed in the SMS database. In the next 5 minutes, the Scheduler should pick it up.

4.6 Software Distribution

Basically software distribution is just:

- The distribution of code
- Executing a setup program

Tivoli does a very good job with code distribution, but you still need to prepare the setup program to execute without user intervention. In the Windows environment there are three traditional ways of doing that:

1. Creating a script with Microsoft Test or Microsoft Visual Test
2. Performing an unattended install with a response file
3. Using a scanner program that scans changes made by the setup program (Tivoli AutoPack or SMS Installer)

Microsoft Visual Test is an application that can translate mouse clicks to scripts. You then run the script on the client. This method is slow and not reliable. If the menus on the client are not exactly the same as they were on the original system, the method will fail. Microsoft recommends using SMS Installer.

The SMS Installer scans files that are copied and registry changes made on the initial system. If the target computer requires different device drivers, this process will fail. Tivoli AutoPack is a similar program that is used in the Tivoli Management Environment. You can't distribute AutoPack file packages through LAN Access to SMS clients.

The best option is to use the unattended feature of the setup program. Most Windows applications use either InstallShield or the ACME setup program. InstallShield is a company that sells a setup program. ACME is a Microsoft proprietary setup program used for Microsoft programs such as Office or Internet Explorer.

In our example we distributed Microsoft Internet Explorer 4.0. Internet Explorer used ACME. If you enter `Ie4setup.exe /Q`, it will perform an unattended (sometimes called silent) installation.

InstallShield supports a response file. For example, we may start the setup program with the parameters:

```
SETUP.EXE -SMS -s -f1 response.iss -f2 logfile.txt
```

-SMS has nothing to do with Systems Management Server. It tells InstallShield to perform a *synchronous* installation. By doing that we are sure that when the setup program finishes the file copies will be finished as well. - switch means do a silent installation. -f1 response.iss means that the setup program will use a response file named response.iss. You can prepare that yourself. A lot of software that is distributed by vendors already has a response file prepared for you.

Not all versions of InstallShield support -SMS and -s switches, but you can download patches from the InstallShield Web site www.installshield.com.

The file extension for software packages in Systems Management Server is PDF. You will often find files with the PDF extension on software media. You can look at them using the Windows Notepad utility or any other text editor. You will find a complete setup command with a response file and all setup options. It is always better to use prepared response files then generating a new one. The prepared one includes all options. On the other hand you can miss a dialog box and the installation on the target system might fail.

A sample PDF for DOS V6.2 follows:

```
[PDF]
Version=1.0

[FULL Setup]
CommandLine=setup.exe /H /G
CommandName=Stand alone setup
UserInputRequired=TRUE
SupportedPlatforms=MS-DOS 5.0, MS-DOS 6.0

[Manual Setup]
CommandLine=setup.exe
CommandName=Manual Setup
UserInputRequired=TRUE
SupportedPlatforms=MS-DOS 5.0, MS-DOS 6.0

[Package Definition]
Product=Microsoft DOS
Version=6.2
Comment=Microsoft DOS 6.2
SetupVariations=FULL, Manual
```

4.7 Installation of LAN Access Components on the SMS Site

To install the components needed on the SMS site, you have to run setup.exe found under \us\w32\ on the CD. You run this on an SMS machine, which can be an SMS central server or an SMS primary server, and not from the Tivoli desktop. In our case we installed the provider on system ntsrv48, which is a central server. Tivoli LAN Access automatically detects what components are needed and selects and installs them for you. Therefore, it is important that you have all your other products installed before you perform this step. For example, you should already have SMS installed. If the node was going to have Netfinity or Intel LANDesk on it, you should install them before you run setup to install the MPM-API. The windows that follow show the steps for the installation.

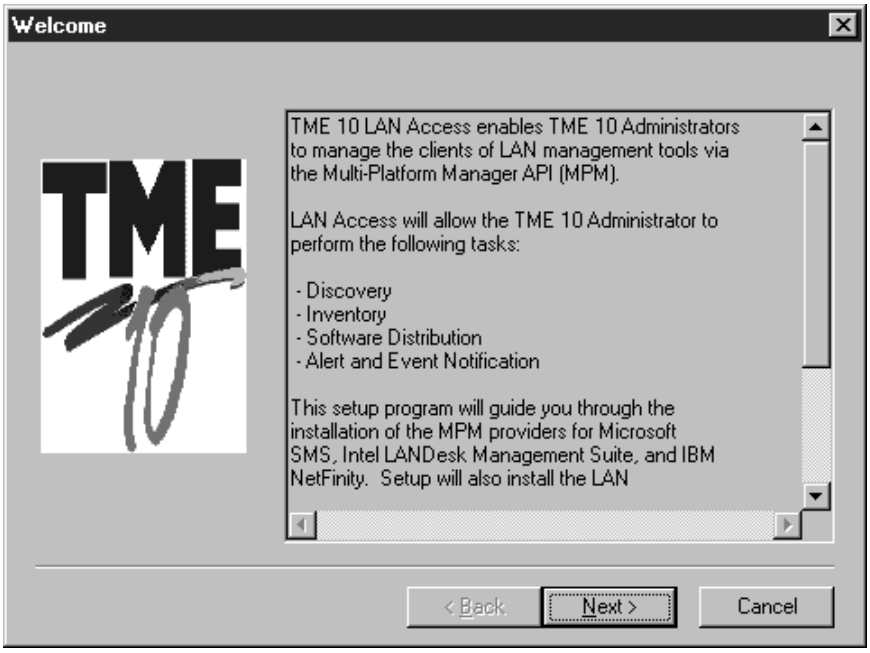


Figure 210. Welcome Window

Installing the MPM-API will permit the integration of LAN Access and the systems management application to occur. The key functions that will be able to be performed are: discovery, inventory, software distribution and event notification.

Click on **Next**.

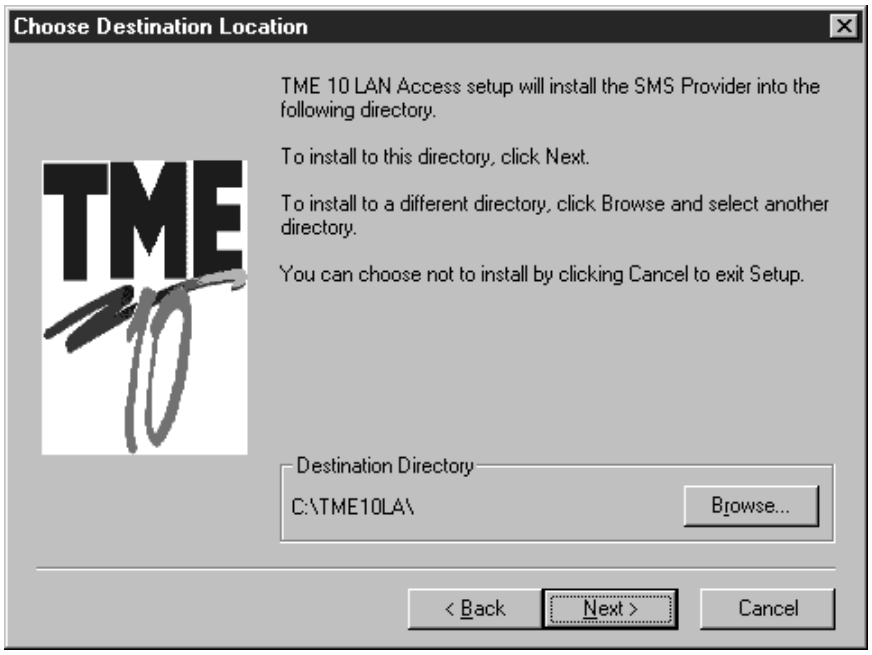


Figure 211. Destination Location Window for SMS Provider

After specifying the directory that you are going to store the code in, you should click on **Next**.

In Figure 212 the fields for the SQL user ID and password were determined when configuring the SMS connection to the SQL database, which was done in 4.4, “Installation of Microsoft Systems Manager Server V1.2” on page 150.

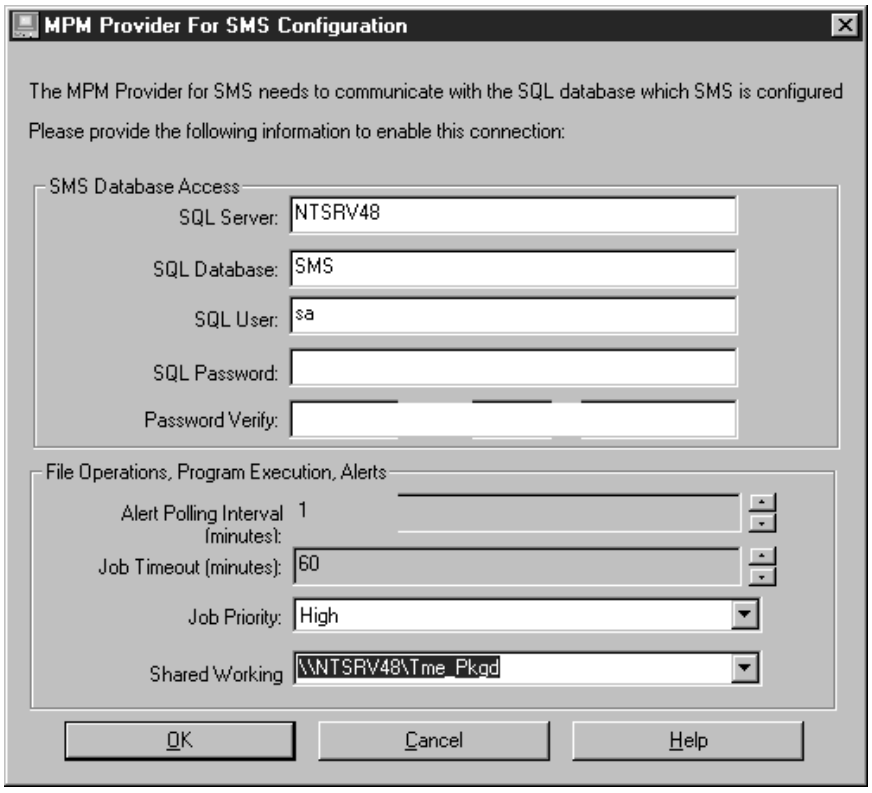


Figure 212. SMS Provider Configuration

In the field Shared Working you should specify a directory in the SMS distribution server and ensure that all SMS clients have at least read access to it. This directory should exist on the SMS server prior to the configuration of the SMS provider and must not be the same one that SMS uses for distribution (\\<server name>\SMS_PKGD). You can create this directory using Windows NT Explorer and edit its properties window to enable sharing to all SMS clients. This was done in 4.5, “Configuring SMS for LAN Access Integration” on page 152.

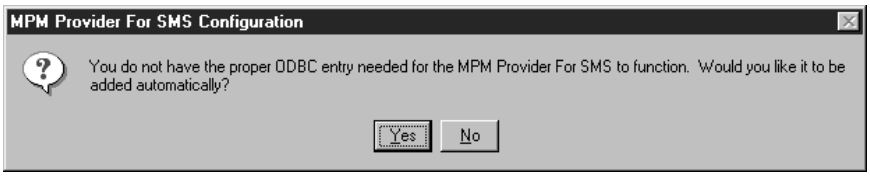


Figure 213. SMS Provider Configuration

We used Version 3.0.28.22 for all ODBC core components.

If you click on **No** in this window, you will have to create the ODBC entry manually later, as the SMS provider uses the ODBC entry to retrieve network information from the SQL database.

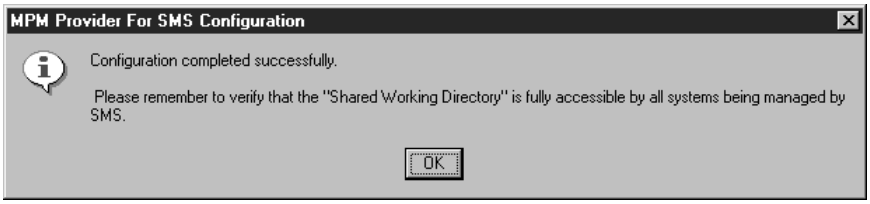


Figure 214. SMS Provider Configuration

Click on **OK** to continue with the installation.

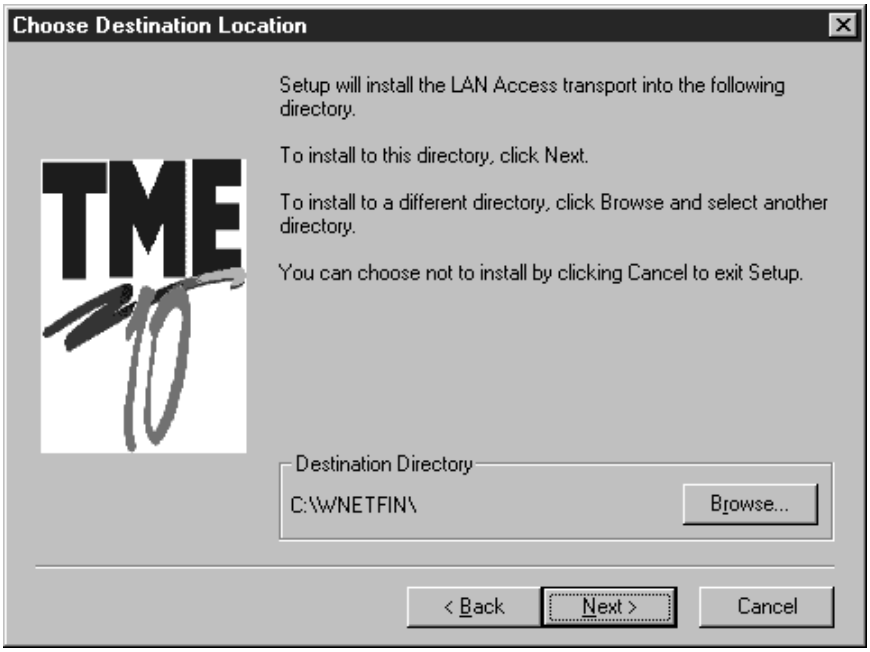


Figure 215. Destination Location Window for LAN Access Transport Component

In Figure 216 on page 174 the fields for the UserName and Password were determined in 4.4, “Installation of Microsoft Systems Manager Server V1.2” on page 150. It refers to the account created for all SMS services during the installation of SMS.

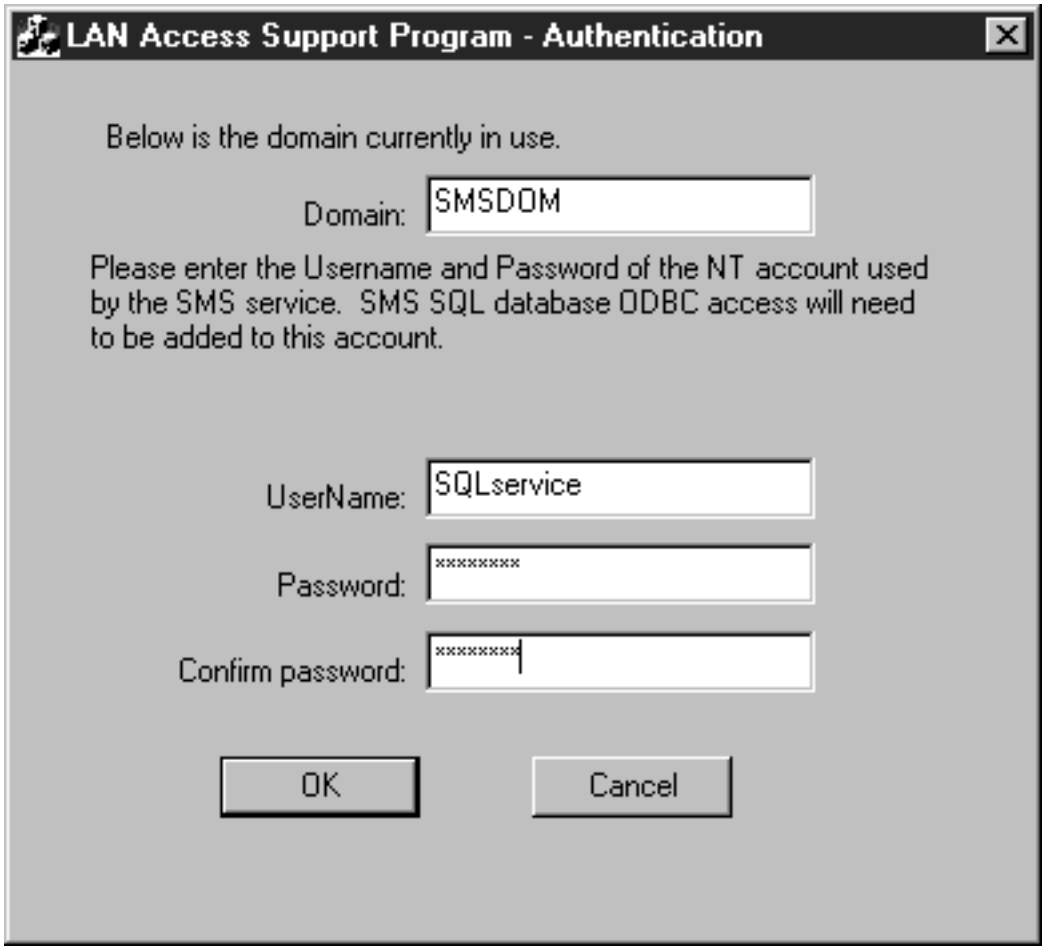


Figure 216. Authentication Window

LAN Access automatically detects the network drivers installed in the system. You should enable the driver that the SMS site is going to use to communicate with the NT managed node. In this example we have NetBIOS, IEEE 802.2(SNA/APPC) and TCP/IP. We will be using TCP/IP and NetBIOS.

Note: Notice that the System Name that appears in Figure 217 on page 175, refers to the SMS central site.

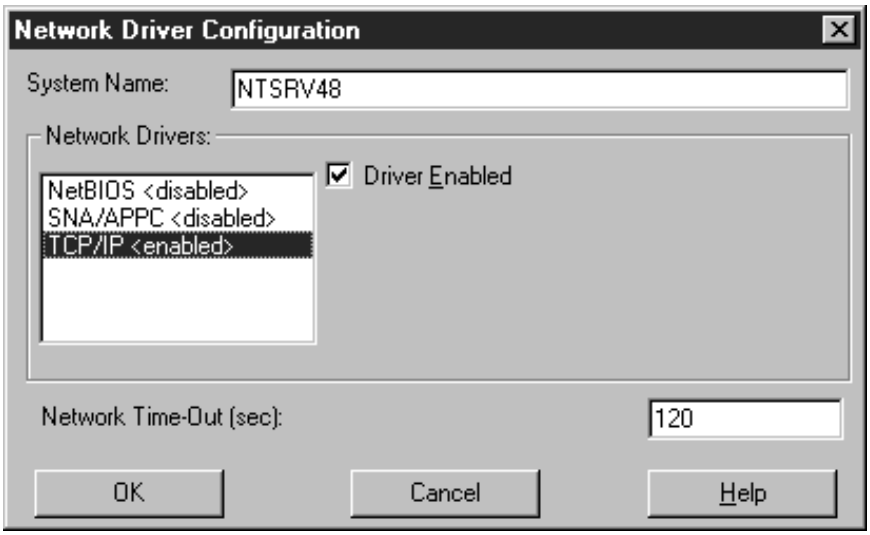


Figure 217. Network Driver Configuration Window

The default network timeout is 15 seconds. You should modify this value taking into consideration the load and speed of your systems and network.

4.8 Working with SMS Clients from Tivoli's Desktop

In Chapter 1, “Installation and Configuration” on page 1 we showed how LAN Access node objects are created on Tivoli's desktop to represent LAN clients and enable TME 10 operations over systems that do not belong to the native Tivoli environment. In the following section we show how Tivoli applications can be used with Tivoli LAN Access.

4.8.1 Distributing Software

Following the normal procedure of Tivoli distribution, a software profile must be created inside a profile manager. As an example we created a profile called Text_File inside a FilePackage profile manager called Software_Distribution, as shown in the following window:

Figure 218. Creating Profile

That will result in the following profile being created:

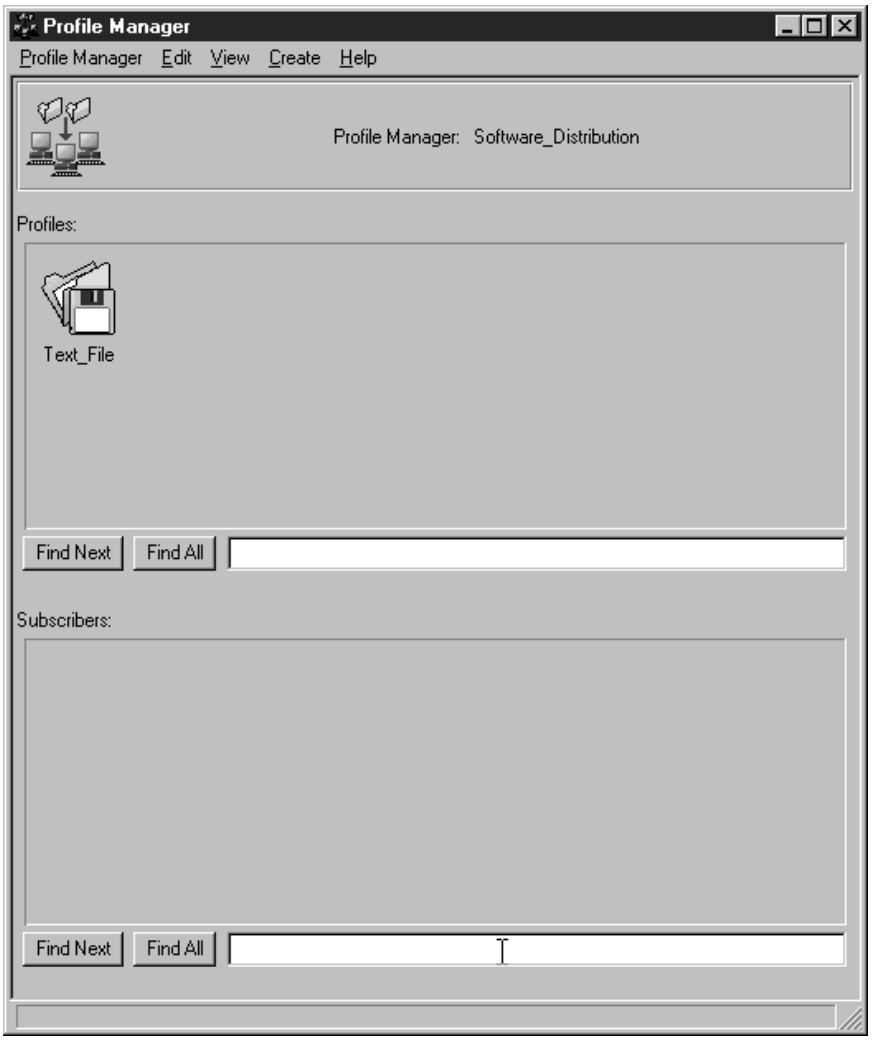


Figure 219. Profile Manager Window

Edit the file package properties to define the distribution options. The fields required in this window are:

- File Package Name
- Source Host
- Source Directories and Files

The other options that we have selected are not necessary but we recommend, for example, to always specify a file where information about the distribution is logged. It can be useful to debug problems. For additional option details see 5.2.1, “Configuring Software Distribution” on page 209.

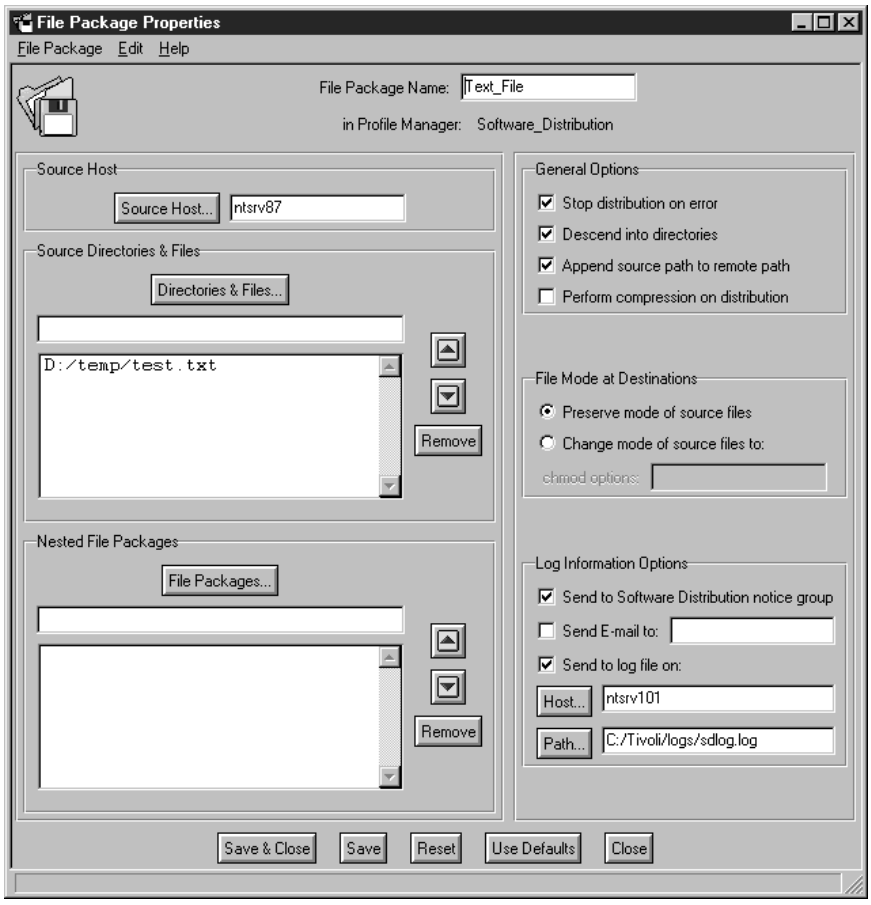


Figure 220. File Package Properties

Note: Always remember to select the **Platform Specific Options** for distribution before closing the profile's properties window. See 5.3.1, “Restrictions on Using Tivoli Software Distribution” on page 233 for more information on Software Distribution.

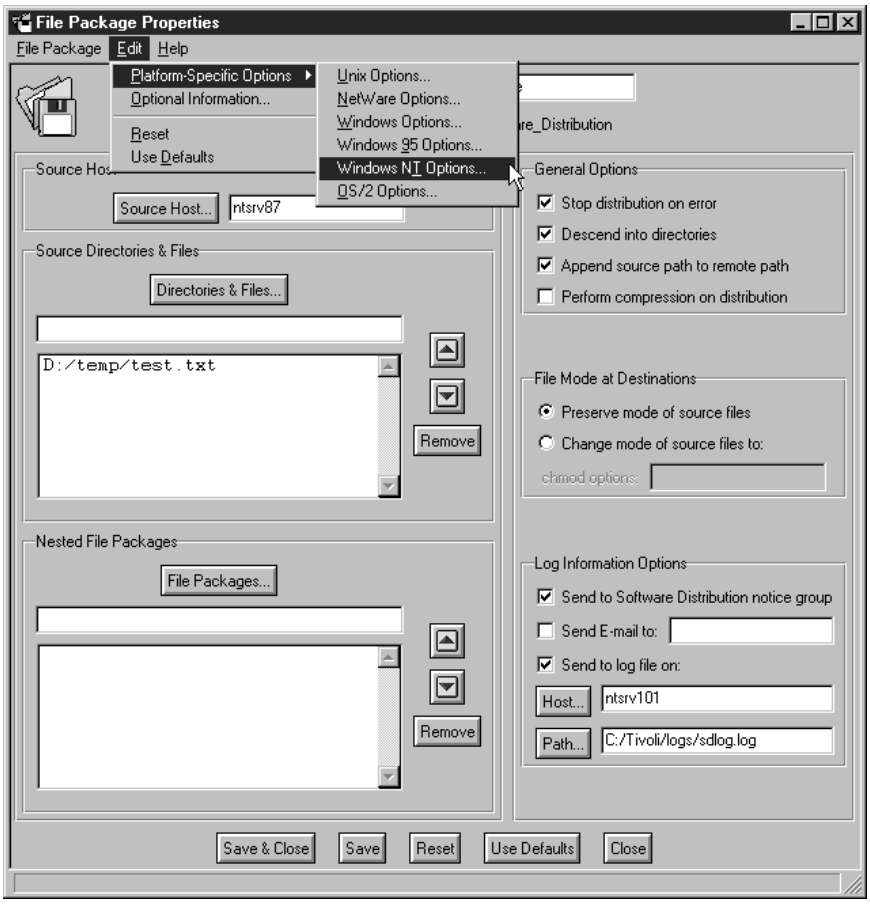


Figure 221. Selecting Platform Specific Options

We set the file package options for a Windows NT system. In this window, the only required field is the Destination Directory Path.

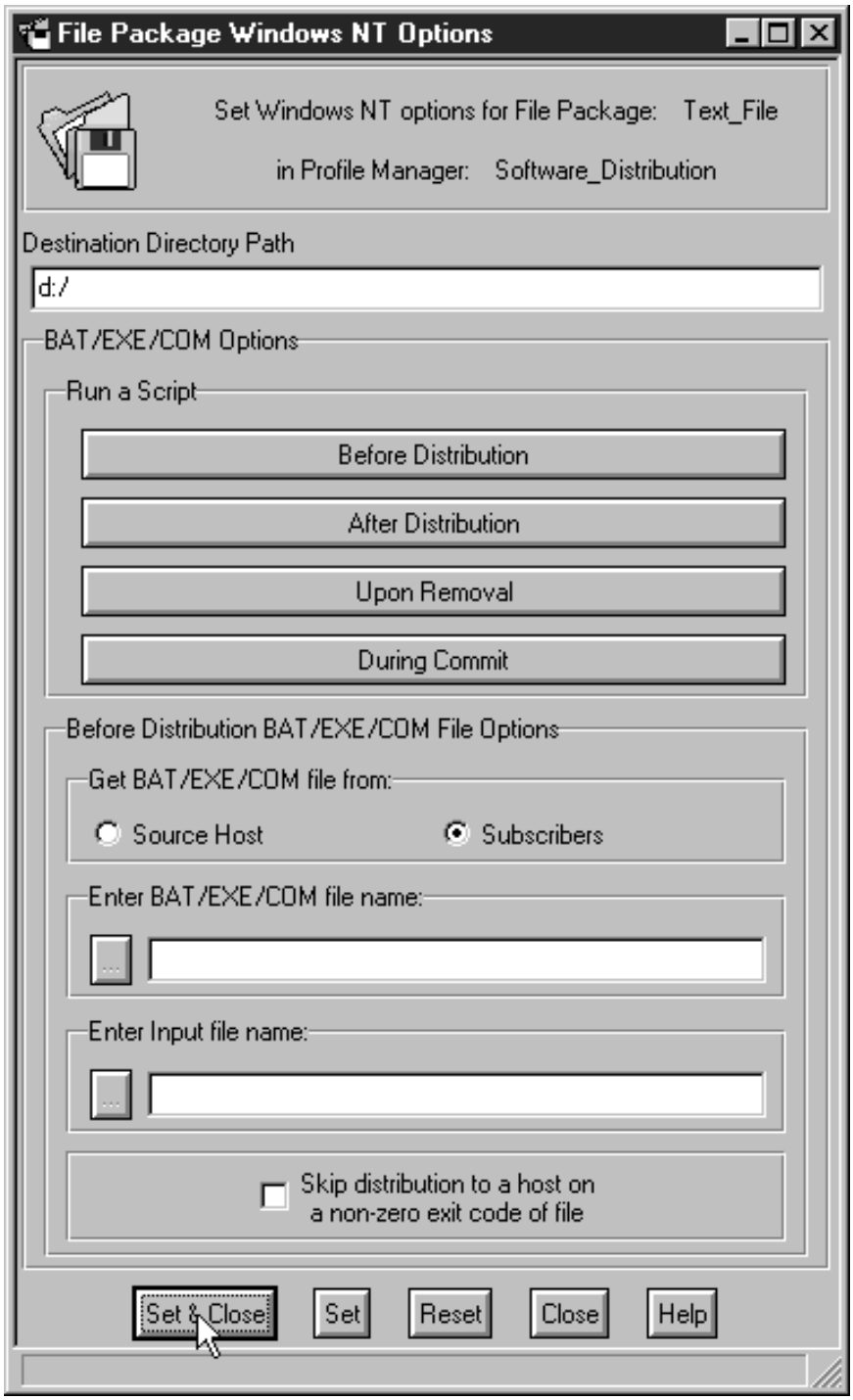


Figure 222. Windows NT Options Window

Select **Set & Close** to go back to the File Package Properties window and on that window select **Save & Close** to return to the profile manager.

Next, we select **Profile Manager**->**Subscribers...** to set the subscribers for this profile manager.

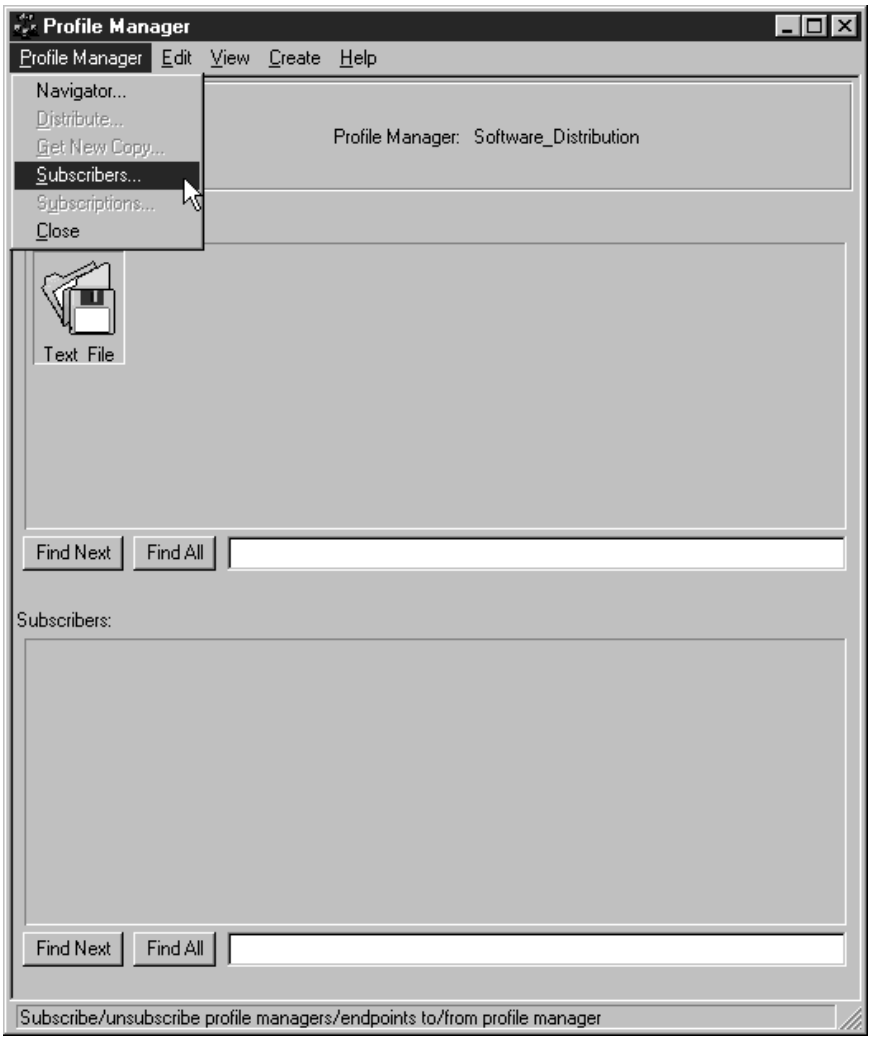


Figure 223. Selecting Subscribers for the Profile

We put in the Current Subscribers list the object that represents our SMS client, which we can recognize because its name includes LANAccessNode in brackets.

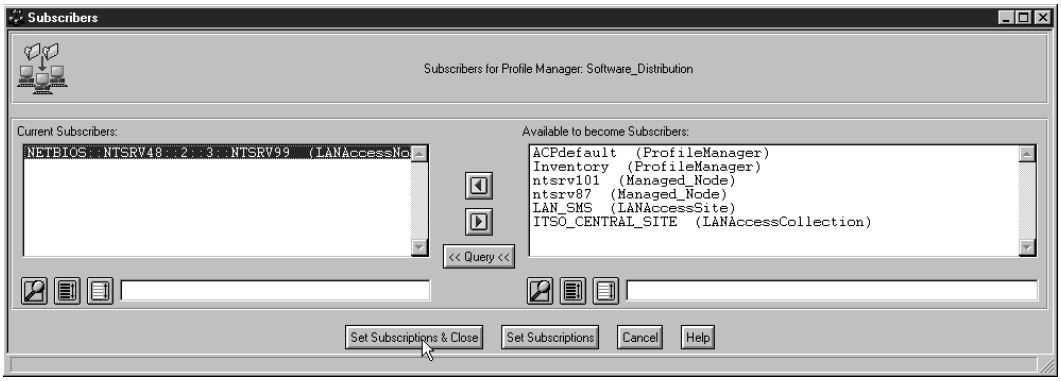


Figure 224. Setting Subscriptions

To distribute the profile, you can either do it from the profile's context menu, or from the window's menu bar by selecting **Profile Manager**->**Distribute...**. Distribution using drag and drop is not supported for Windows NT clients.

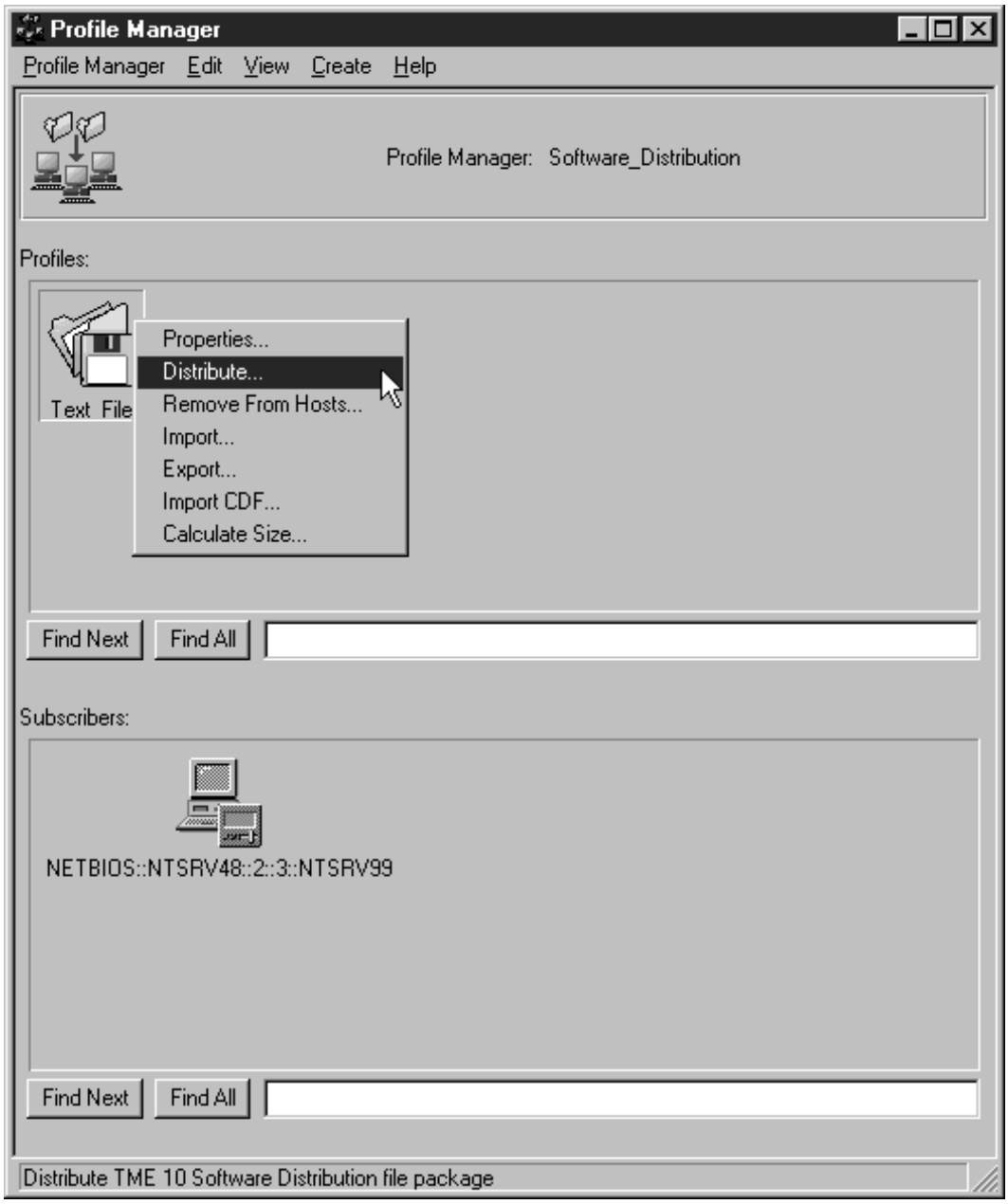


Figure 225. Distributing Profile

Put the subscriber of the profile into the Distribute File Package To box and select **Distribute & Close** to start the distribution.

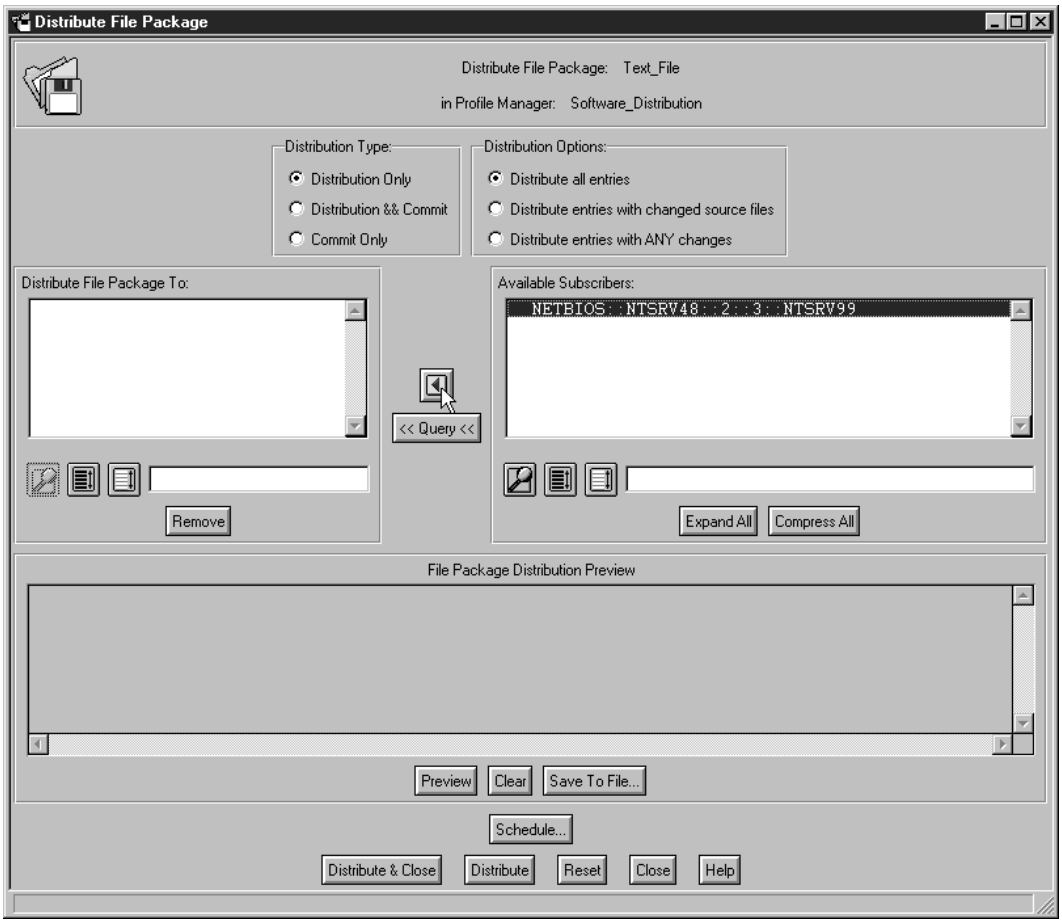


Figure 226. File Package Distribution Window

Next we show the process that goes on during distribution at the SMS site when no more intervention is required from an administrator.

LAN Access generates on the SMS site two packages, two jobs and a query. These two packages contain the LAN Access agent code and the execution instructions to install this agent on the SMS client. One package is for Windows 95/NT clients and the other package is for DOS/Windows 3.1 clients. LAN Access uses SMS to distribute its agent code in order to enable a TME 10 file package installation or a remote execution on an SMS client. That is, once the agent is installed, Tivoli will not use SMS for software distribution.

LAN Access depends on the TME database for information that will be used to create the SMS package and the execution instructions.

You can see the MPM packages, jobs and the query in the SMS Administrator console at the SMS site.

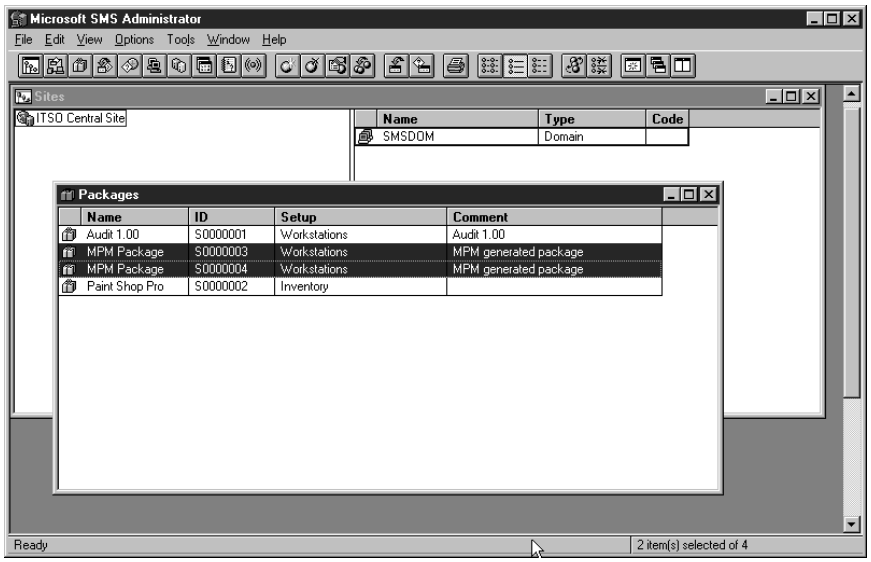


Figure 227. Packages

To display the Packages dialog select **Packages** in the Open SMS Window. The packages that LAN Access generates are the MPM packages.

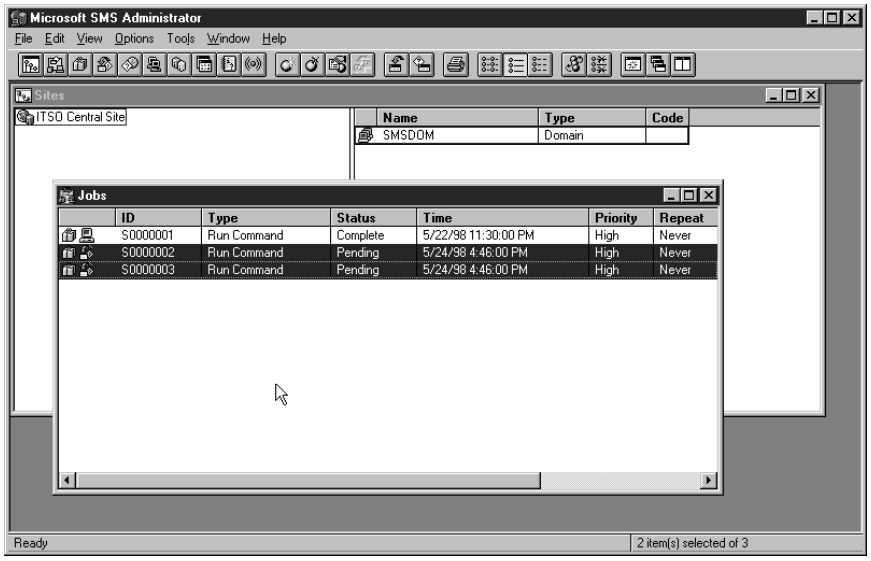


Figure 228. Jobs

To view the jobs, select **Jobs** in the Open SMS window.

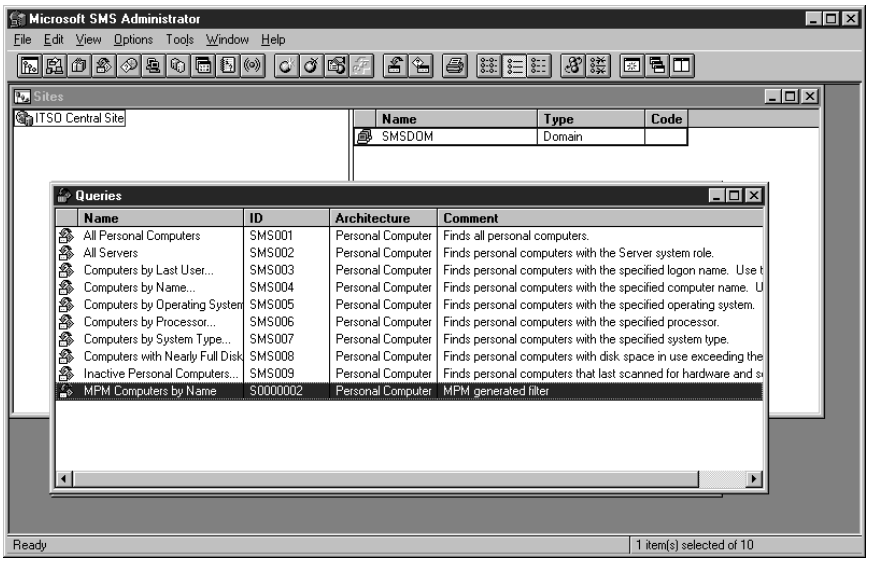


Figure 229. Queries

The queries are displayed selecting **Queries** in the Open SMS window. The query that LAN Access generates is called MPM Computers by Name.

Figure 230 through Figure 232 on page 186 show the details and the status of the job.

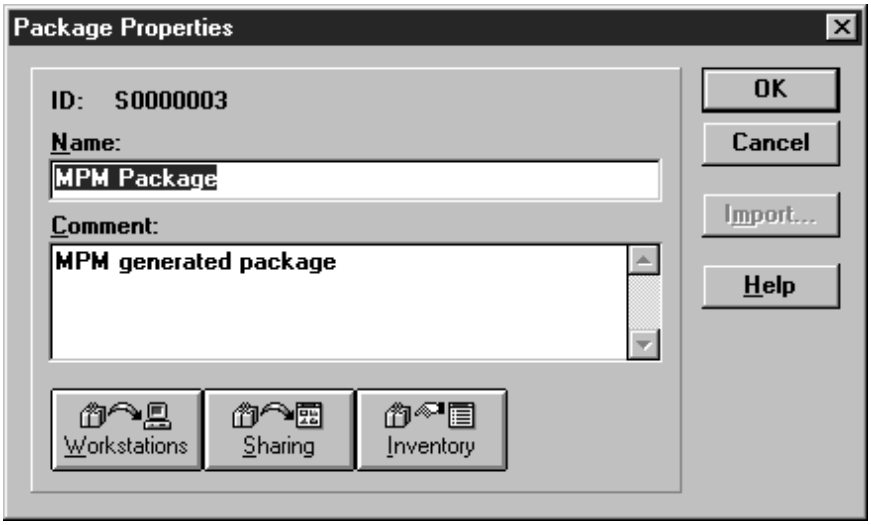


Figure 230. Package Properties

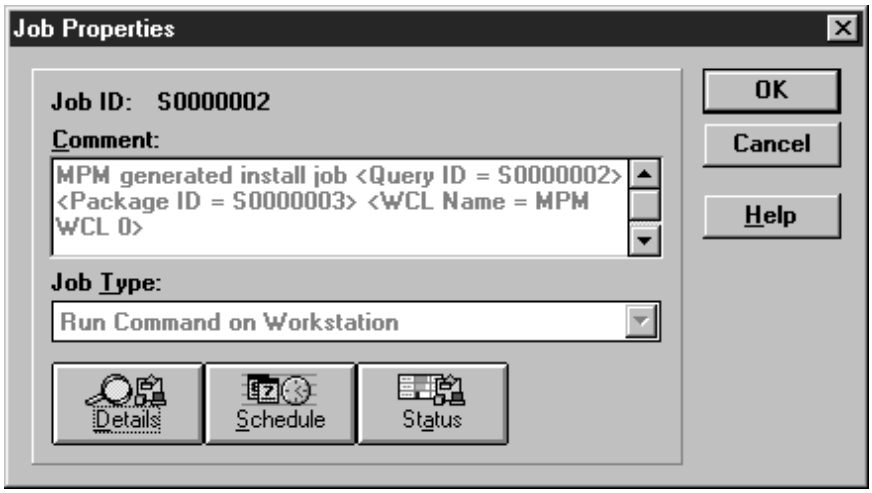


Figure 231. Job Properties

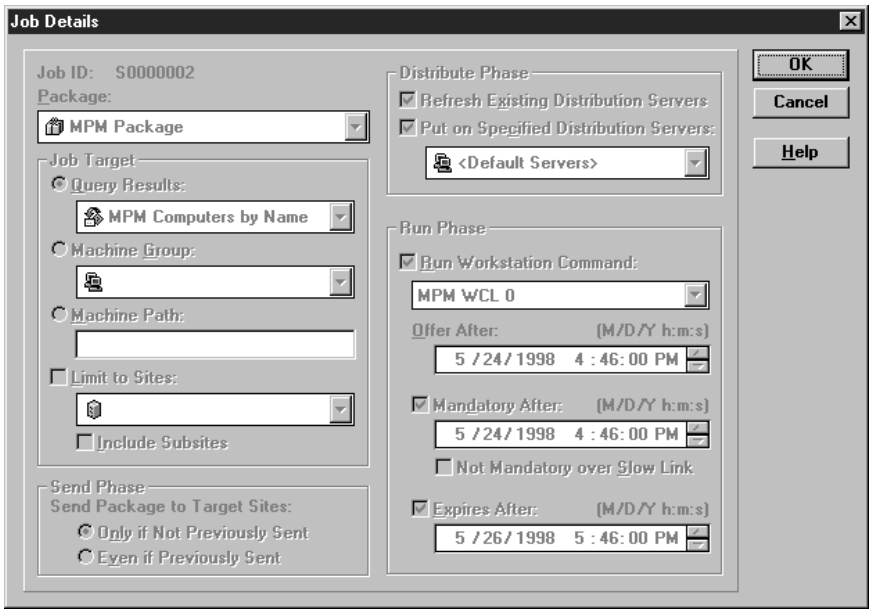


Figure 232. Job Details

The SMS server sends these MPM packages to its clients but only one of the two packages will be executed depending on the operating system at the target. The next time the SMS client logs on to see if there are new packages, it will pull the MPM package from the server and execute it. The Package Command Manager, as well as a pop-up warning that the package will be executed in five minutes, get displayed on the clients' screens. You can click on **Execute Now** if you want it executed immediately.

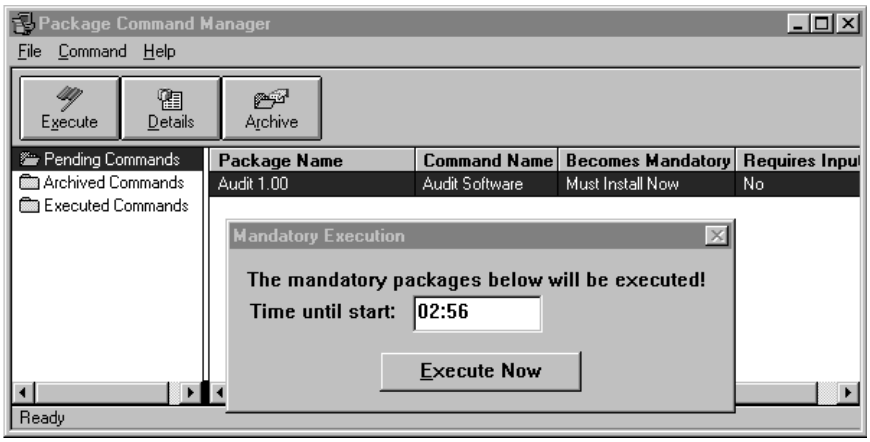


Figure 233. Package Command Manager at the SMS Client

When the MPM package is executed on the SMS client, the LAN Access agent, starts running on the client. As soon as this happens, SMS no longer takes part in the software distribution. The LAN Access managed node sends the file package directly to the SMS client.

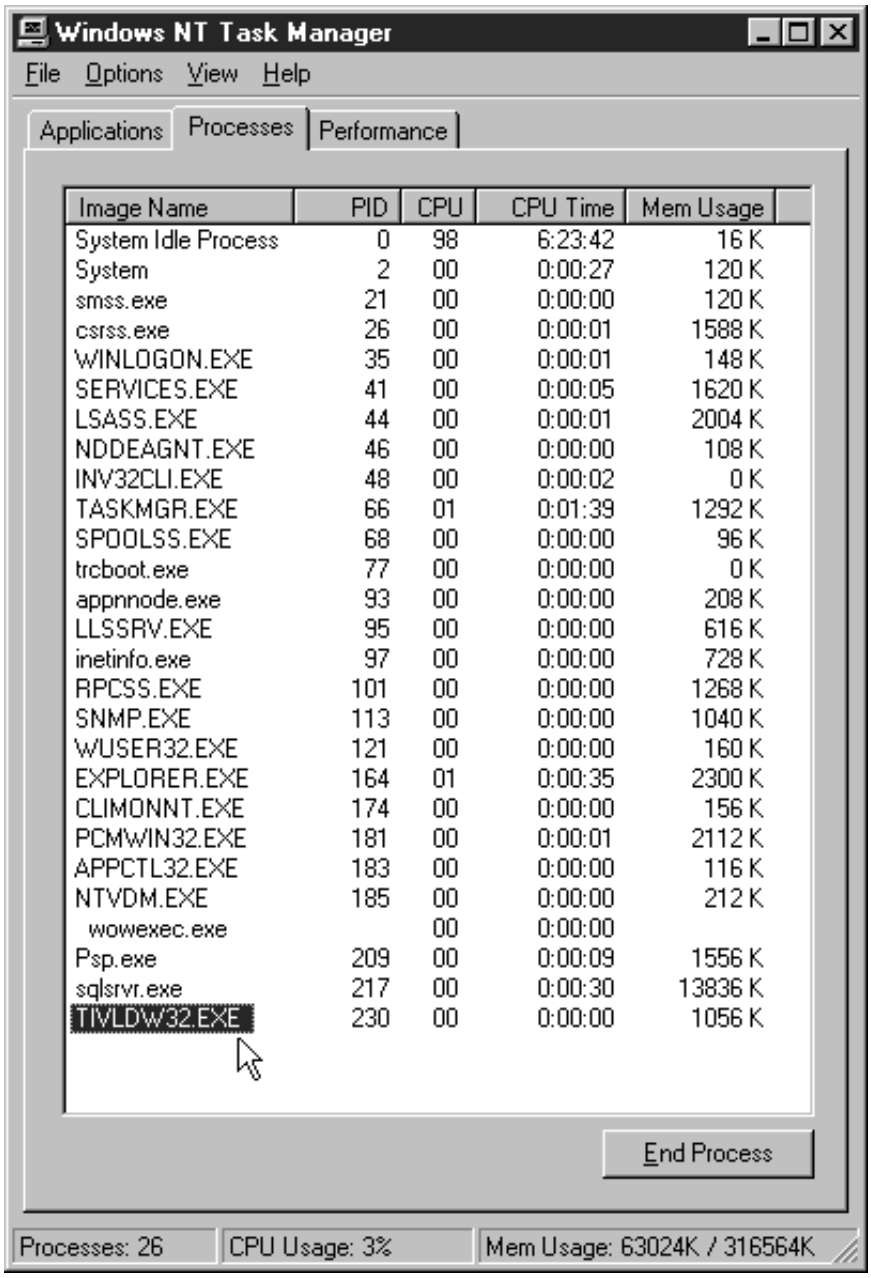


Figure 234. Task Manager Window of the SMS Client

You can see the process running on the client in the task manager.

- TIVLDW32 is the agent for Windows 95/NT clients.
- TIVLDW16 is the agent for DOS/Windows 3.1 clients.

LAN Access relies on SMS to install its agent. Once the agent is installed the SMS Software Distribution process is bypassed. It works this way because Tivoli has a more robust software distribution process than SMS since SMS has no error recovery mechanism built into it.

We have observed that the LAN Access agent can stay active in the client for two hours. If you distribute more Tivoli file packages while the agent is still running, LAN Access detects the agent running, and sends the package directly to the SMS

client with no SMS intervention at all. When the agent times out, the next time you send a file package to a LAN client, SMS will reinstall it.

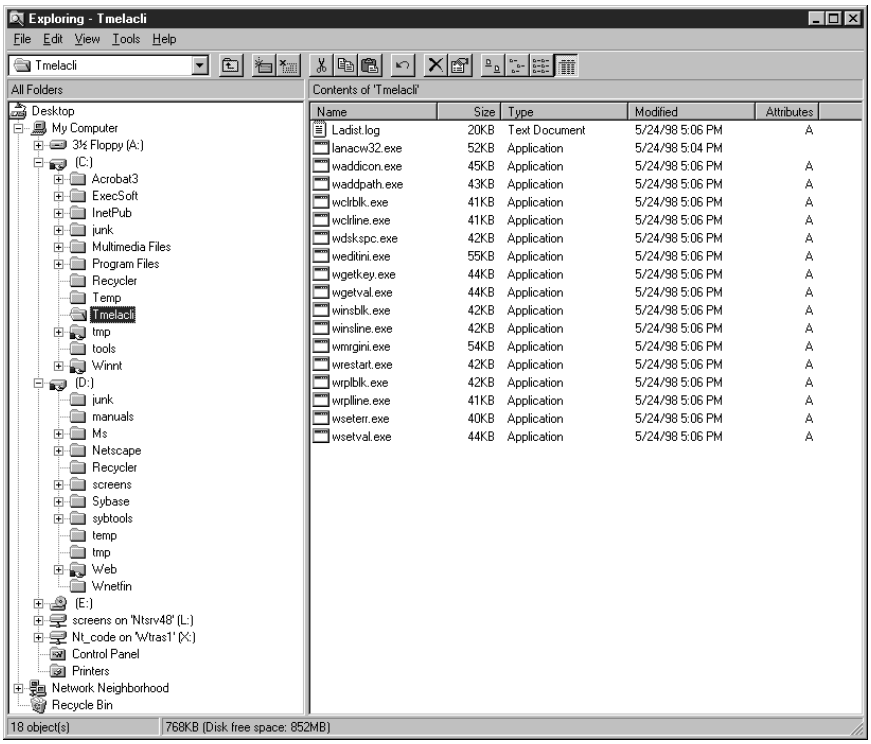


Figure 235. Windows NT Explorer

The first time that LAN Access distributes a file package to an SMS client, a directory called Tmelacli is created on the client. This directory contains command-line utilities for the client as well as two log files. The first log file is called ladist.log and writes down information about the installation of the file package on the client. The other log file is called labarc.log and it is created only if you specify, when you create a file package profile, a BARC program to run on the target. BARC stands for:

- *Before* distrbution
- *After* distribution
- Upon *removal*
- During *commit*

These are platform-specific options that you can configure when you create a TME software distribution profile to run scripts on the client (see Figure 222 on page 180).

A subset of ladist.log follows:

```
Sun May 24 17:06:10 1998 -----------  processing the archive  ---------
Sun May 24 17:06:10 1998 Processing winntcli.bin...
Sun May 24 17:06:10 1998    Last Access   = Sun May 24 17:06:10 1998
Sun May 24 17:06:10 1998    Last modified = Sun May 24 17:06:10 1998
Sun May 24 17:06:10 1998    Time created  = Sun May 24 17:06:10 1998
Sun May 24 17:06:10 1998  Opening file: wsetval.exe
Sun May 24 17:06:10 1998   Writing 16384 bytes of wsetval.exe to file...
Sun May 24 17:06:10 1998   Writing 16384 bytes of wsetval.exe to file...
Sun May 24 17:06:11 1998 Success!
Sun May 24 17:06:55 1998 -----------  processing the archive  ---------
Sun May 24 17:06:55 1998 Processing archiv2...
Sun May 24 17:06:55 1998  Opening file: temp\test.txt
Sun May 24 17:06:55 1998   Writing 384 bytes of temp\test.txt to file...
Sun May 24 17:06:55 1998 Success!
```

A copy of labarc.log follows:

```
Mon May 25 10:20:17 1998 -----------  running the BARC program  ---------
Mon May 25 10:20:17 1998 Setting PATH to C:\TMELACLI;C:\WINNT\system32;
C:\WINNT;d:\sybase\dll;d:\sybase\bin;C:\Program Files\
\Personal Communications;d:\sybtools\WIN32;d:\sybtools\ASEP;
C:\WNETFIN;D:\WNETFIN;
Mon May 25 10:20:17 1998  PATH size = 165
Mon May 25 10:20:17 1998 Spawning clock.exe'
Mon May 25 10:20:17 1998 CreateProcess failed for clock.exe'! Error = 2
```

4.8.2 Viewing Inventory Data

To retrieve software inventory information from SMS clients, an SMS process called audit software must be run on the clients. This process is explained in 4.5.2, “Enabling Inventory” on page 153. You should also make sure you run the database script create_os_detail_view.sql, which comes with the Tivoli LAN Access 1.1.1 upgrade code. It is located in the directory $BINDIR/TME/LACCESS and it should be run against the Tivoli Inventory RDBMS database. In our setup we were using Sybase, so we had to modify the script on the CD, since it was written for Oracle. Where Oracle uses a semi-colon, sybase uses the keyword go.

create_os_detail_view.sql - Notepad

File Edit Search Help

```
drop view INSTALLED_OS_DETAILS_VIEW
go
create view INSTALLED_OS_DETAILS_VIEW
as
select
    INSTALLED_OS_DETAILS.HARDWARE_SYSTEM_ID,
    TME_OBJECT_ID,
    NAME,
    VERSION_LEVEL
from INSTALLED_OS_DETAILS, COMPUTER_SYSTEM
where INSTALLED_OS_DETAILS.HARDWARE_SYSTEM_ID =
      COMPUTER_SYSTEM.HARDWARE_SYSTEM_ID
      and (INSTALLED_OS_DETAILS.CONFIG_CHANGE_TYPE = 'INSERT'
      or INSTALLED_OS_DETAILS.CONFIG_CHANGE_TYPE = 'UPDATE')
go

commit
go
```

Figure 236. create_os_detail_view.sql for Sybase

This step is necessary since you will need this view to access the software inventory information for the SMS clients written in the Tivoli database. You can query this view from the Tivoli desktop.

4.8.3 Retrieving Inventory Data

Once you have ensured that you have done all the prerequisite steps, follow the normal procedures used with the Tivoli Inventory application.

First you create a Tivoli inventory profile. We created an inventory profile called HW-SW inside a profile manager called Inventory.

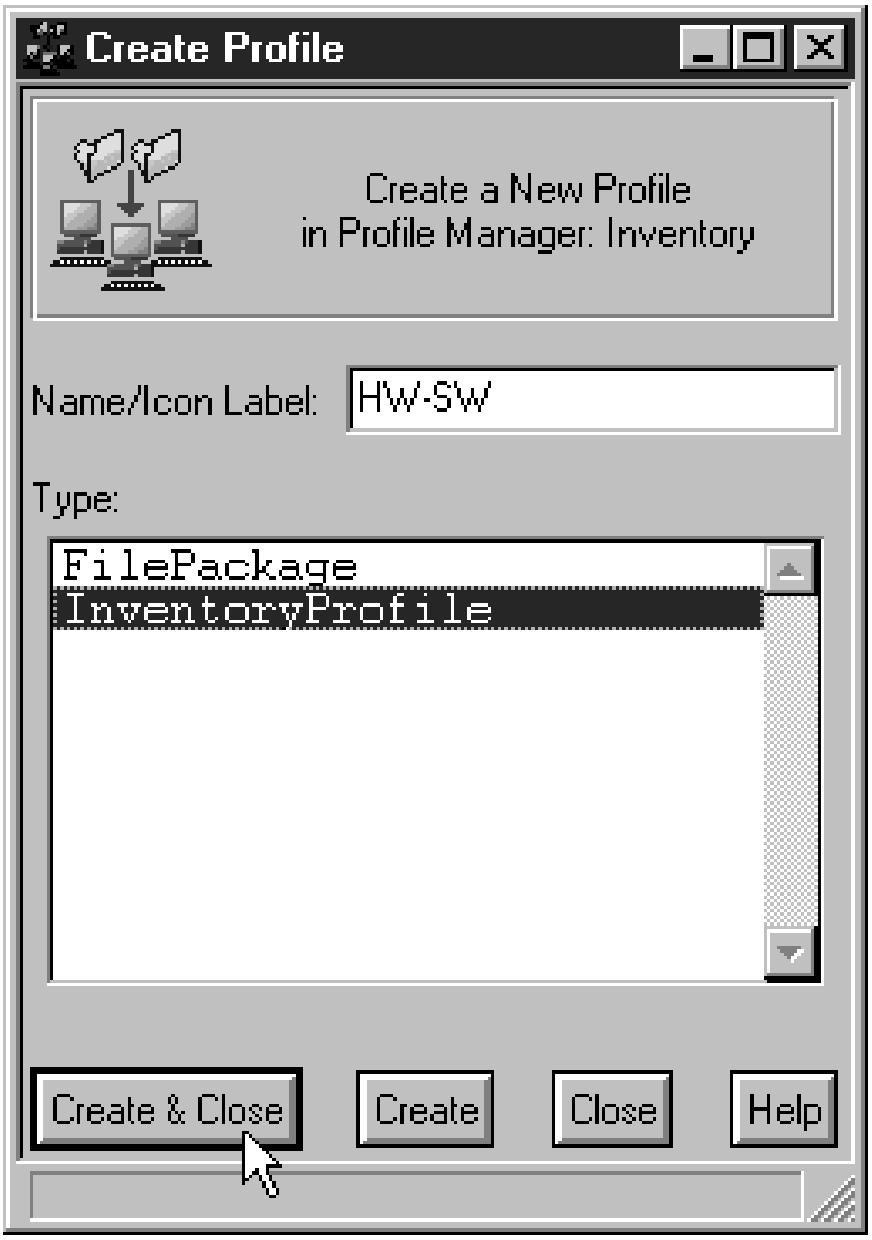


Figure 237. Create Profile Window

Select **Customize...** from the profiles context menu to configure the profile.

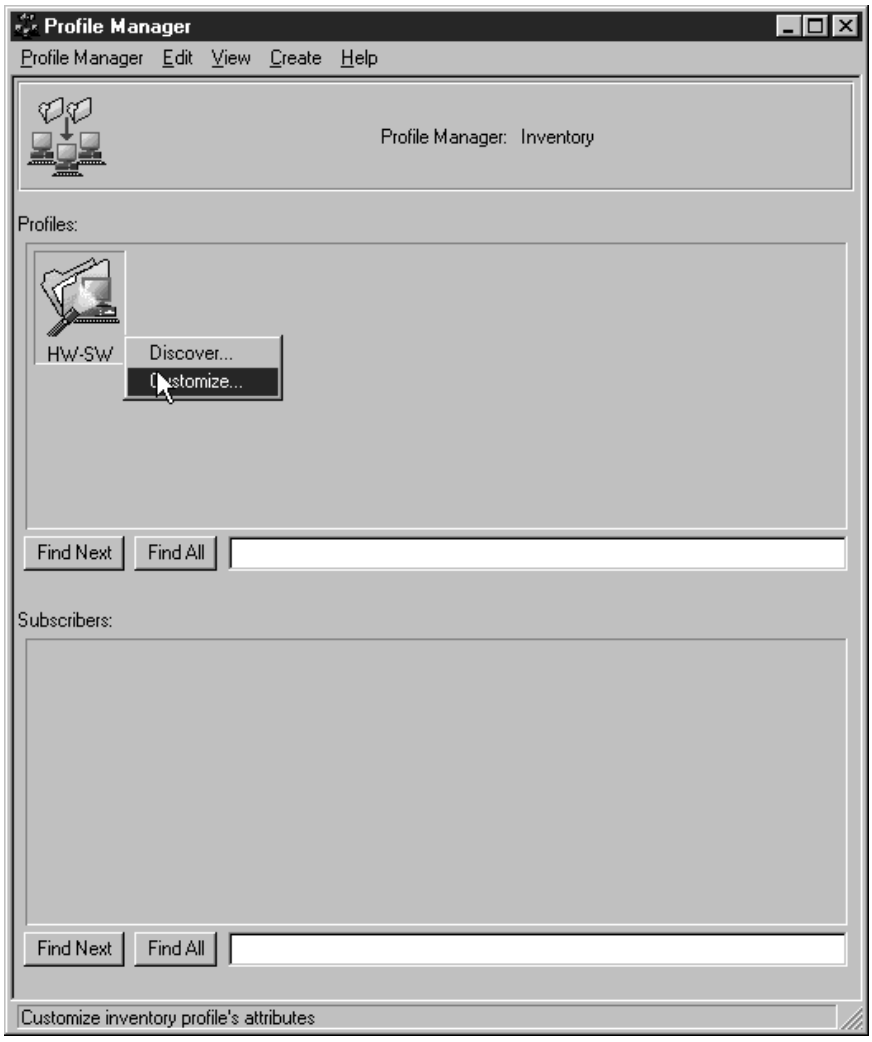


Figure 238. Customizing an Inventory Profile

This will bring you to the Customize Inventory Profile window where you will select the details for this profile:

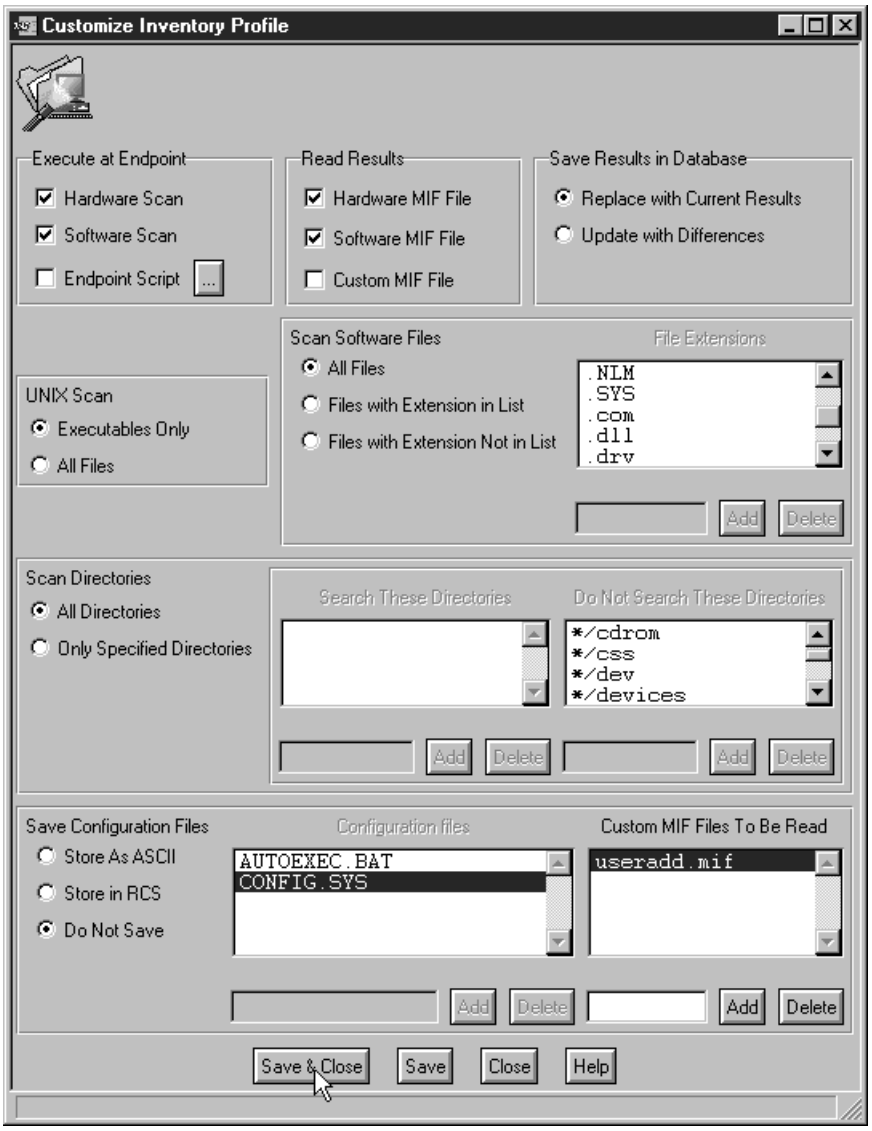


Figure 239. Customize Inventory Profile Window

LAN Access discovery profiles always query the SMS database for hardware and software inventory, so in this case there is no difference when choosing a hardware scan, a software scan, or both.

Note: For more details on Inventory see 5.4.3, “Restrictions on Using Tivoli Inventory” on page 248.

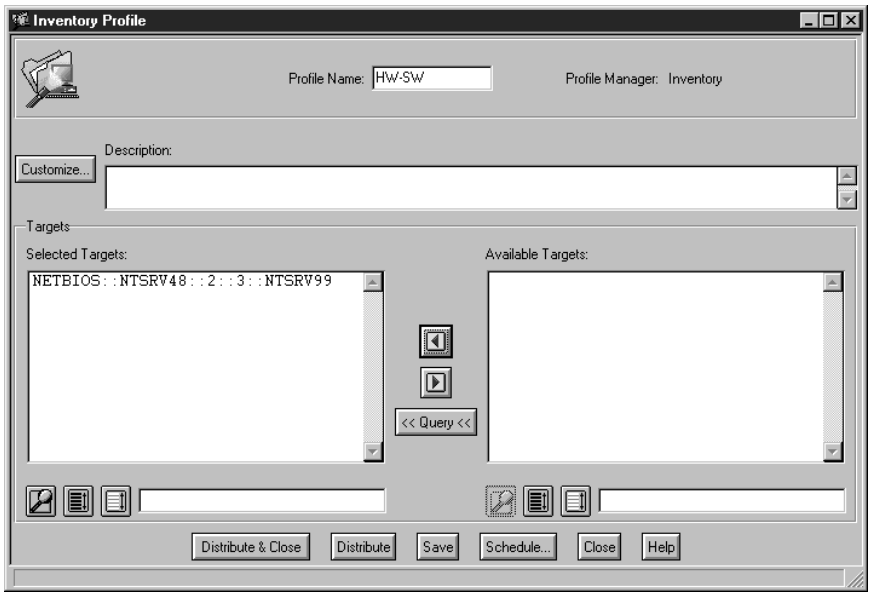


Figure 240. Selecting Targets for Discovery

Once the inventory discovery of SMS clients is completed you can see the hardware information by selecting the **Hardware Inventory..** option from the pop-up menu on the client's icon.

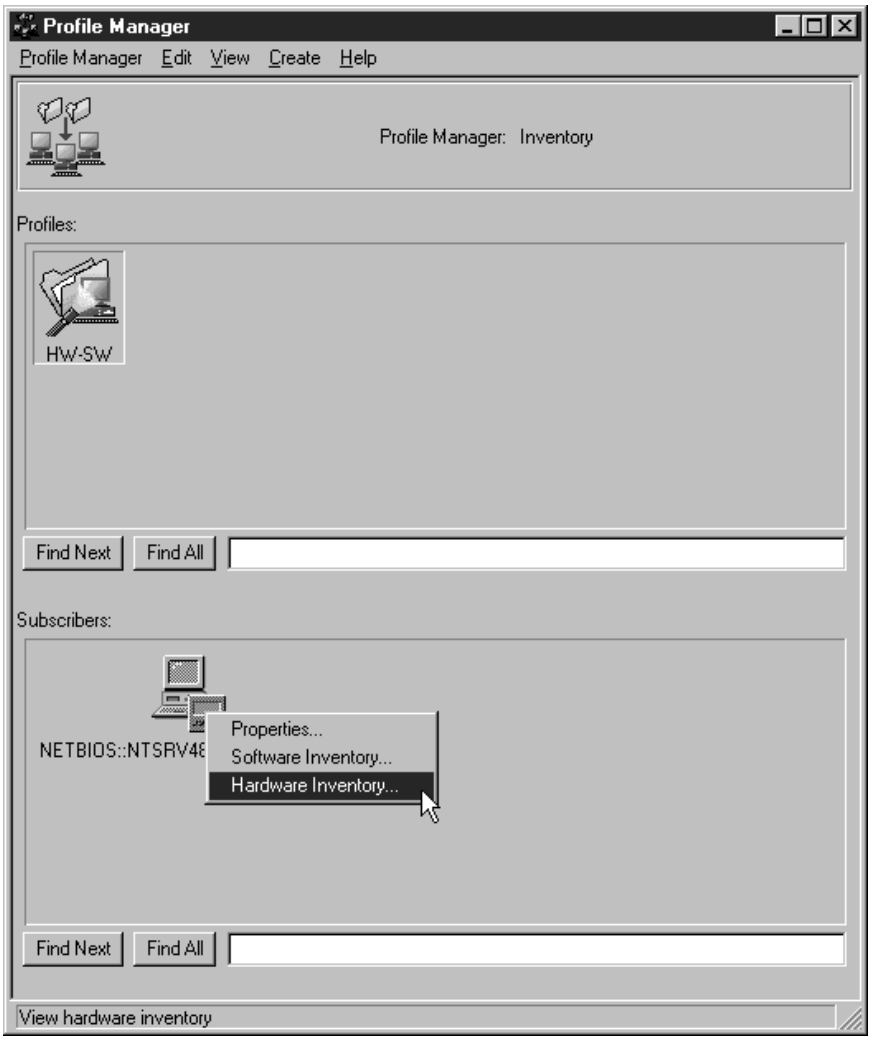


Figure 241. Running the Hardware Query

The information displayed is the result of running the default Tivoli query called INVENTORY_HARDWARE.

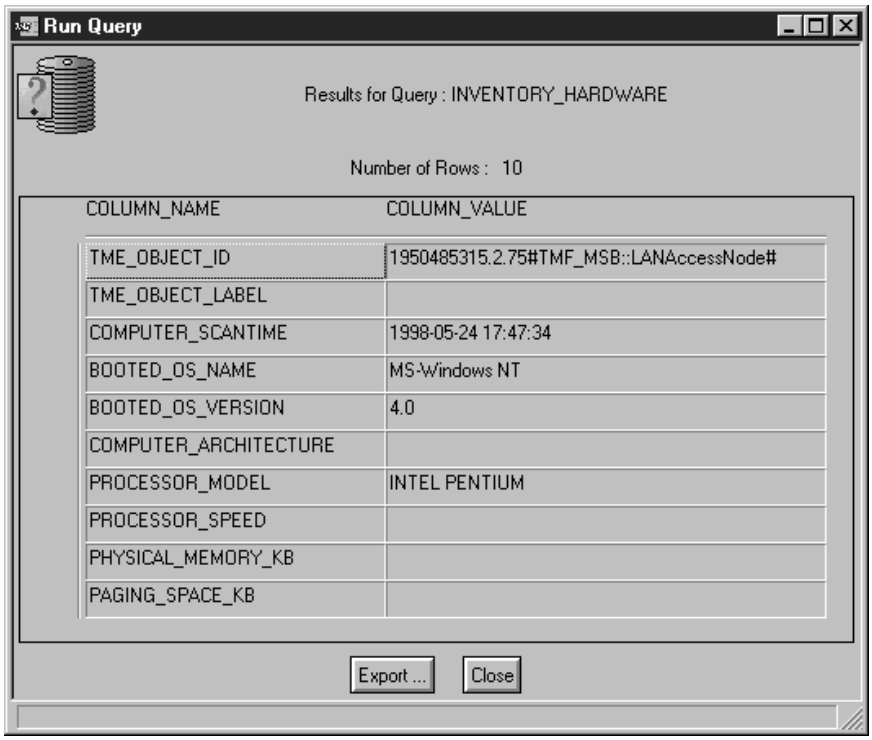


Figure 242. Results of Query

Note: In our environment we were only able to get the hardware inventory data. There was a problem with our implementing, such that, we were not successful in getting the software inventory. The way to get it is described in the following paragraph.

To obtain the software inventory you must create a new query and specify in the Repository field, `inventory` and in the Table/View Name field, `CREATE_OS_DETAILS_VIEW`.

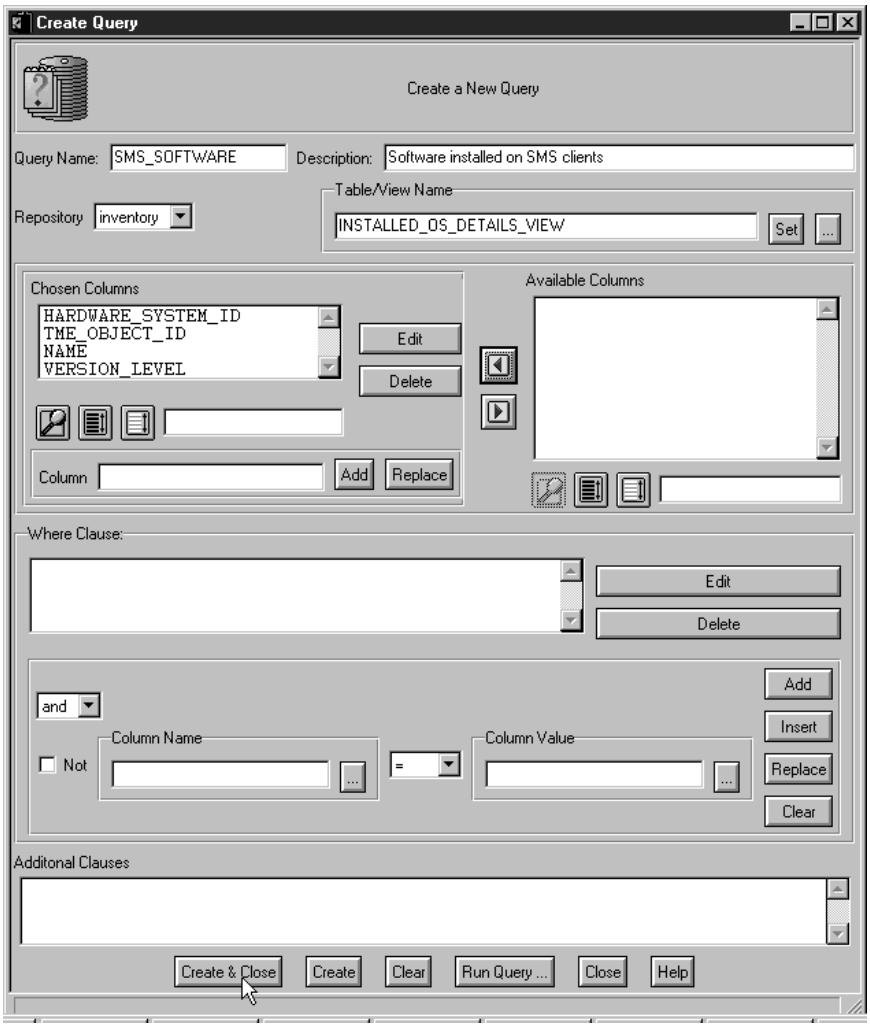


Figure 243. Create Profile Window

After distributing the inventory profile to the SMS clients, run this query to display the information about the software installed in the SMS clients.

4.8.4 Receiving Alerts

If you have already configured the TEC event server as described in 5.4.4, “Configuring the TEC Event Server” on page 249 and have completed the steps in 1.9, “Importing LAN Access Event Classes” on page 64 you will not need to do anything else to start receiving alerts on the Tivoli Enterprise Console from the SMS clients.

The LAN Access event adapter monitors for events created by the SMS provider. You do not need to start the LAN Access event adapter, since it is automatically started when the LAN Access managed node starts. But if you want to stop the event adapter, enter at the command prompt:

```
tecadst shutdown
```

To restart it:

```
tecadst.cmd
```

The tecadst.cmd script follows:

```
CALL %SystemRoot%\system32\drivers\etc\tivoli\setup_env.cmd
tecad_msb.exe %1 %2 %3 %4
```

Chapter 5. Integration with the Framework

This chapter shows how Tivoli LAN Access integrates with the following Tivoli applications:

- Tivoli Software Distribution
- Tivoli Inventory
- Tivoli Event Console

5.1 Tivoli Application Support

Tivoli LAN Access enables network administrators to use the Tivoli Inventory, Software Distribution, and Enterprise Console applications to access network data through the SMS, LANDesk, and Netfinity LAN management applications. The following levels of these Tivoli applications are supported:

- Tivoli Courier 3.0 and Tivoli Software Distribution Version 3.1
- Tivoli Inventory Version 3.1 and V3.2
- TME 1.0 Enterprise Console Version 2.6 and 3.1

LAN Access and these Tivoli applications use combinations of the following networking functions to access LAN client data:

- Topology (discovery)
- Inventory
- File transfer
- Remote command execution
- Alert recognition

5.1.1 Using Tivoli Software Distribution

Tivoli LAN Access support of the file transfer and remote command execution functions enables the Tivoli Software Distribution service to:

- Create file packages for distribution from the TME to client nodes of supported LAN management applications.
- Remotely execute specified application programs on these LAN clients.

5.1.2 Using Tivoli Inventory

Tivoli LAN Access support of the topology and inventory functions allows the Tivoli Inventory service to collect descriptive information from clients of supported LAN management applications. You can collect vital information on LAN clients located outside the Tivoli Management Region (TMR) using a single management station within TME. This information can then be used as a basis for other network management tasks, for example, performing software updates.

5.1.3 Using the Tivoli Enterprise Console

Tivoli LAN Access event support enables you to use the TME event service and the enterprise console to monitor for events that originate from LAN clients located outside a TMR. To capture LAN alerts, LAN Access supplies all required software components, including a dedicated event adapter and event class definitions.

5.1.3.1 Example of Using the Tivoli Enterprise Console

In this section we show how to use TEC with LANDesk. The same procedures can be used with the other MPM's.

If TEC has been configured properly, the MPM will send the alert to TEC. To see the information that is sent up to TEC, from your TME Desktop log on to your TMR (see Figure 244).

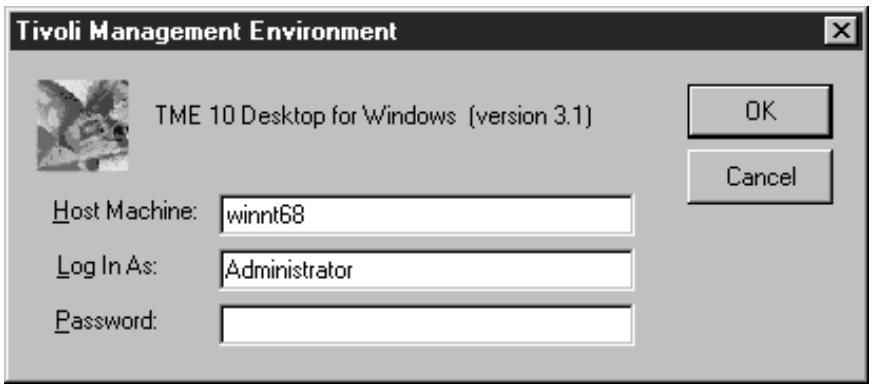


Figure 244. Desktop Logon Panel

It could take some time before Figure 245 on page 201 comes up. This depends upon what you have configured to start at the logon to your TMR. If you see a red arrow circling the globe on the Event Server icon, the server is up and running. If not, you must start it by right clicking on the **Event Server** icon then **Start-up**. While the event server is starting the arrow circling the globe is just an outline. Starting the event server can take a little bit of time and resource. You will know the event server is started when the server turns solid red (see Figure 246 on page 202).

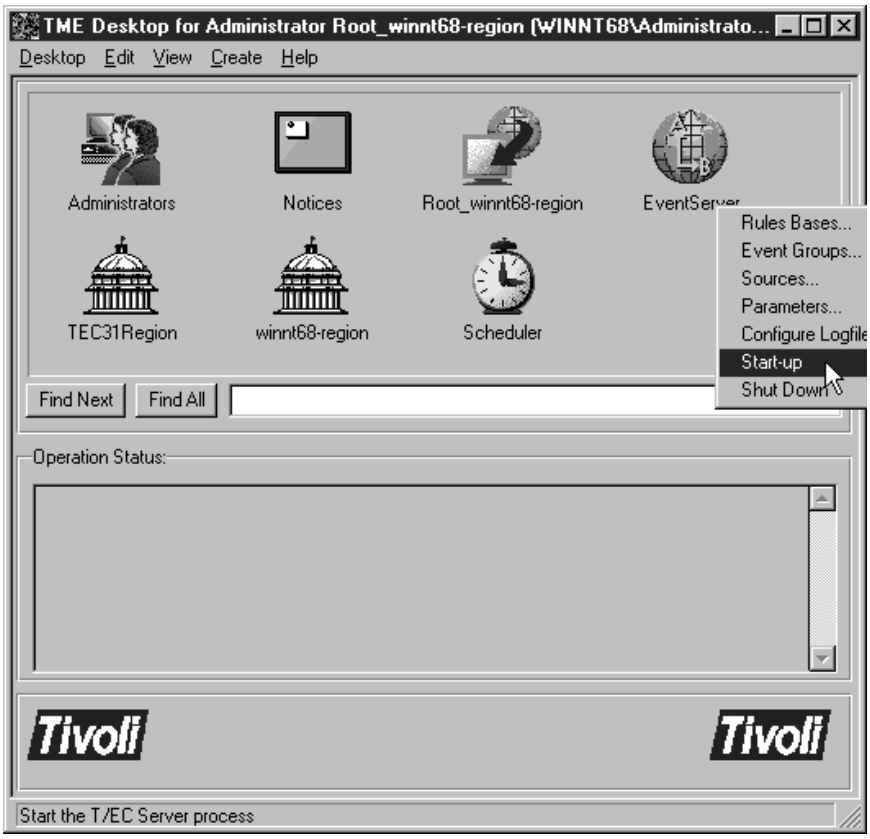


Figure 245. TME Desktop

If you had to start the event server, you will see two messages in the Operation Status box:

1. `The Tivoli Enterprise Console Server is Initializing...`
2. `Tivoli Enterprise Console Server successfully started.`

If not, this box is empty until you start the TME Enterprise Console. To start the Enterprise Console, double-click on its icon. In our case the name of this icon was Root_winnt68-region (see Figure 246 on page 202). The following two messages will eventually appear in the Operation Status box:

1. `Retrieving the event cache from the Tivoli Enterprise Console Server`
   This may take some time. The Enterprise Console is not started until you receive the second message.
2. `Tivoli Enterprise Console initialization complete.`

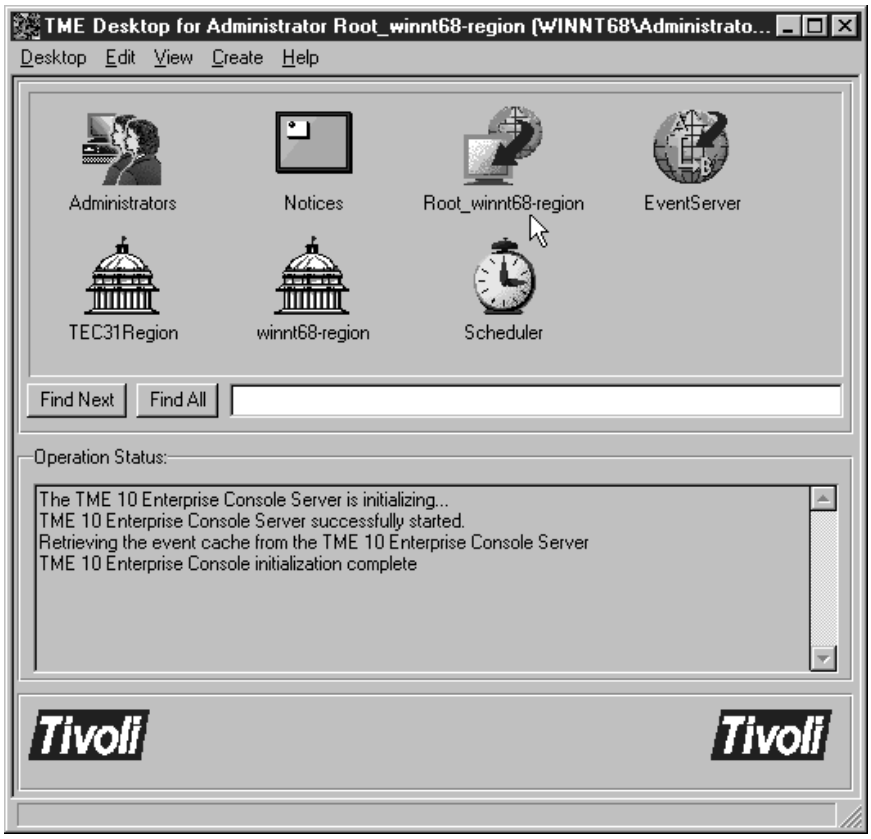


Figure 246. TME Desktop with TEC Server and Enterprise Console Started

As soon as the initialization has completed two windows will come up:

1. The TME Event Source (Figure 247 on page 203).
2. The TME Event Group (Figure 248 on page 203).

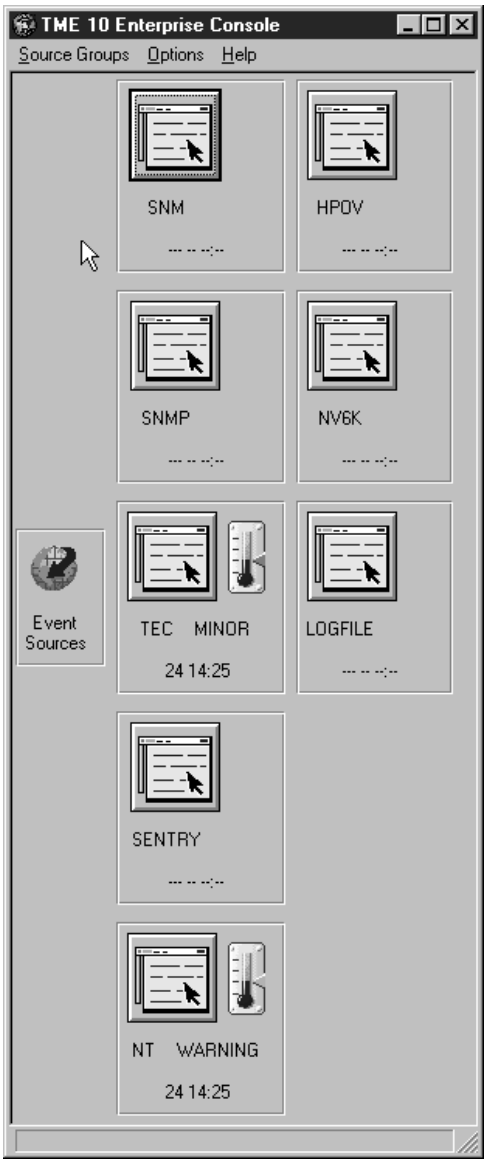


Figure 247. TME Event Source

If in Figure 248 you click on the All minor group, it will bring up Figure 249 on page 204. If you have not set any filters, you will see all the alerts TEC knows about.

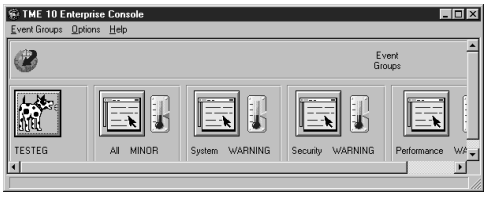


Figure 248. TME Event Groups

To view the alert, either double-click on the listing or highlight it by clicking on it and then clicking on the **View Message** button.

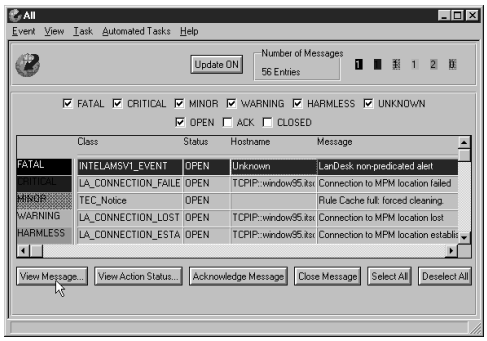


Figure 249. TME All Group's Display

The messages in Figure 250 on page 205 and Figure 251 on page 206 were created by a CPU utilization threshold being exceeded. This created a LANDesk event, that started an MPM tool. The MPM provider then sent the alert to the managed node and the managed node then sent it to TEC. All this information is shown in Figure 250 on page 205 and Figure 251 on page 206.

Figure 250. TEC-MPM CPU Utilization Alert 1 of 2

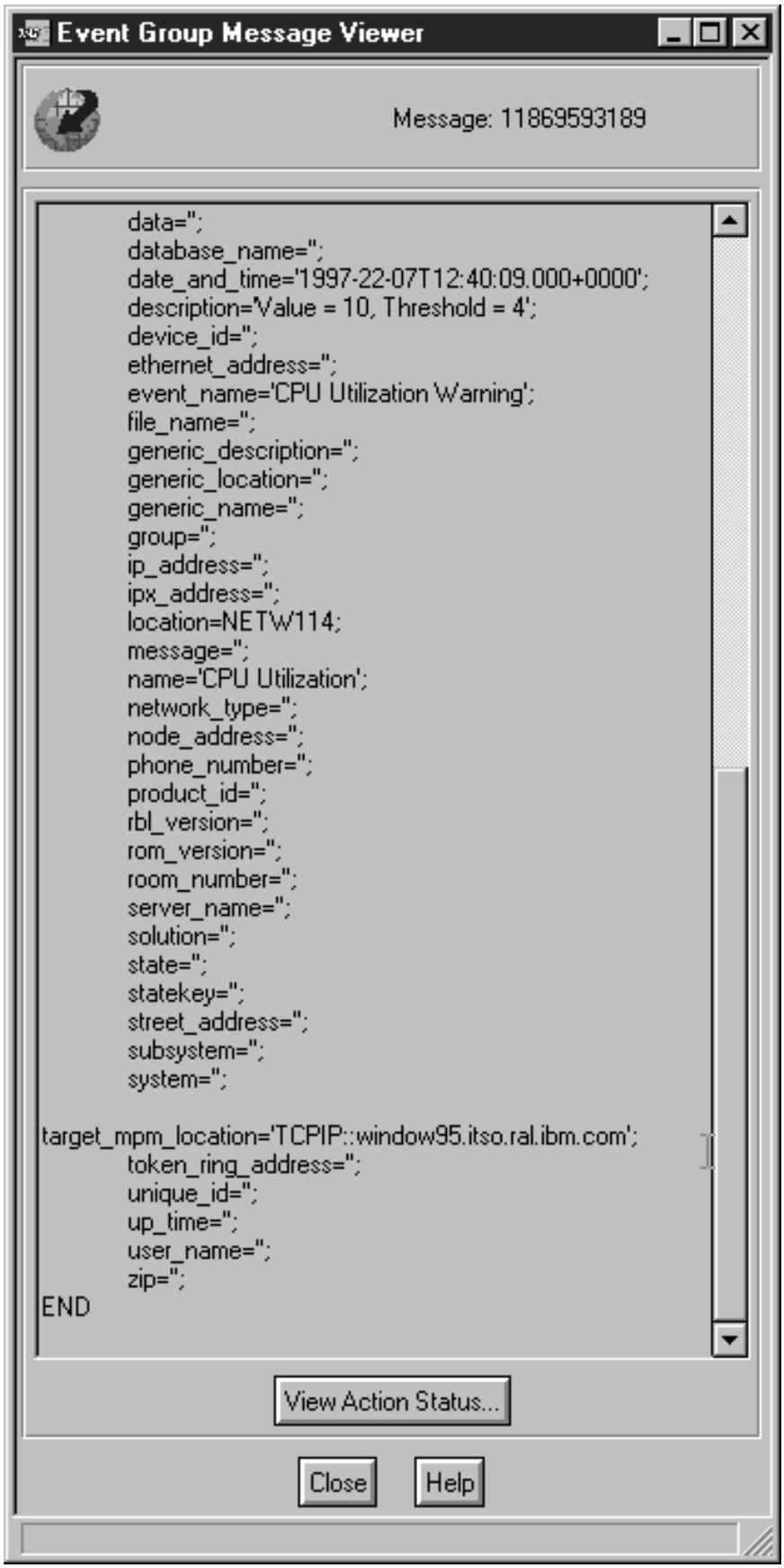


Figure 251. TEC-MPM CPU Utilization Alert 2 of 2

After a CPU threshold has been created, there will be a line across the bar graph as shown in Figure 252 on page 207. If you want to adjust the scaling so that you can read the graph better, the percentage can be adjusted with your mouse by placing the cursor on the line and holding down the right mouse button. Then, just move the line to the new threshold level.

Attention

If you place the threshold under 5%, it will cause AMS.NLM to page fault the NetWare Server.

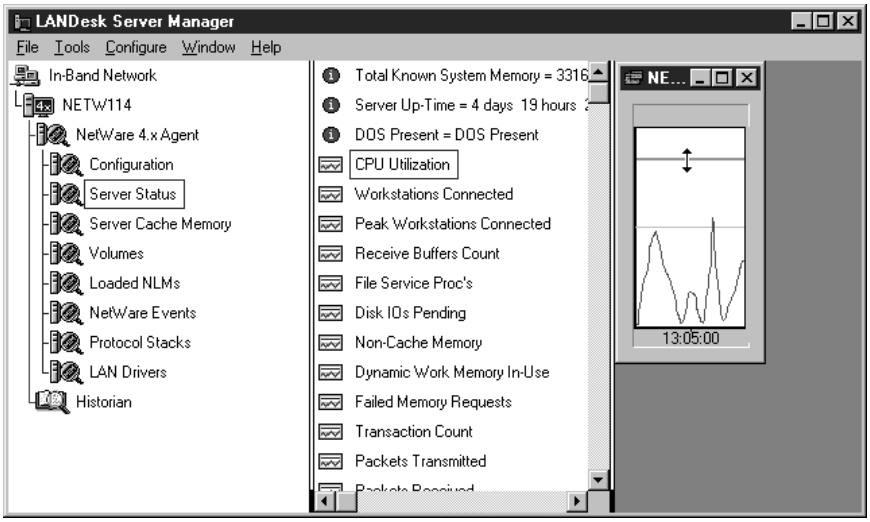


Figure 252. Adjusting a CPU Threshold

5.2 Installing TME Software Distribution 3.1

Use the following steps to install Software Distribution on the TMR server and managed nodes from the desktop. You must install Software Distribution on the TMR server first and then install it on your clients. Insert the Tivoli Software Distribution 3.1 CD and select **Desktop → Install → Product...** to display the Install Product dialog. Select the Software product and clients on which Software Distribution will get installed and click on **Install & Close**.

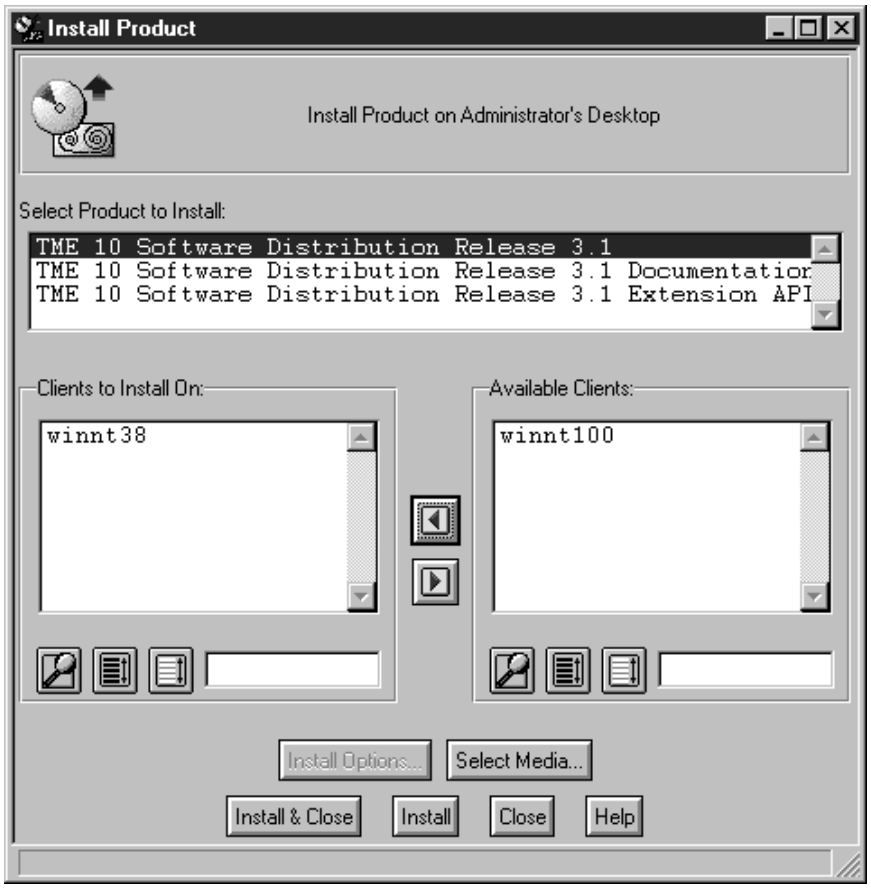


Figure 253. Install Product

After that, the Product Install panel is displayed. If the dependency check passed successfully, click on **Continue Install** to install the Tivoli Software Distribution product(s).

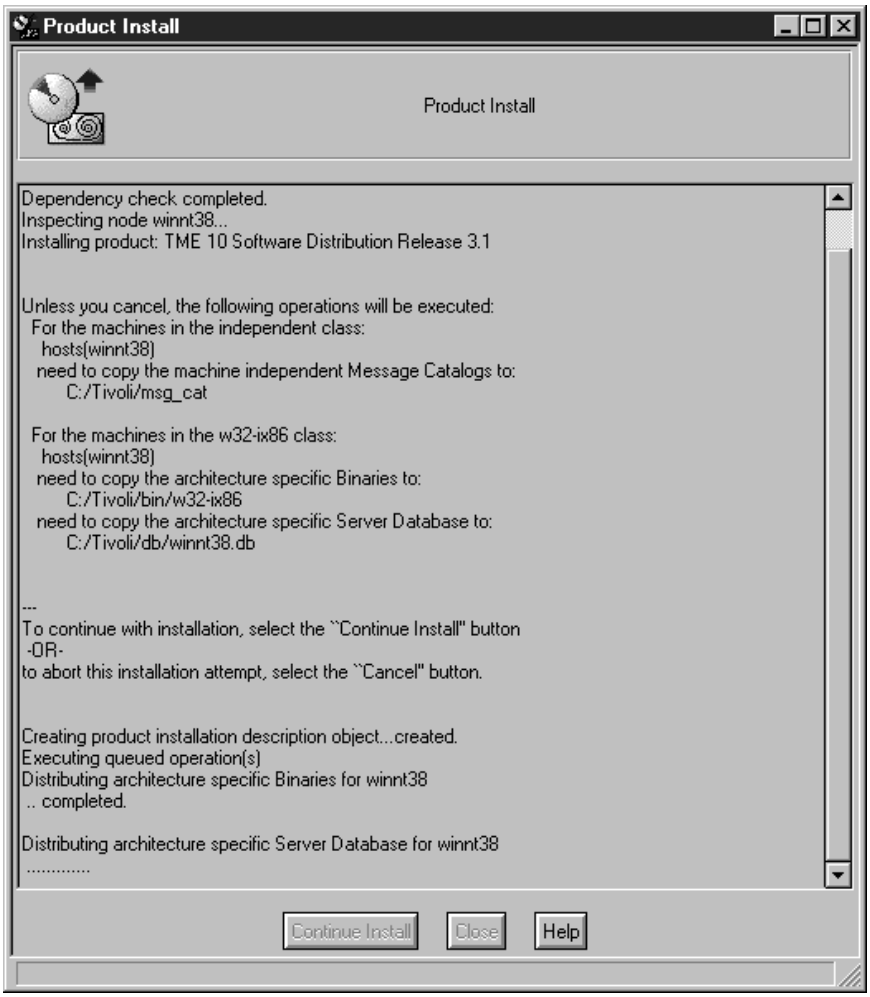


Figure 254. Product Install

5.2.1 Configuring Software Distribution

Use the following steps to create a Software Distribution profile from the desktop:

- Add the FilePackage profile and profile manager resources to the policy region's list of managed resources.
- Create a profile manager in which the FilePackage profile will reside.
- From the Policy Region window, select **ProfileManager...** from the Create pull-down menu to display the Create Profile Manager dialog.

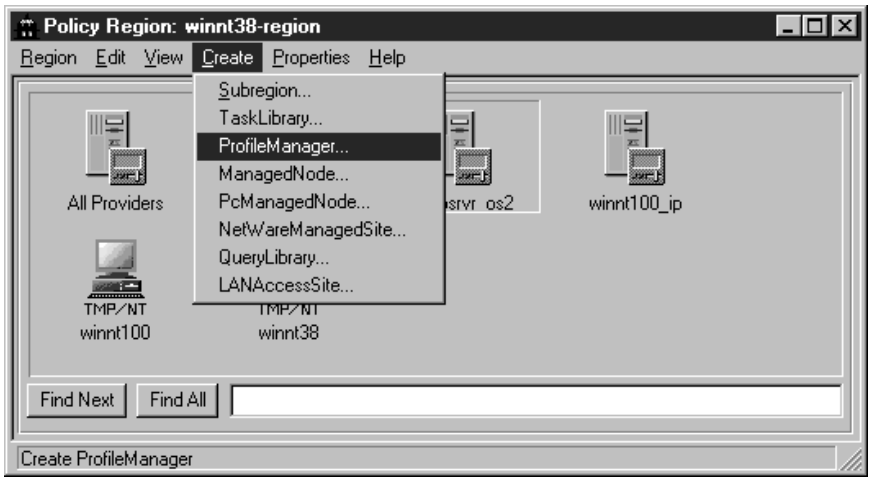


Figure 255. Create Profile Manager in Policy Region

- Enter the name of the profile you want to create and click on **Create & Close**.

Figure 256. Create Profile Manager

- From the policy region, double-click on a profile manager icon to display the Profile Manager window.

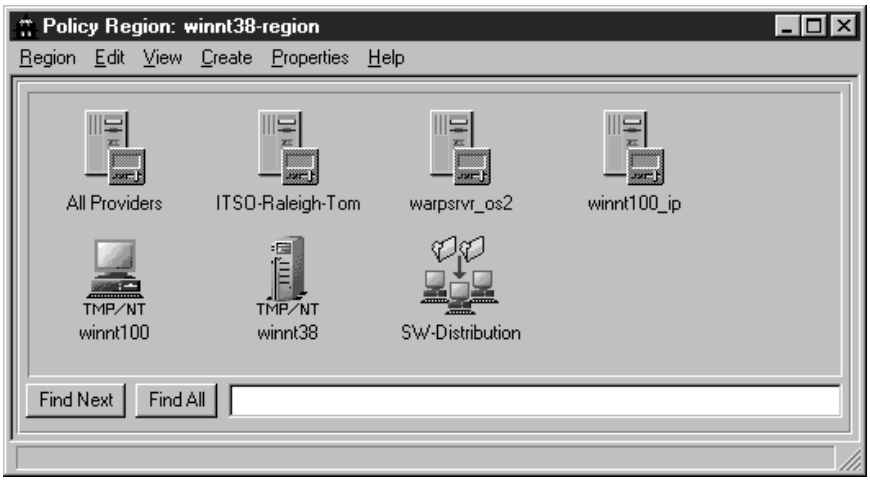


Figure 257. New Profile Manager in Policy Region

- Select **Profile...** from the Create menu in the Profile Manager window to display the Create Profile dialog.
- Enter a unique name for the profile in the Name/Icon Label field that describes the Software Distribution profile.

  Note: You should avoid using characters other than alphanumerics, - and _.
- Select **FilePackage** from the Type list.

  Note: If the FilePackage resource is not available, you must add this resource type as a managed resource of your policy region. For more information on this procedure, see 1.5.1.2, “Configuring the Policy Region” on page 18.
- Click the **Create & Close** button to create the new profile and return to the Profile Manager window.

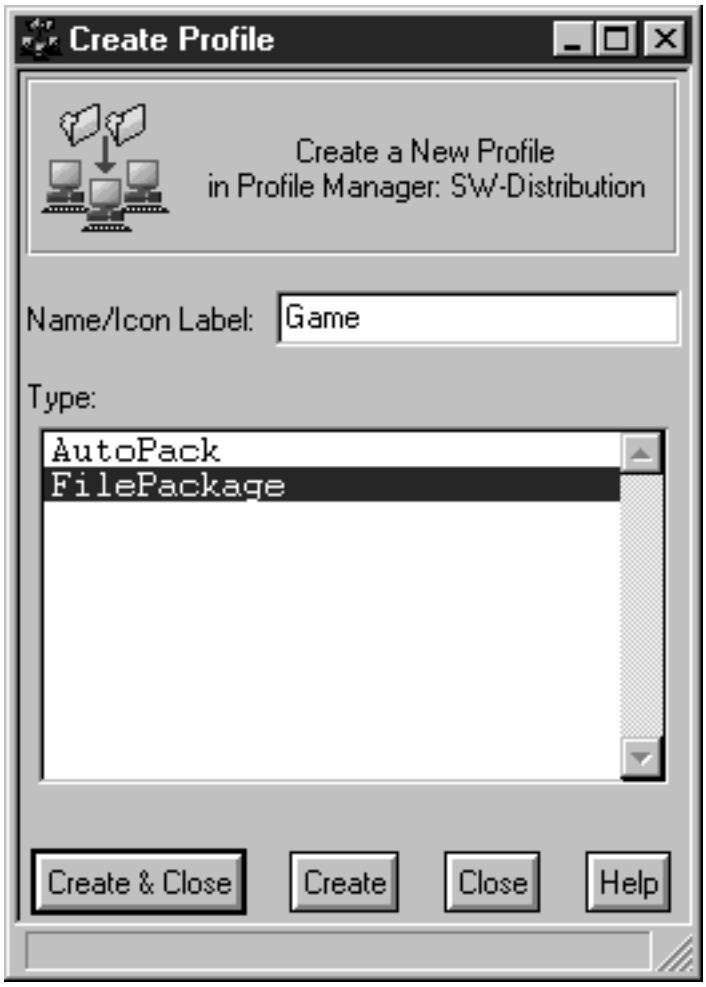


Figure 258. Create Profile

An icon representing the newly created Software Distribution profile is displayed in the Profile Manager window.

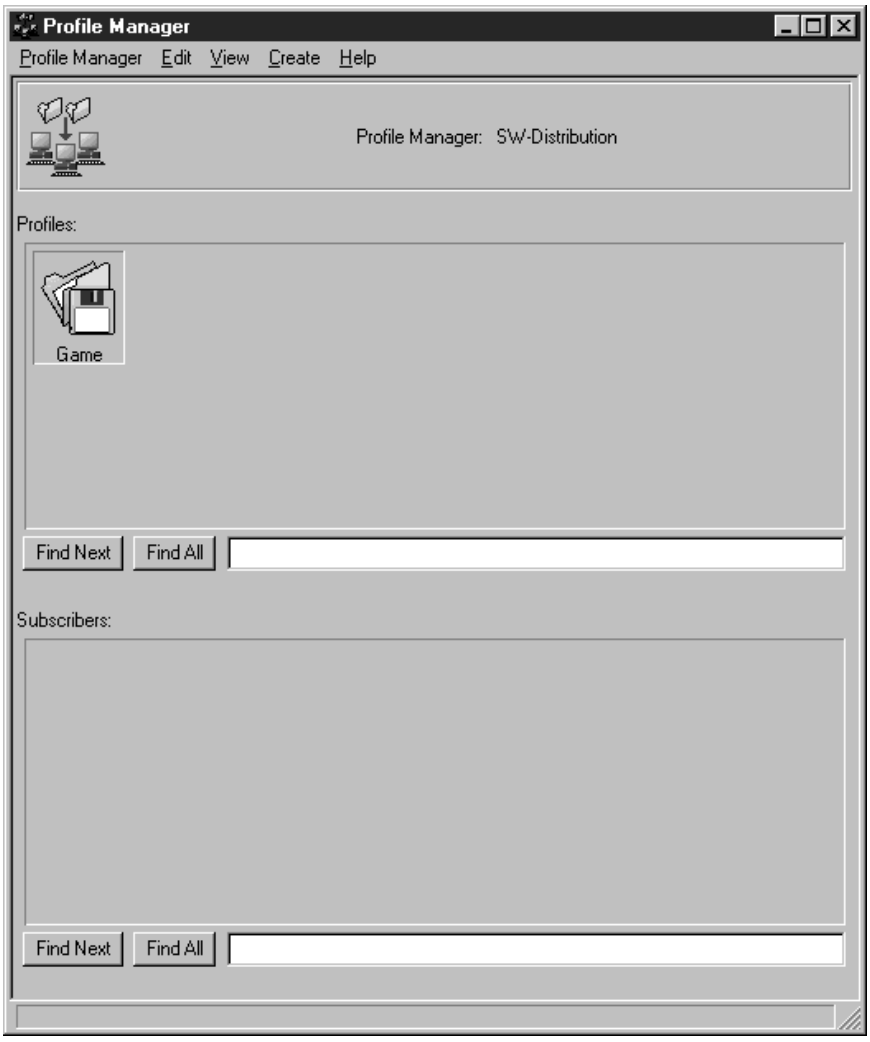


Figure 259. Profile Manager

- Double-click on the **Game** file package icon to display its File Package Properties window:

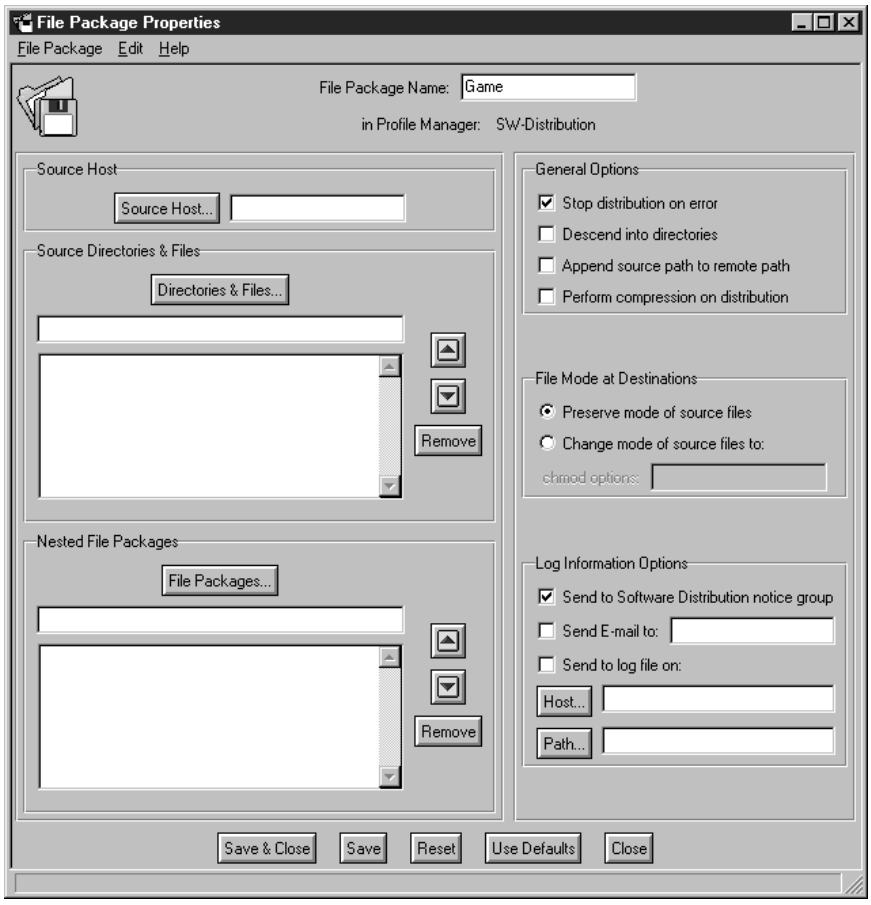


Figure 260. File Package Properties

- In the Source Host field, specify the machine on which the source files reside.

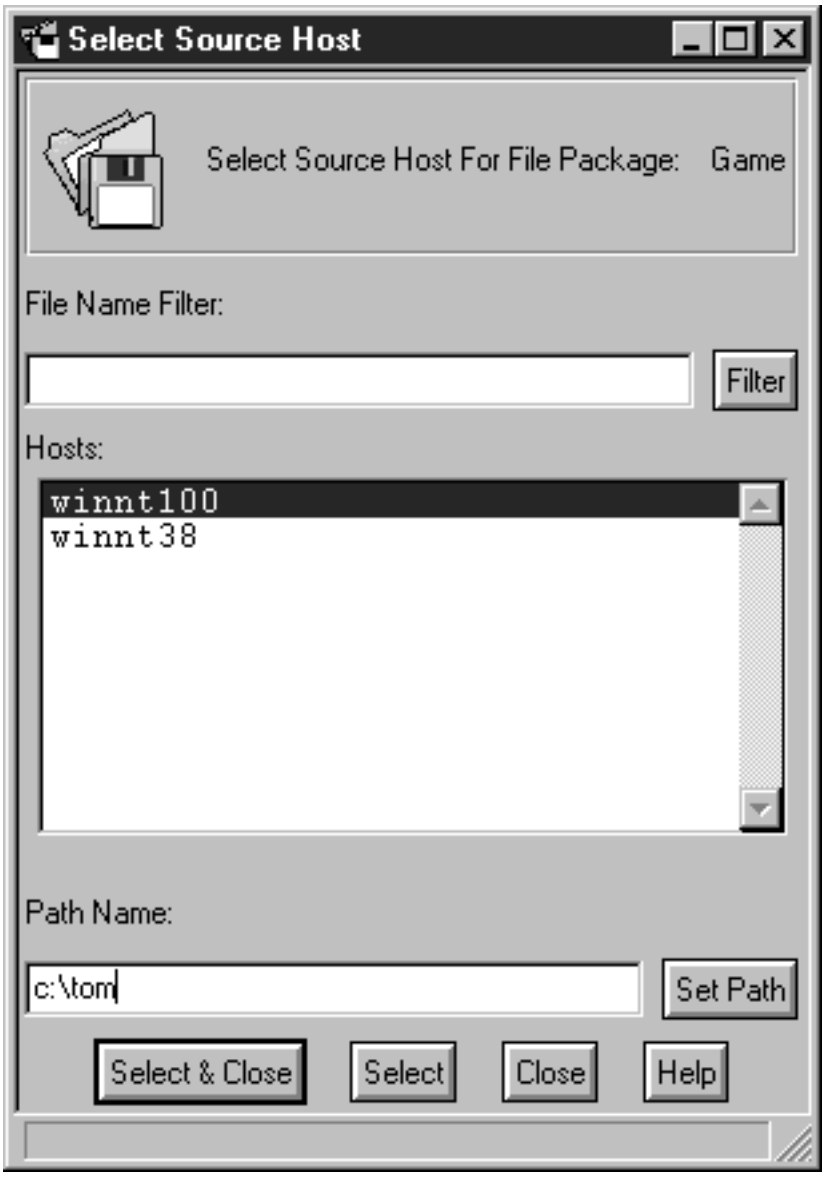


Figure 261. Select Source Host

- Select the appropriate directory and files that you want added to the file package.

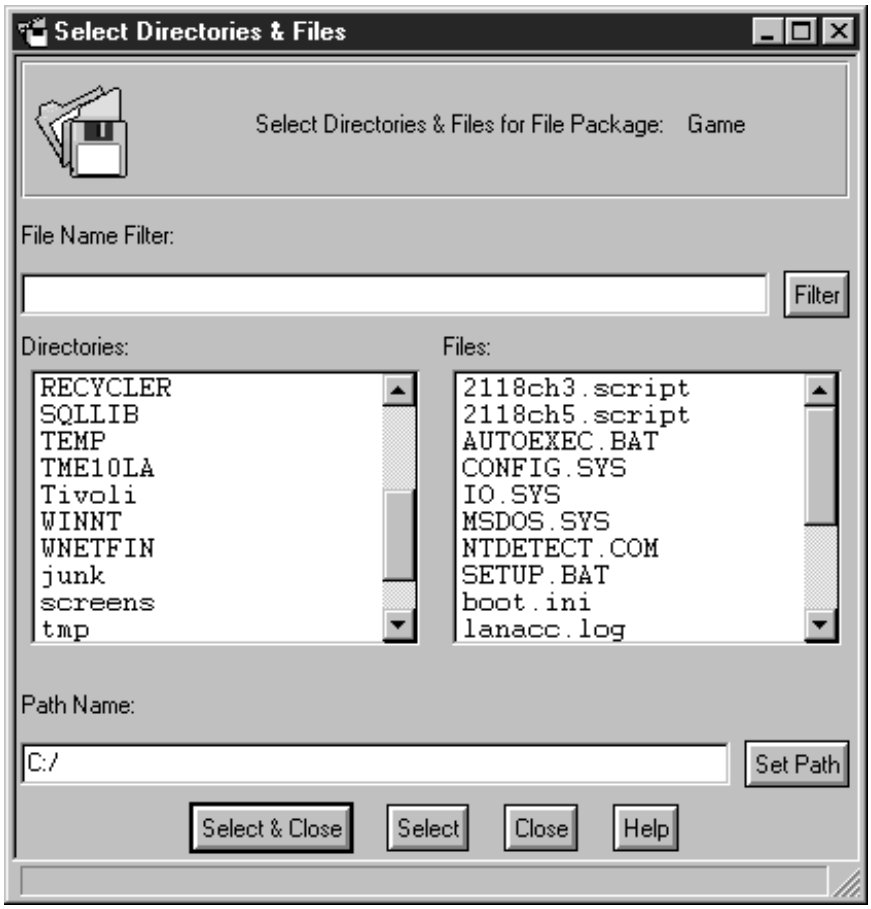


Figure 262. Select Directories & Files

- Set the distribution options from the General Options check boxes:
  - If you select the Stop distribution on error check box and an error occurs during a distribution to one of the target machines, the distribution should stop so that you can determine the cause.
  - Select the **Descend into directories** check box. This option distributes the contents of any subdirectories that may be included in the source directories.
  - Select the Append source path to remote path check box if the same directory structure should be created on the destination machine.
  - Select the Perform compression on distribution check box if you have large files to distribute. This will reduce the time of file transfer.

  File Mode at Destinations:
  - Select the Preserve mode of source files radio button to set the permission of the distributed files to those of the source files.
  - Select the Change mode of source files to radio button if you want the file mode (UNIX) to be changed.

  Set the logging options:
  - If you select the Send to Software Distribution notice group check box, Software Distribution sends information to the notice group whenever a file package operation is performed.

– Select the Send E-mail to check box and enter the appropriate e-mail address if needed.

– Select the Send to log file on check box to have Software Distribution send information to the specified log file.

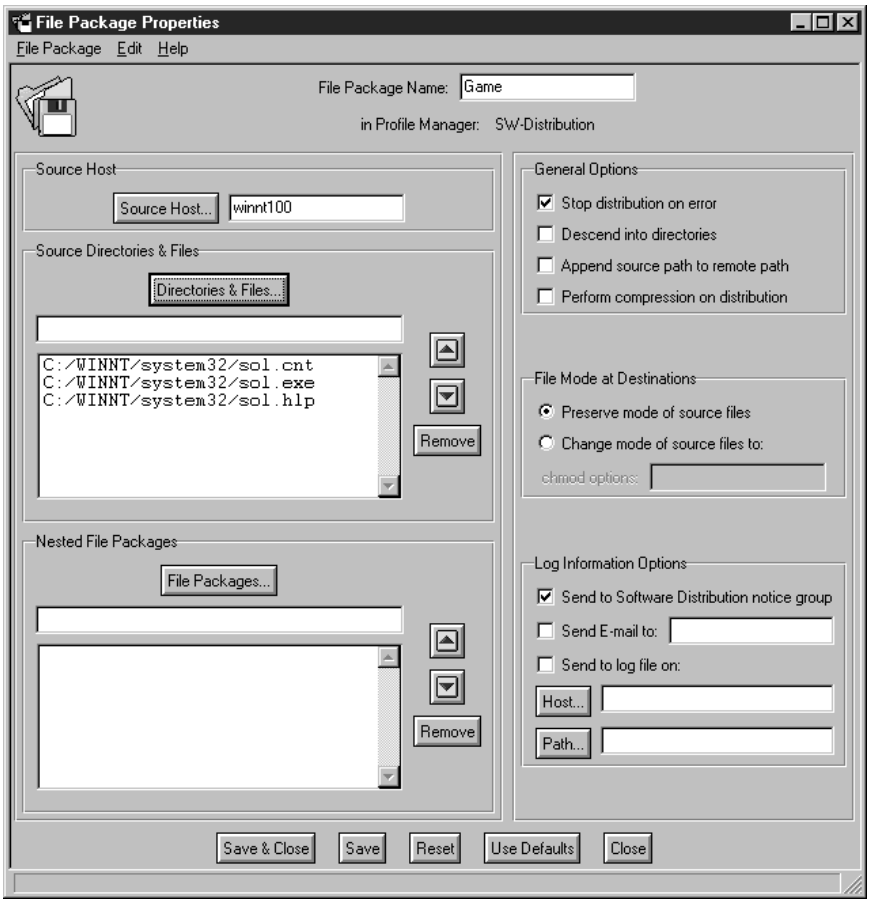


Figure 263. File Package Properties

- Define platform-specific properties that determine where the distributed files will reside and what configuration programs should be run on the target.

  To set NT options, select **Platform-Specific Options -> Windows NT Options...** from the Edit menu. Software Distribution displays the File Package Windows NT Options dialog:

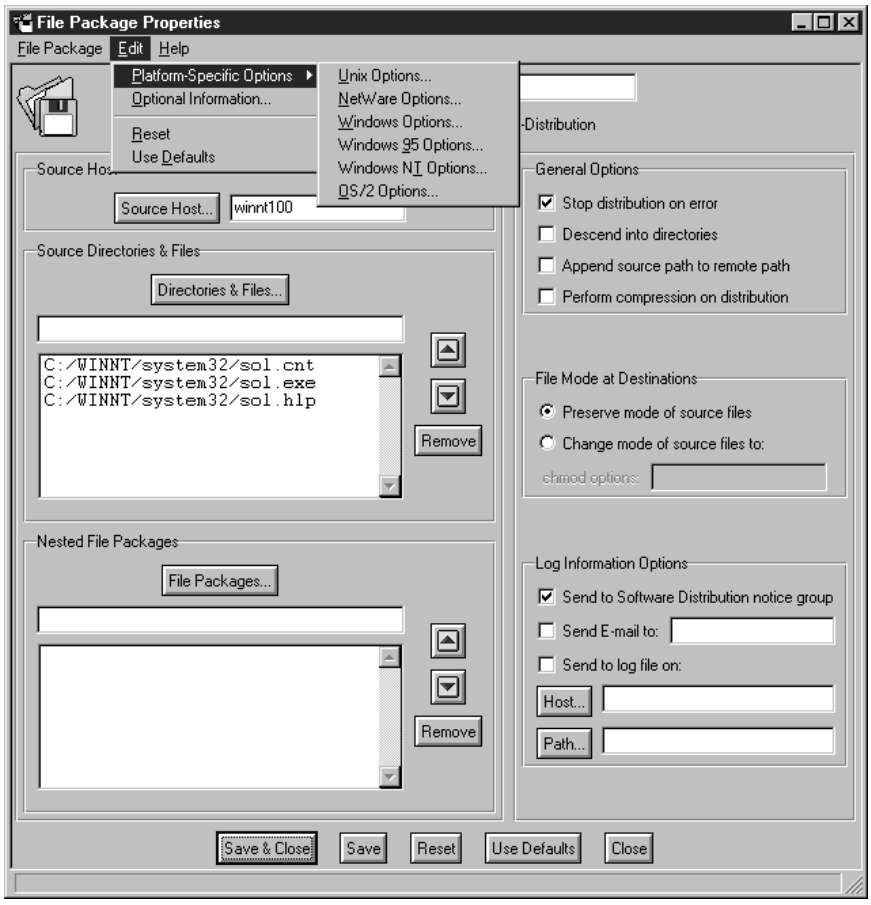


Figure 264. Select Platform-Specific Options

- In the Destination Directory Path field, specify where the files distributed by Software Distribution will reside on the target.
- If you want to have a script before or after distribution to be executed, click the Before Distribution or After Distribution button under BAT/EXE/COM Options. You can also specify whether there is script to be executed after removal or on a later commit time.

  If you have decided to run a script, you have to specify where to get the BAT/EXE/COM file from. Select the Source Host or the Subscribers radio button and enter the path and file name of the file to be executed. In addition, you can specify parameters to be used by the execution program.

  If there is a reboot or restart required after distribution, you can also specify this in the radio buttons at the bottom of the menu.

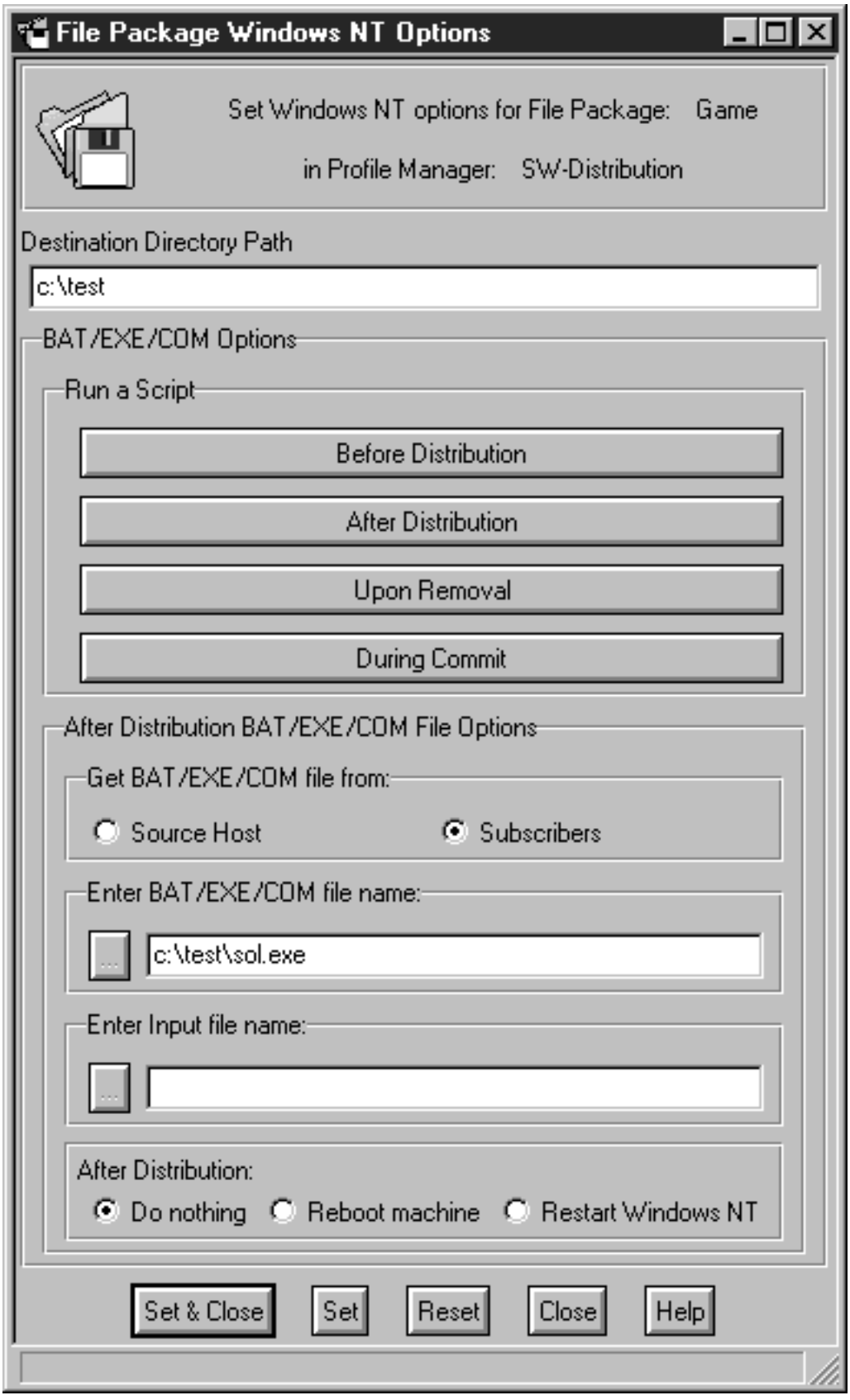


Figure 265. Build File Package Windows NT Options

After finishing all your input you must click the **Set & Close** button to save your options.

- In the File Package Properties Window you have to click the **Set & Close** option to have your new profile created and displayed in the profile manager.

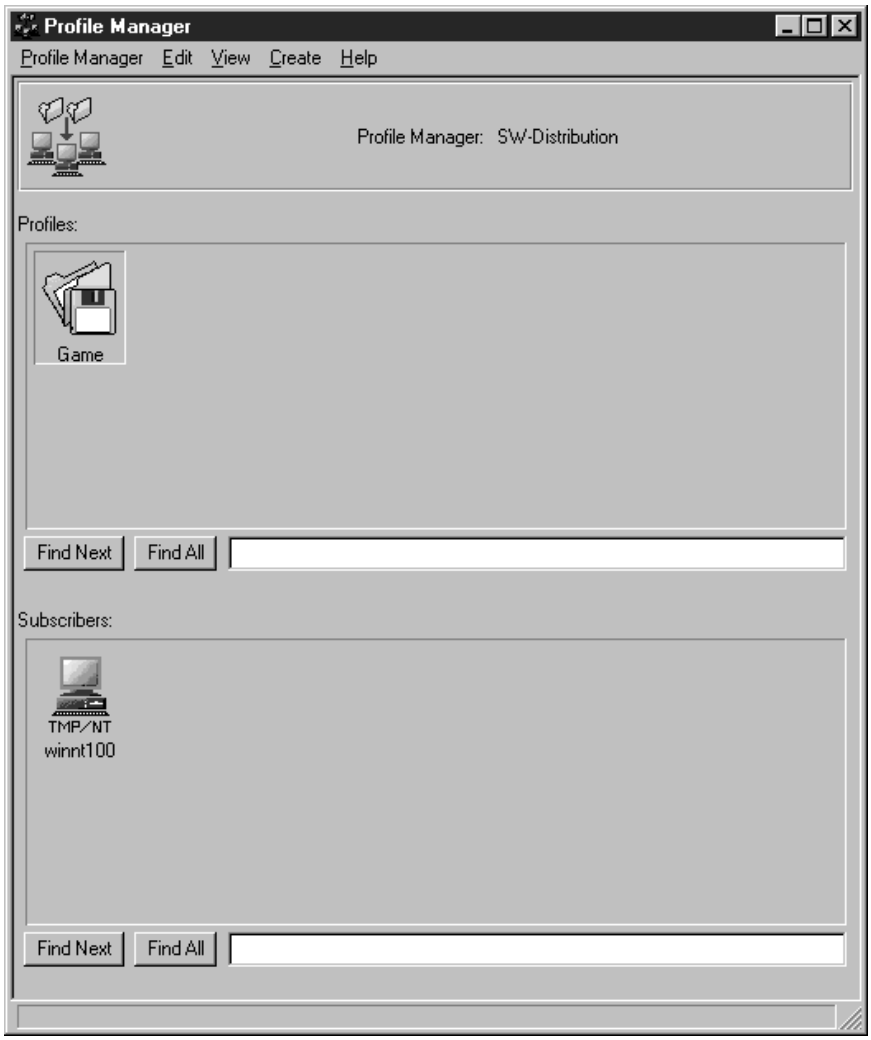


Figure 266. New Profile in Profile Manager

After you have created your profile you have to add subscribers to it. The easiest way to do this is to just drag and drop the required machines from the policy region to the profile manager.

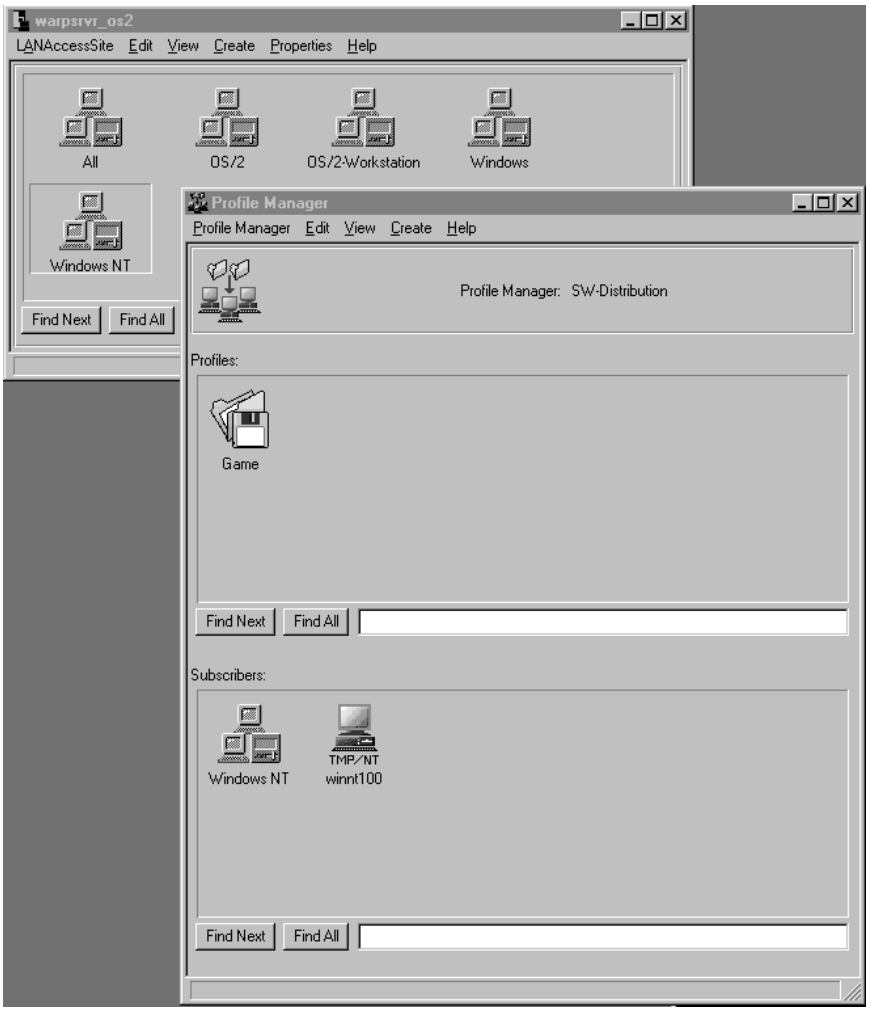


Figure 267. Subscribers Added

5.2.2 Using LAN Access Together with Software Distribution

Use the following steps to add subscribers to the profile manager:

- From the profile manager, select **Subscribers...** from the Profile Manager menu to display the Subscribers dialog.

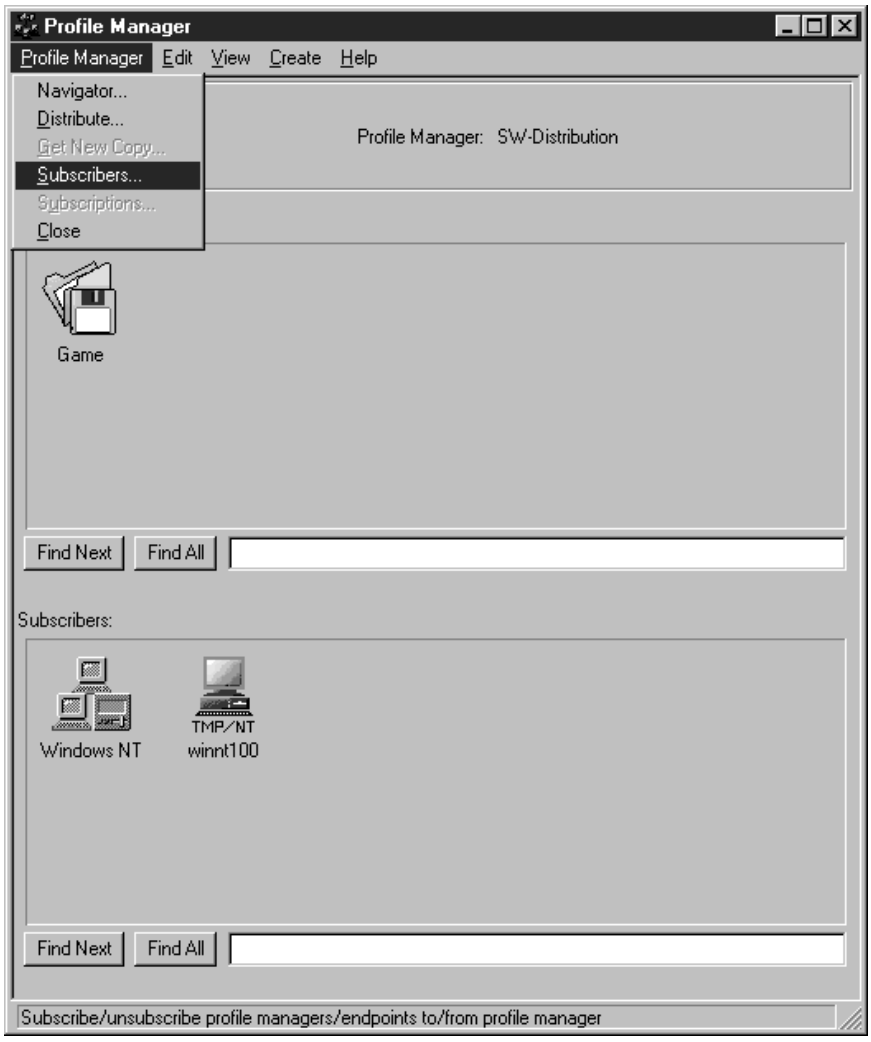


Figure 268. Profile Manager - Add Subscriber

In the Available to become Subscriber box, you see all available resources that are available for distribution:

Managed_Nodes:

- winnt38

LAN Access Sites:

- All providers
- ITSO-Raleigh-Tom
- warpsrvr-os2
- winnt100_ip

LAN Access Collections:

- All
- OS/2
- OS/2-Workstation
- Windows

- Test

All LAN Access Clients

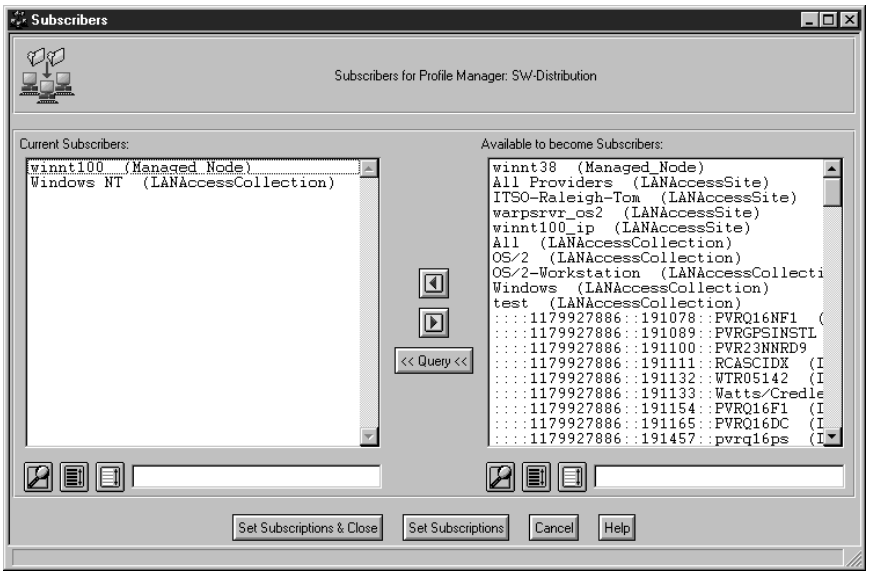


Figure 269. Available Subscribers

- Select a subscriber from the Available Targets scroll list and click the left button to move the subscriber to the Selected Targets scroll list.

  In our case we have already selected the managed node winnt100, the LAN Access Collection Windows NT and the client winnt101. The highlighted client ntdomc is going to be added by clicking on the left arrow.

- Click the **Set Subscriptions & Close** button to set the new subscriptions and return to the Profile Manager window.

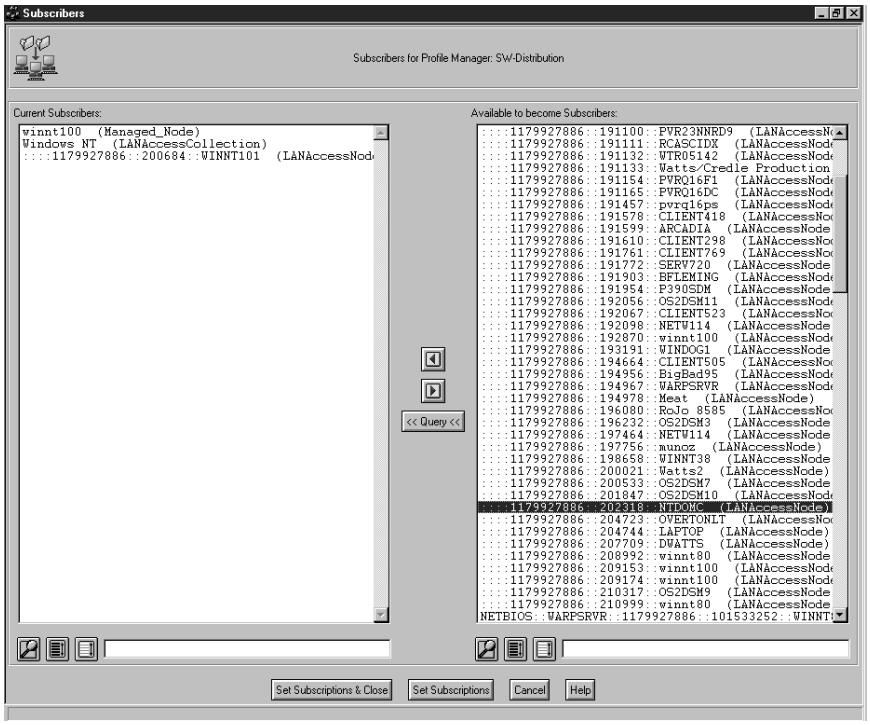


Figure 270. Select the Subscribers

The new subscribers are added to the profile manager's list of subscribers.

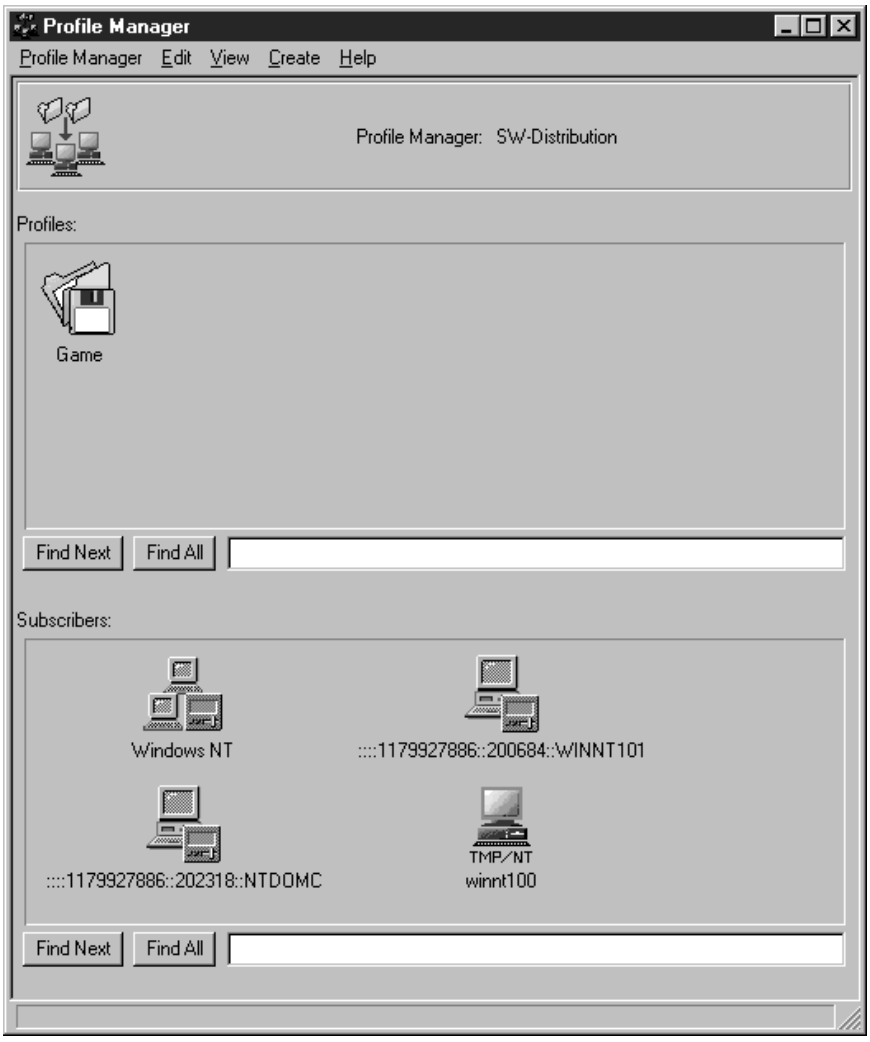


Figure 271. Profile Manager with New Subscribers Added

5.2.3 Distribution to a LAN Access Client

In this example we distribute the game Solitaire to a Windows NT LAN Access Client. We distributed the three required files and created the same test directory on the target machine as well as generated a log file.

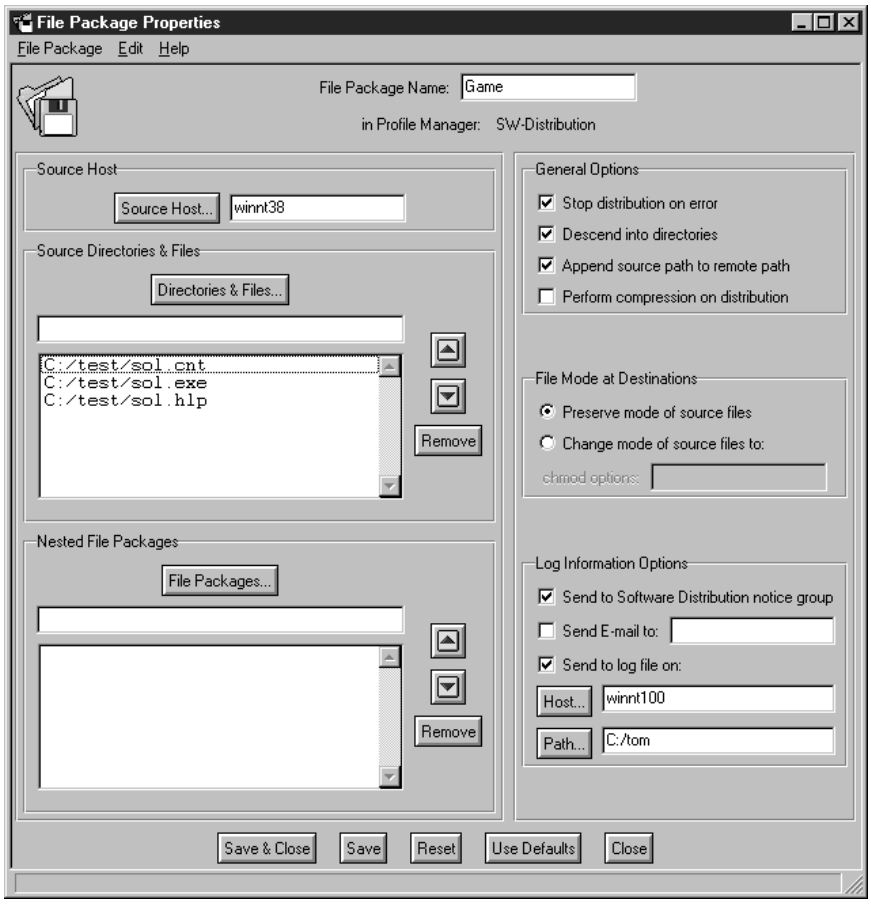


Figure 272. File Package Properties

On the destination machine we installed on the C: drive and ran an After Distribution script sol.bat, which was located on the source host and which started the Solitaire game. After clicking on **Set & Close** and then **Save & Close** you have to choose **Distribute** from the File Package Properties window's File Package option.

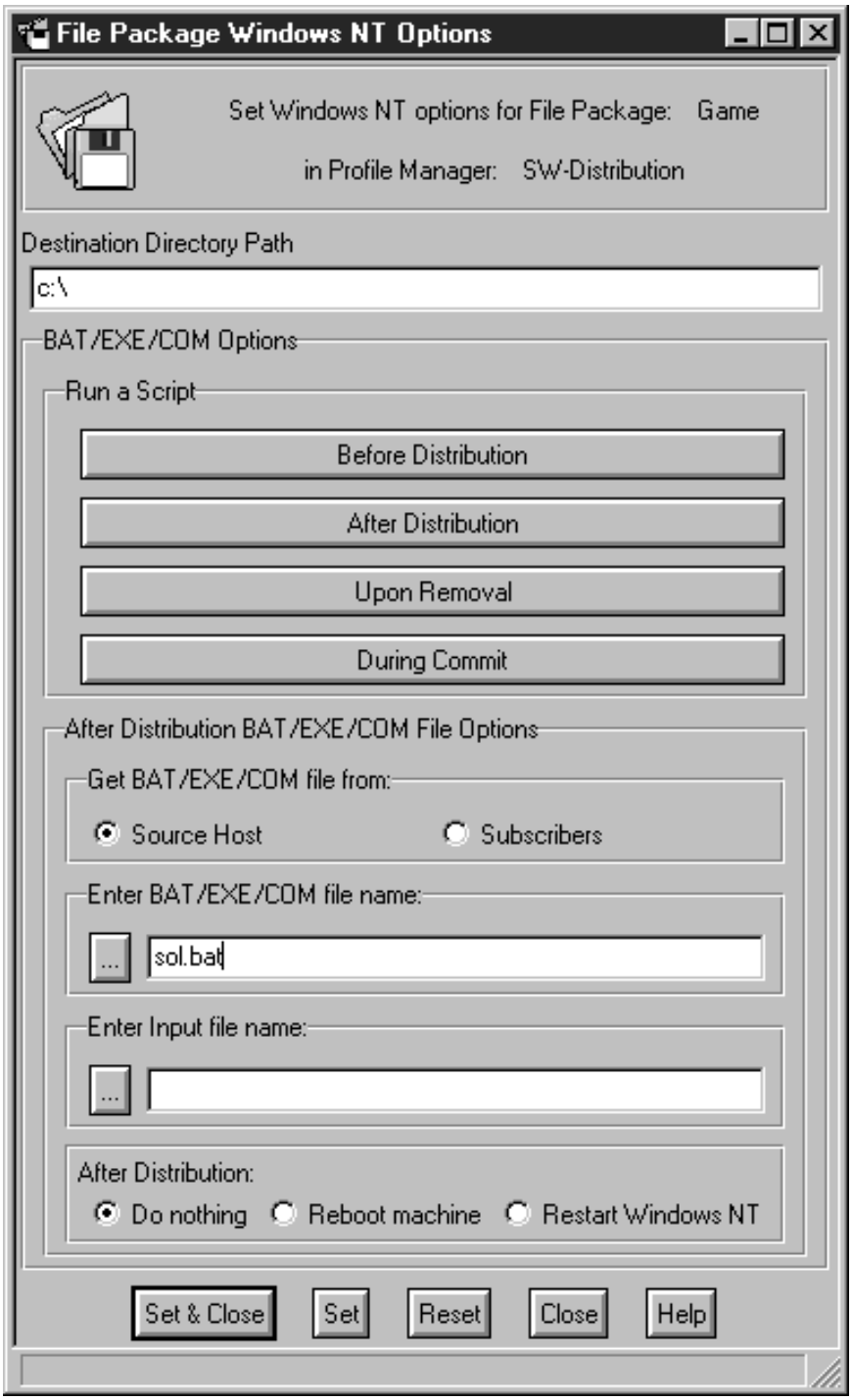


Figure 273. Setting Platform-Specific Options

Set the distribution type from the available list.

Select **Distribution Only** to distribute only the file package. We had no commit script specified in this example.

Set the Distribution Options field to control which files in the file package are distributed.

We selected **Distribute all entries** to distribute all files and directories in the file package.

We chose the winnt101 system from the Available Subscribers list and moved it to the Distribute File Package To list using the arrow. Then, we selected **Distribute & Close** to begin distributing the file package to the target LAN Access Client winnt101.

Note: The dialog will not be dismissed until the distribution is complete. If the distribution fails for any of the subscribers, a pop-up dialog is displayed to inform you of which subscribers distribution failed.

Tivoli Software Distribution will send from the source to the target any source directories and files specified. Then it will start the After Distribution script specified in the file package.

Once the distribution is complete, you may check the log file you specified in the Log Information Options when you created the file Package Properties.

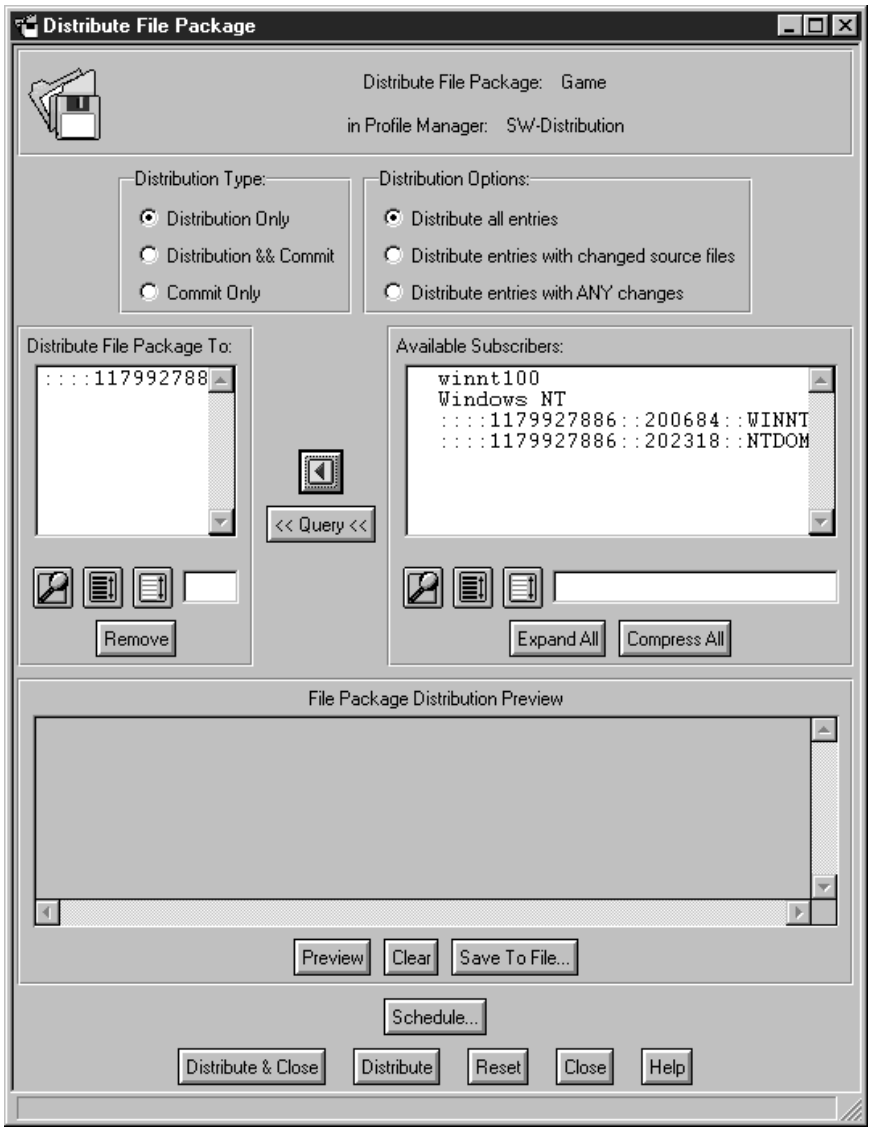


Figure 274. Distribute File Package

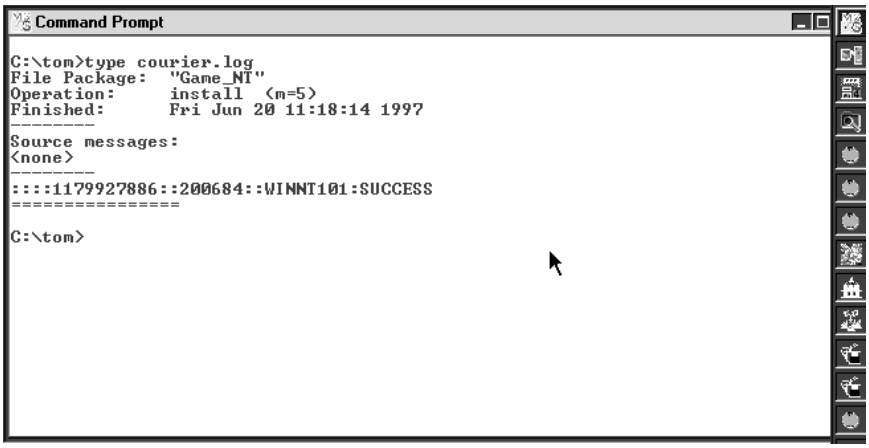


Figure 275. Log File after Successful Distribution

Looking at the target system using Netfinity's Remote Control function, we see that the game has successfully started and using a command prompt we can verify that the directory has been created and the three files transferred.

Figure 276. Target Machine

5.3 Example for Remote Command Execution

We can use the Software Distribution profiles to initiate a remote command to be executed on a target system.

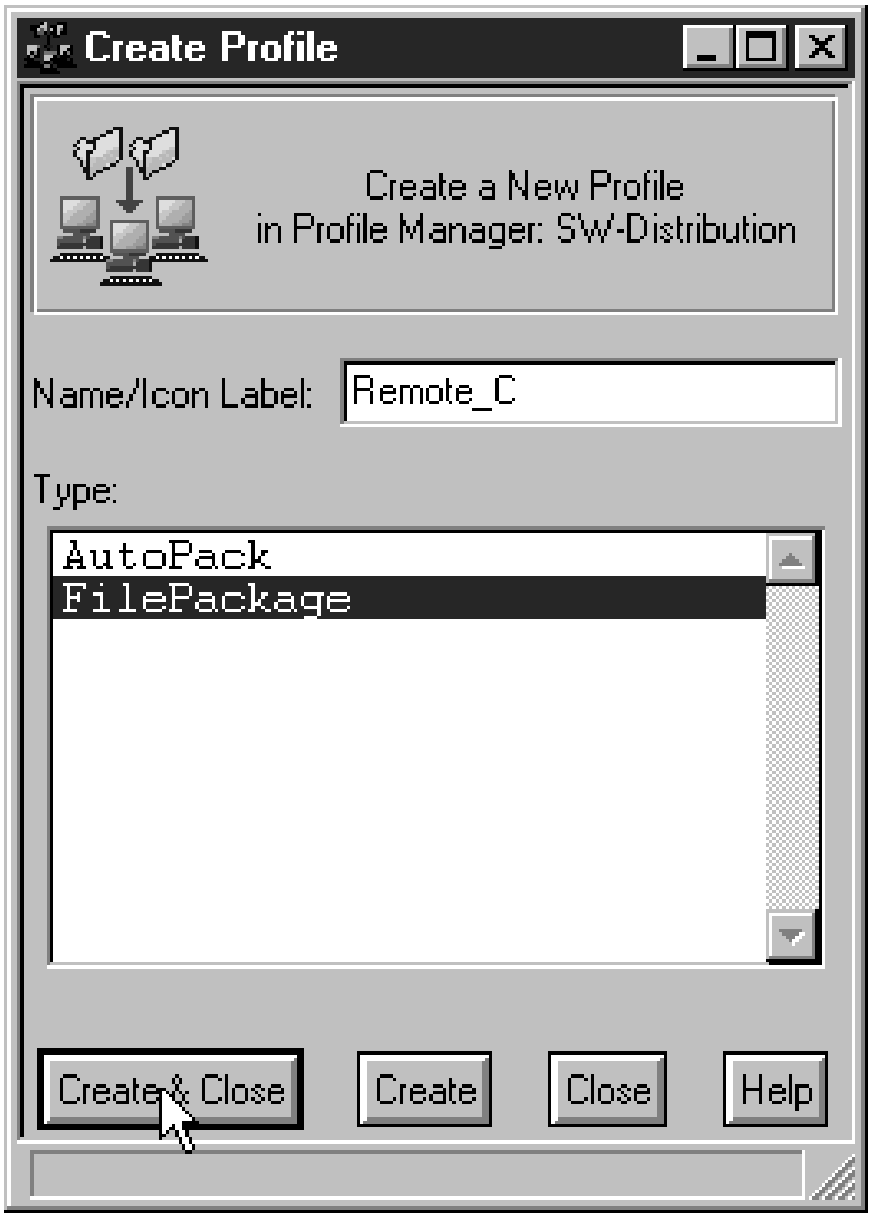


Figure 277. Create Profile

In this example we want the program clock.exe to be executed. We created a During Commit script with the clock.exe file.

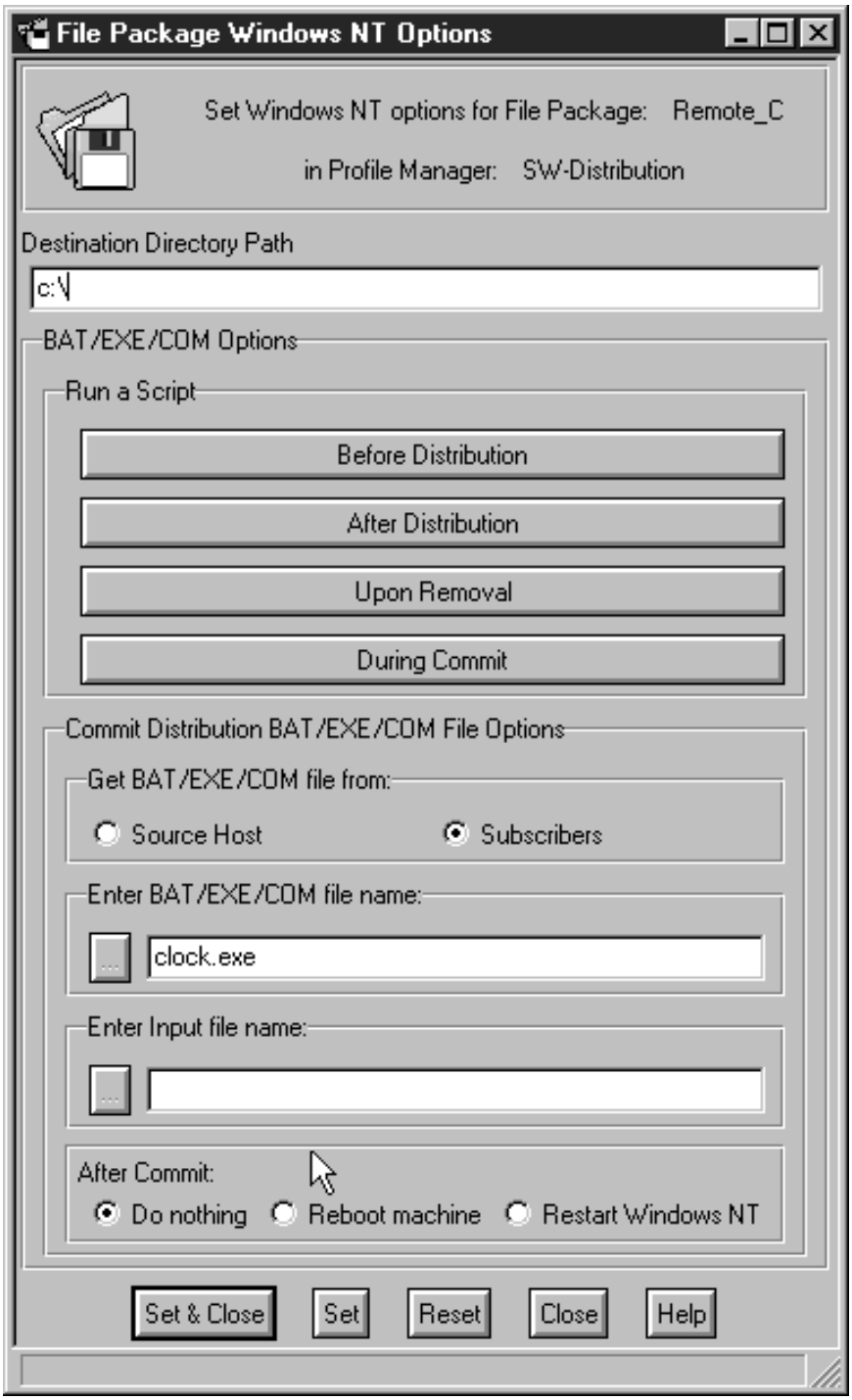


Figure 278. Create Commit Script

In the Distribute File Package window shown in Figure 279 on page 232 click on **Commit Only**. This means nothing is distributed at all. By distributing this profile you just start the specified program clock.exe on the target machine.

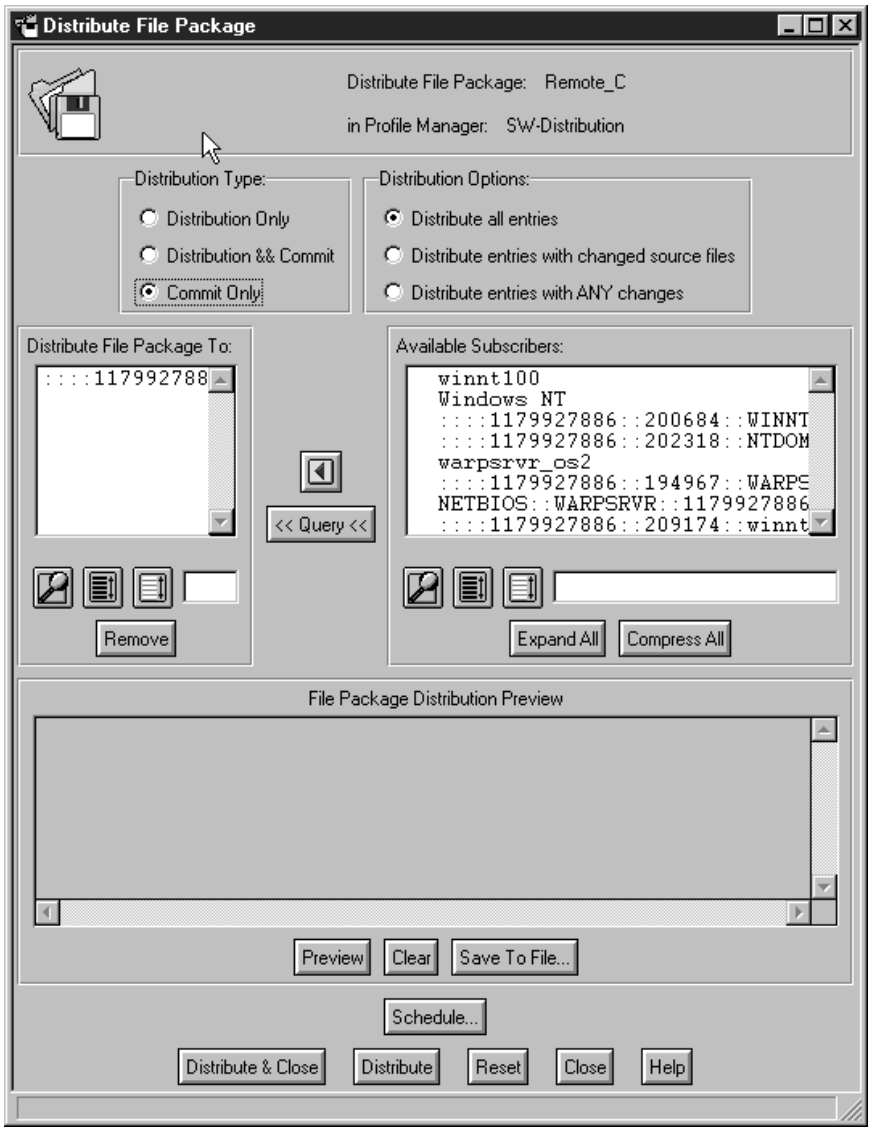


Figure 279. Start Program Using the Commit Only Option

If we take a look at the target system, we are shown that the program has been successfully started.

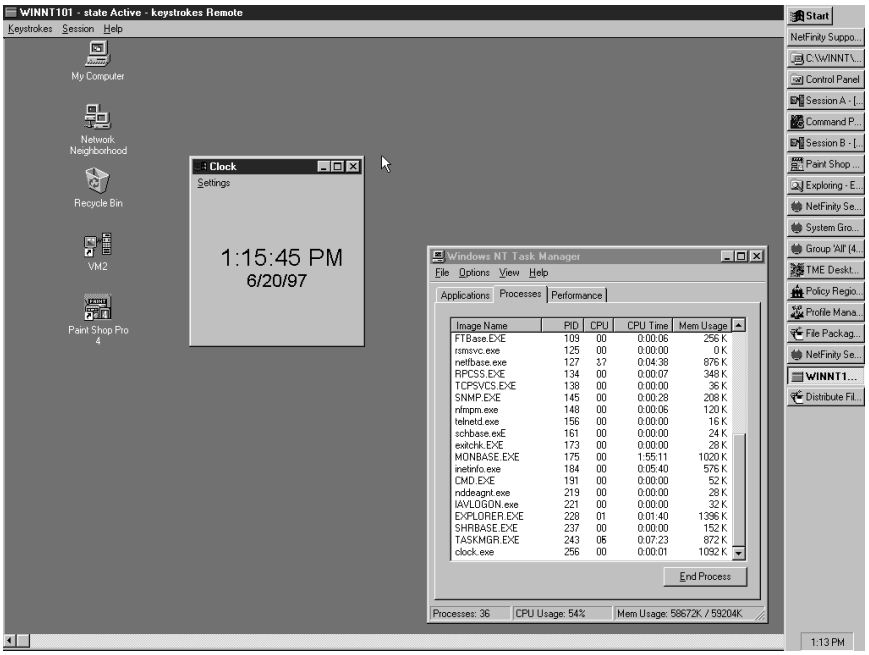


Figure 280. clock.exe Started

5.3.1 Restrictions on Using Tivoli Software Distribution

The following restrictions apply to Tivoli Software Distribution profile options when targeted at supported LAN clients:

- The AutoPack feature of Software Distribution Version 3.1 is not supported.
- Software Distribution to Windows 3.1, Windows 3.11, Windows for Workgroups, and Windows 95 is always mandatory. You are not prompted if you select the optional distribution object.
- The system restart and reboot options are not supported for Windows 3.1, Windows 3.11, Windows for Workgroups, Windows 95, and Windows NT.
- You cannot use drag and drop to distribute software to LAN Access objects on Windows NT. Perform the distribution from the File Package dialog, which is opened through the Context menu on the profile.
- Support for nested packages (packages within packages) is not available in this release.

5.4 Preparing for Inventory

Before installing Inventory make sure that a database is installed and an RDBMS server is configured. The following is an example of how to configure the Sybase database. Make sure that the database has been started by clicking on **Start/Continue** in the Sybase - Service Manager window.

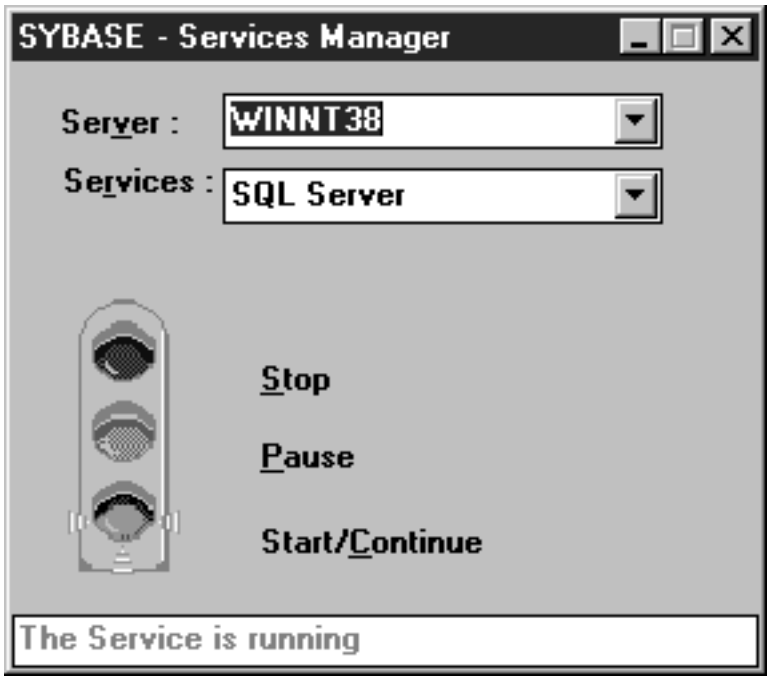


Figure 281. Start Sybase

You can use the SYBPING command to ping the database server for verifying that the database is running.

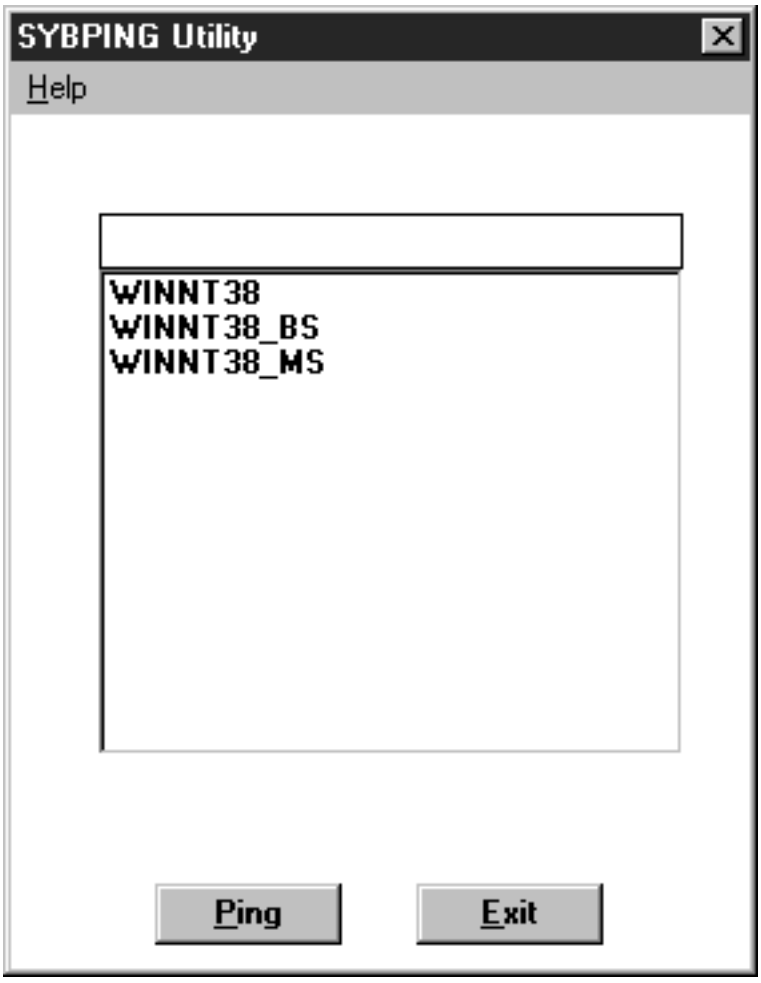


Figure 282. Sybase Ping Utility

If the ping was successful, the following panel will appear:

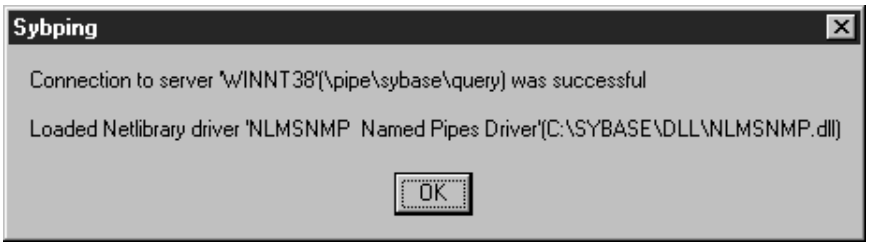


Figure 283. Sybping

If you select Sybase as your database, then there are two scripts that will need to be executed. These scripts are provided with the Tivoli Framework and are located in the $BINDIR/TAS/RIM/SQL/scripts directory on the TMR server.

Copy the tivoli_syb_admin.sql script from the above-mentioned directory on the TMR server to another directory where you want to create the database on the RDBMS server. A copy of the script follows:

```
use master
go

create database inventory on master
go

alter database inventory on master = 20
go

sp_dboption "inventory", "trunc. log on chkpt.", true
go

sp_addlogin tivoli, tivoli, inventory
go

use inventory
go

sp_adduser tivoli
go

grant create table to tivoli
go
grant create view to tivoli
go

quit
```

Figure 284. tivoli_syb_admin.sql

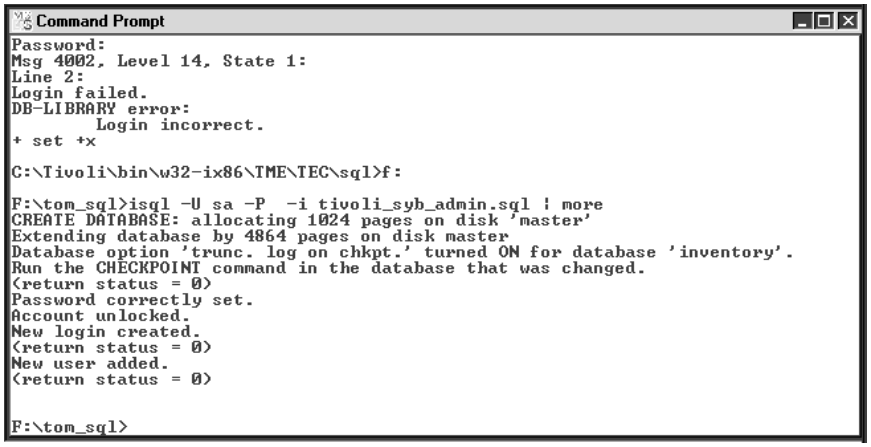


Figure 285. Creating Inventory Database

Run the script by entering the following:

- `isql -U sa -P password -i /path/tivoli_syb_admin.sql`

This script creates the tivoli user ID (with the tivoli password) and the inventory database.

To create the database schema run the tivoli_syb_schema.sql script, which creates the database schema on the RDBMS server. Note that the schema must be installed by the user tivoli. The command is as follows:

- `isql -U tivoli -P tivoli -i /path/tivoli_syb_schema.sql`

The script adds the database schema to RDBMS.

Note: Make sure that the Tivoli environment variable is set.

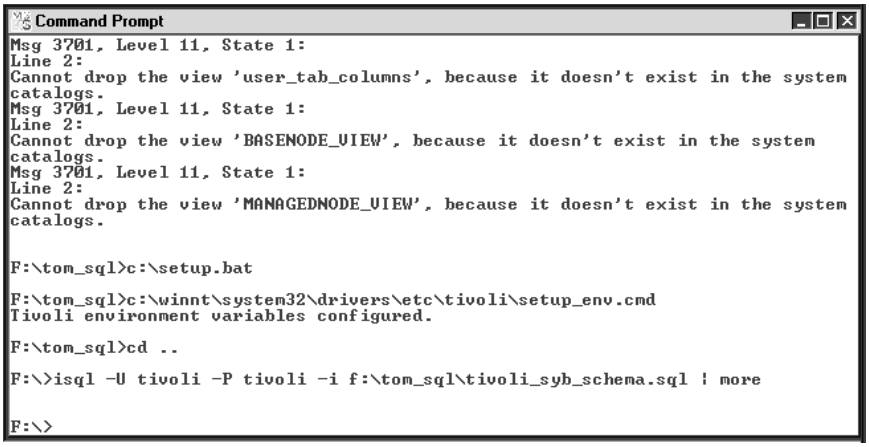


Figure 286. Create Database Schema

After that, check the database connection by entering the following:

- `isql -U tivoli -P password`
- `select * from INVENTORYDATA`
- `go`

The results from these commands should indicate that zero rows were found (instead of a message indicating that INVENTORYDATA is unknown). This test also verifies that the inventory database was created.

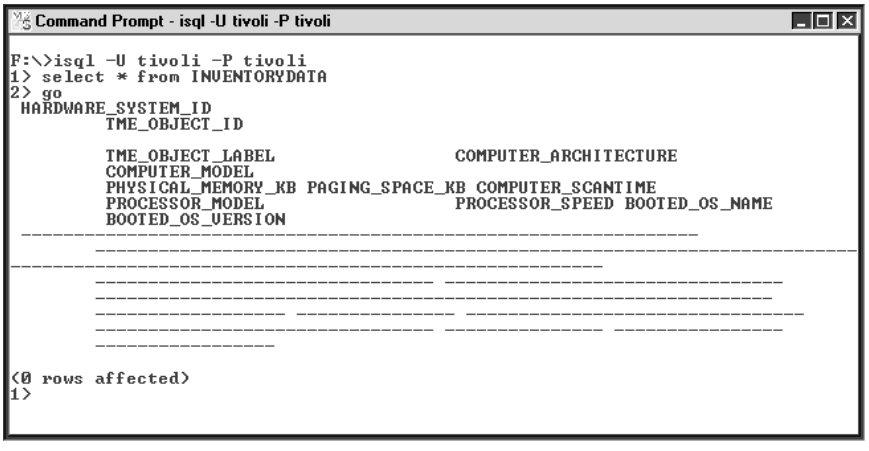


Figure 287. Check Database Connection

5.4.1 Configure Inventory

From the Inventory Profile icon menu, select **Customize...** to display the Customize Inventory Retrieval dialog.

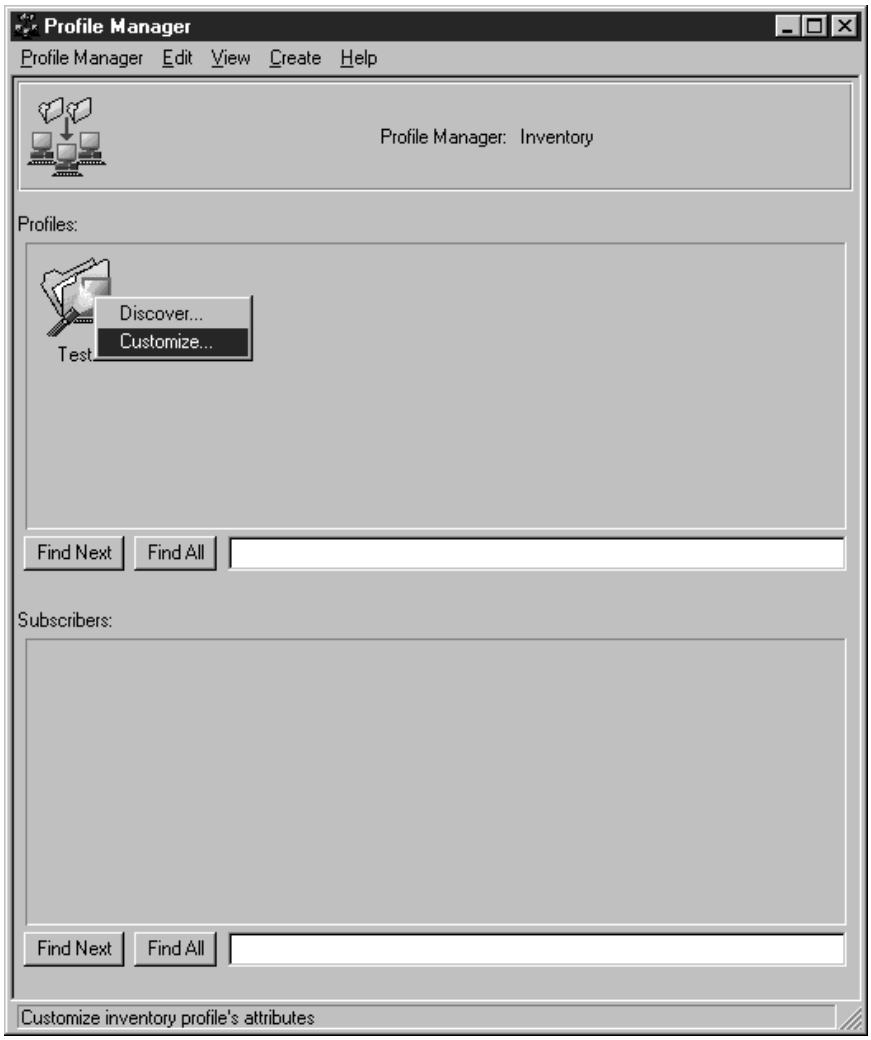


Figure 288. Start Customize Inventory Profile

The Customize Inventory Retrieval dialog lists the scanning instructions for the selected Inventory profile. The option settings displayed in this dialog are the default settings.

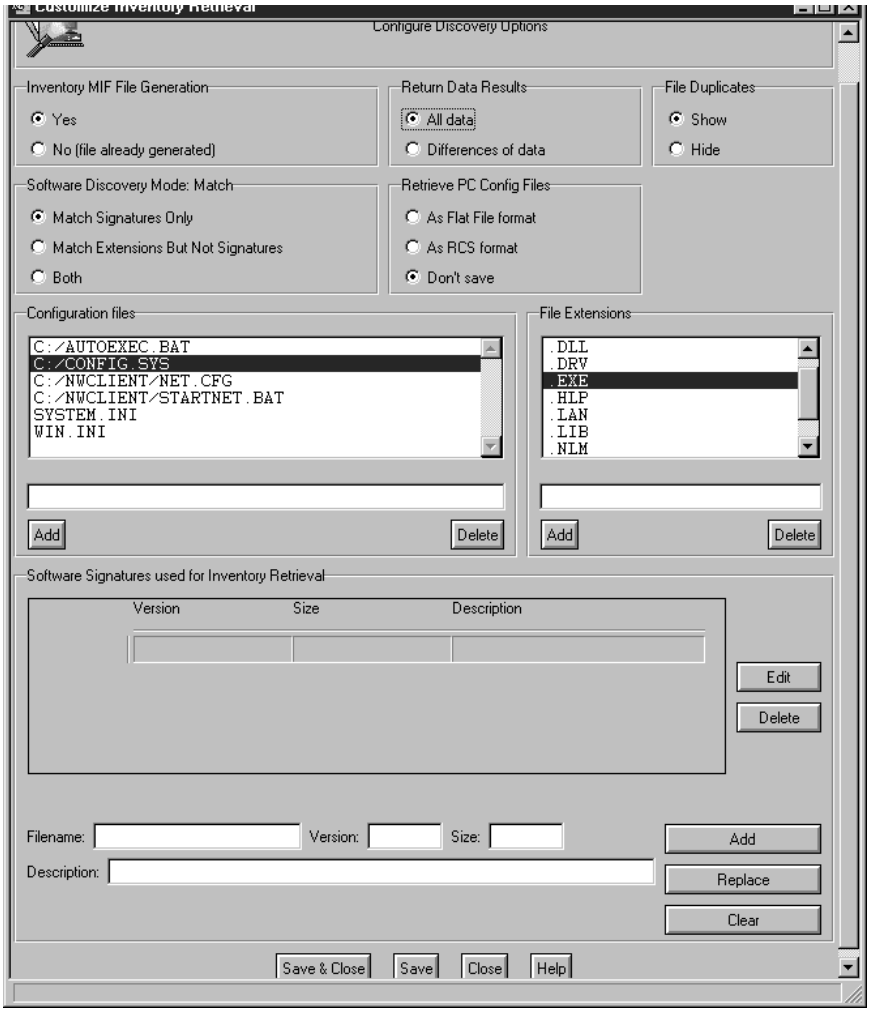


Figure 289. Customize Inventory Retrieval

The fields that we filled in for the Inventory Retrieval window are listed below. Not every option is required for Tivoli LAN Access.

- Specify if you want to generate a new MIF file during the scan by clicking one of the Inventory MIF File Generation radio buttons.
- Indicate whether Inventory will return all inventory information to the database by clicking one of the Return Data Results radio buttons.
- Specify whether to monitor duplicate files that reside in different directories by clicking one of the File Duplicates radio buttons.
- Click one of the Software Discovery Mode:Match radio buttons to monitor file extensions and file signatures on PC endpoints.
- Set up to retrieve configuration files by selecting one of the Retrieve PC Config Files radio buttons.
- List the configuration files to monitor and save, if applicable, in the Configuration Files scrolling list.
- List the file extensions that Inventory must monitor in the File Extensions scrolling list.

- List the user-defined software signatures that Inventory should monitor in the Software Signatures used for Inventory Retrieval list. Inventory adds the signatures to the useradd.ini file. Add new signatures to track an application that was developed in-house or that is not currently supported by the Inventory.
- Save the software scanning instructions specified in this dialog by clicking the **Save & Close** button.

5.4.2 Setting the Inventory Profile Subscribers in Tivoli LAN Access

To subscribe to a profile manager, drag and drop the respective icon onto the icon of the profile manager that contains the Inventory profile. Or, from the profile manager, select **Subscribers...** from the Profile Manager menu.

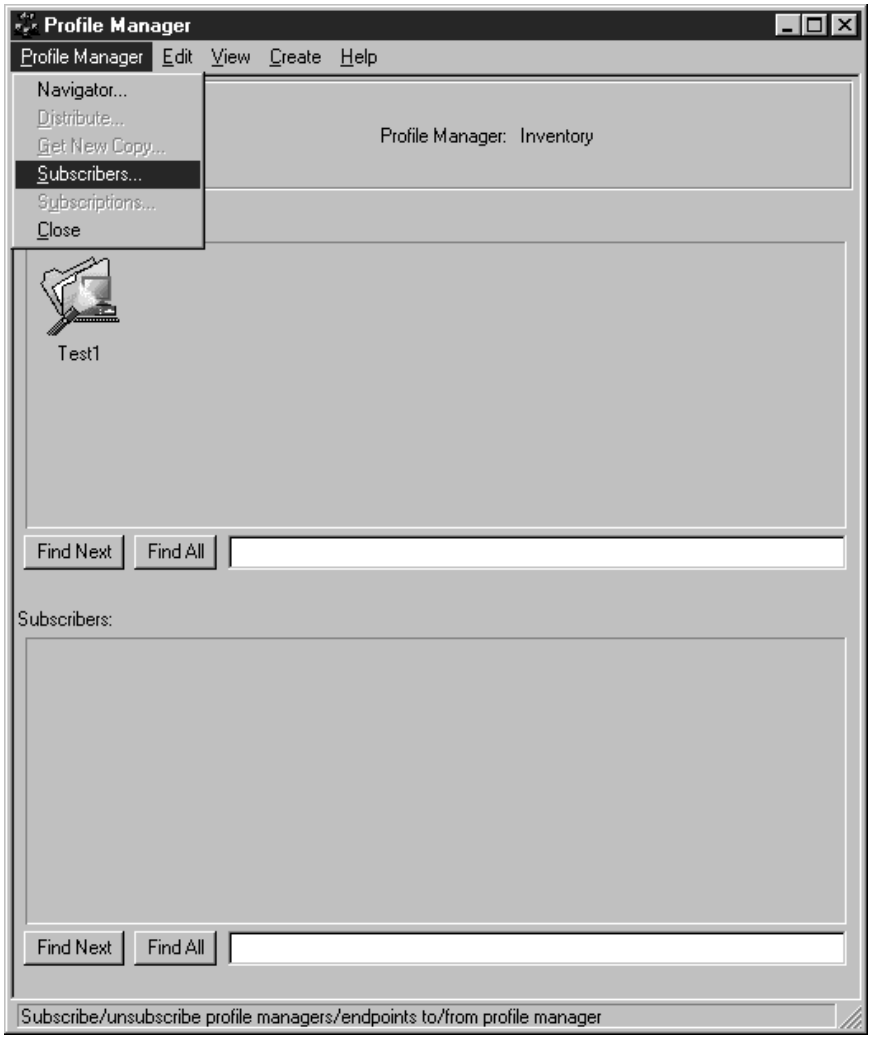


Figure 290. Start Add Subscribers to Profile Manager

In the Available to become Subscriber window pane, you see all resources that are available for distribution:

Profile Managers:

– SW-Distribution

Managed_Nodes:

– winnt38

- winnt100
- ntdomc

LAN Access Sites:

- All providers
- ITSO-Raleigh-Tom
- warpsrvr-os2
- winnt100_ip

LAN Access Collections:

- All
- OS/2
- OS/2-Workstation
- Windows NT
- Windows
- Test

All LAN Access Clients

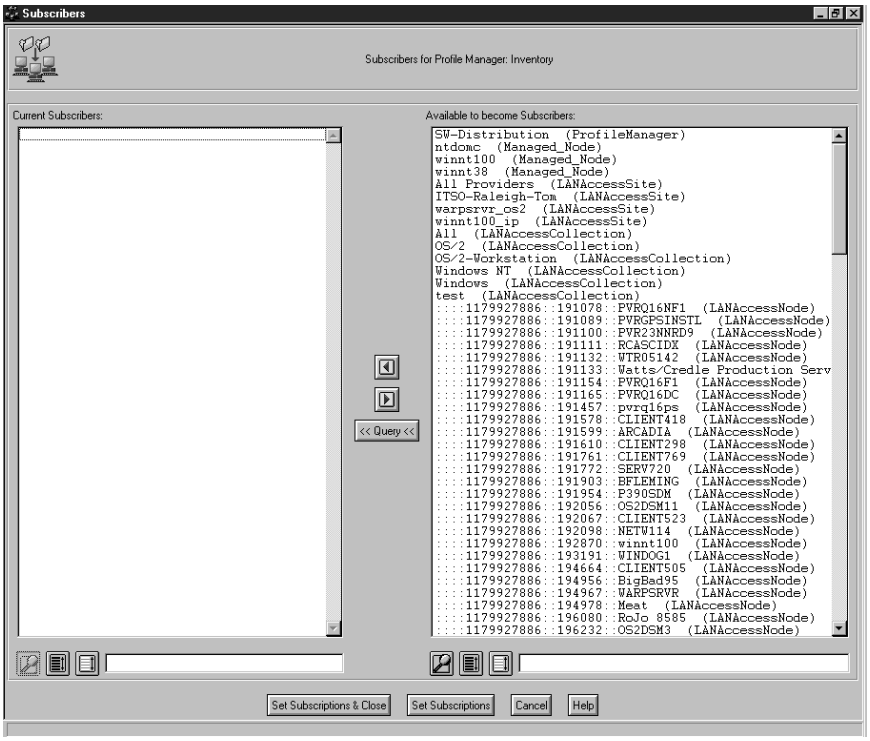


Figure 291. Available Subscribers

Select a subscriber from the Available Targets scrolling list and click the left button to move the subscriber to the Selected Targets scrolling list.

In this case we had already selected the client node winnt101. The highlighted clients are added by clicking on the left arrow.

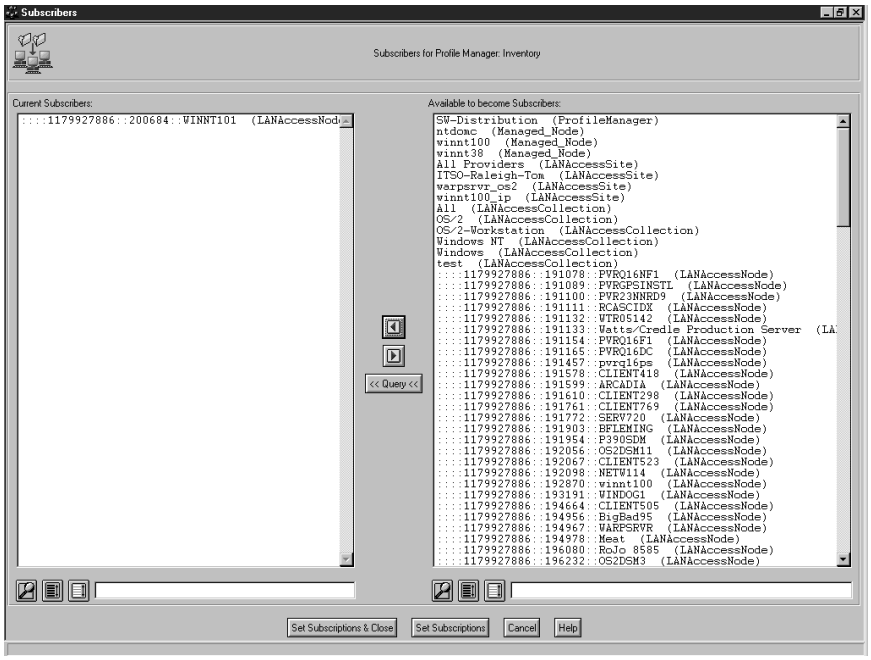


Figure 292. Adding Clients to the Current Subscribers Field

Three more LAN Access clients were added to the current subscriber list:

1. WARPSRVR
2. winnt100
3. NTDOMC

Click the **Set Subscriptions & Close** button to set the new subscriptions and return to the Profile Manager window.

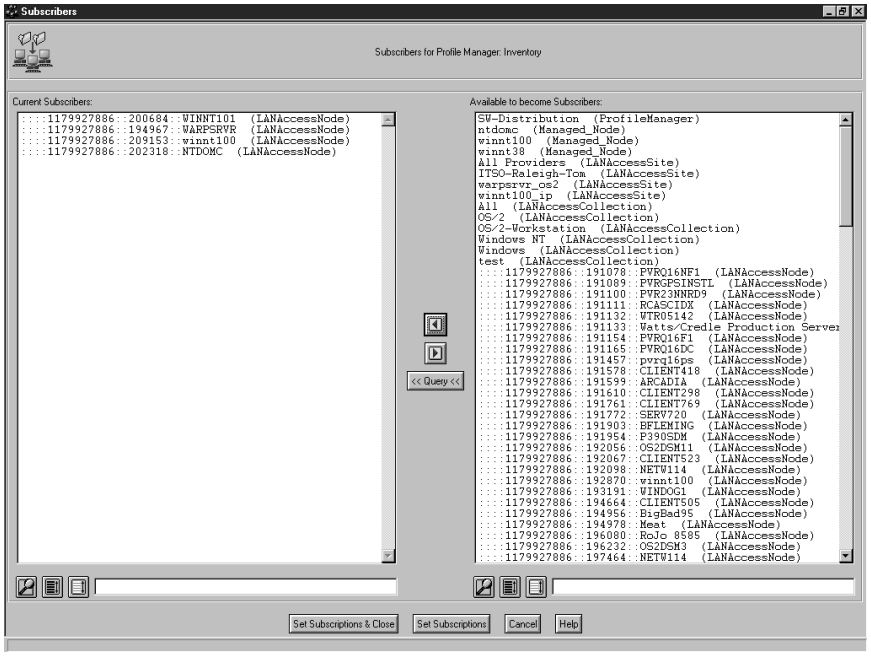


Figure 293. Subscribers

The new subscribers are added to the profile manager's list of subscribers.

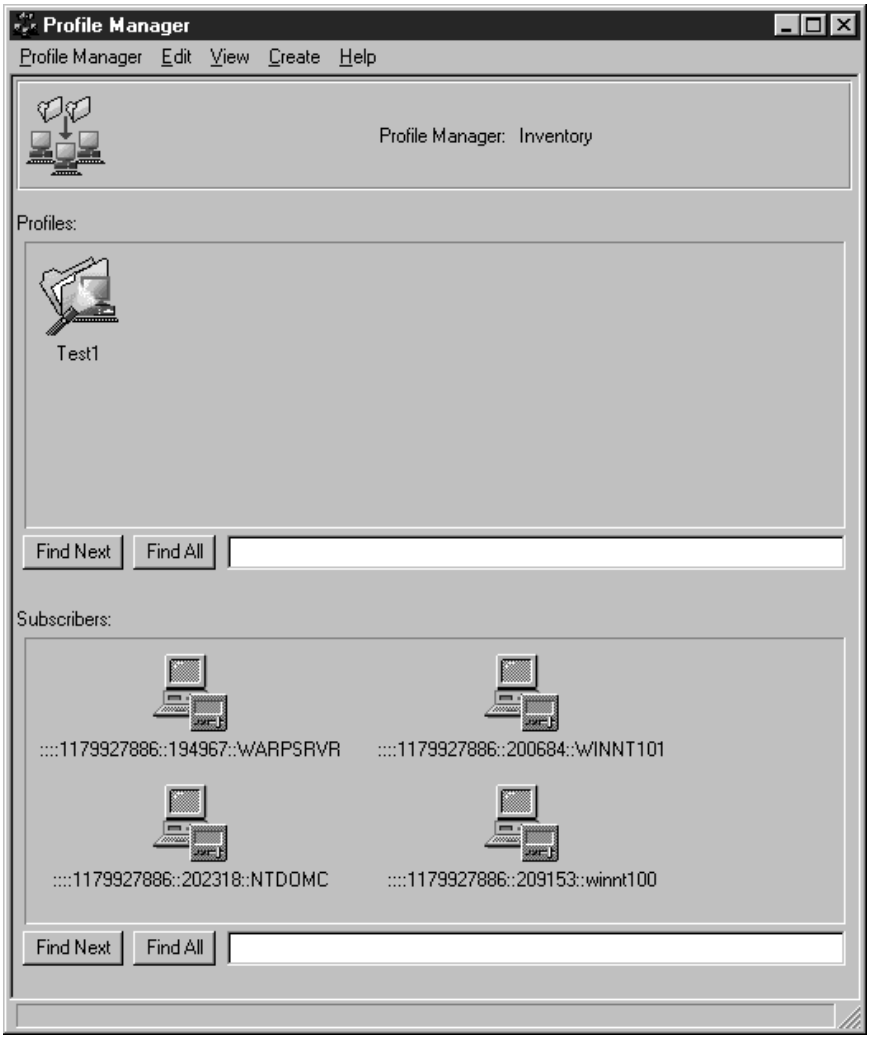


Figure 294. Profile Manager with New Subscribers

5.4.2.1 Distributing an Inventory Profile to a LAN Access Client

In the Inventory profile manager, double-click on an Inventory profile to display the Inventory Profile dialog.

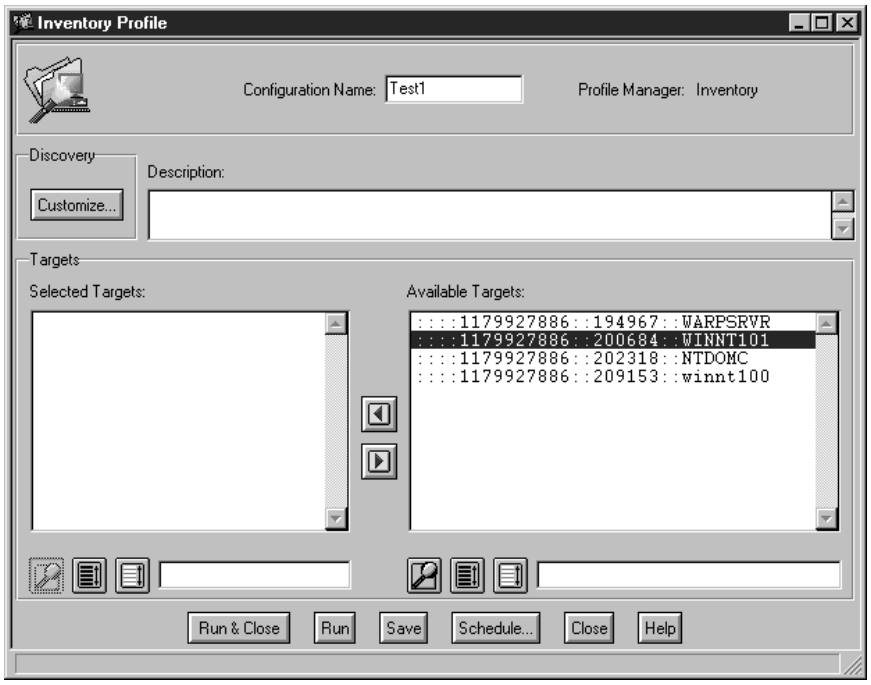


Figure 295. Inventory Profile Dialog

Select the LAN Access clients from the Available Targets scroll list. Click the left button to move the clients to the Selected Targets scroll list. These machines will be scanned for hardware and PC software information using the scan tool from the LAN management tool you are using.

Click the **Run & Close** button to begin a scan on the selected subscribers and return to the Inventory Profile dialog. The Inventory Profile dialog is not completed until the scan is complete on each subscriber. If the scan fails for any of the subscribers, a pop-up window is displayed to inform you which subscribers failed.

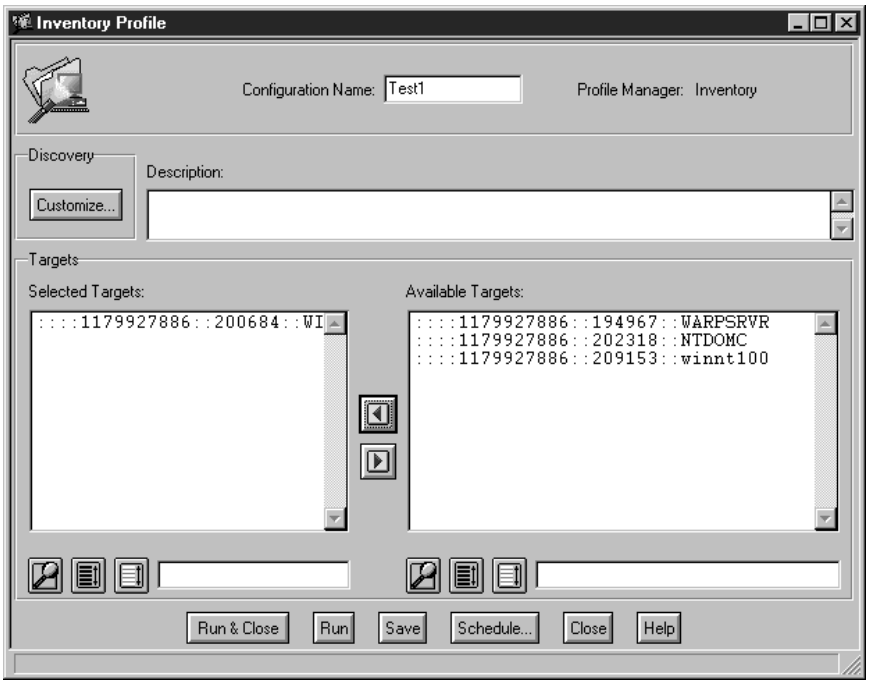


Figure 296. Build Inventory Profile - Start Scan

5.4.2.2 Creating a Query Library

To create a query library, you need to first add the QueryLibrary resource to the policy region.

From the policy region, select **QueryLibrary...** from the Create menu. Enter a name for the query library in the Name/Icon Label field.

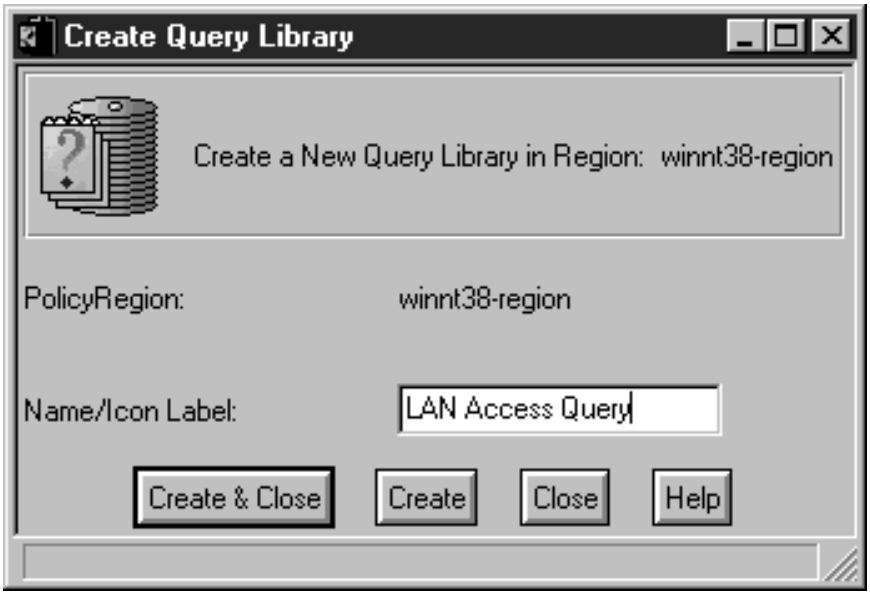


Figure 297. Create Query Library

Click the **Create & Close** button. This creates the query library and returns you to the Policy Region window.

Double-click on the query library icon to display the query library window.

Figure 298. Policy Region with New Query Library

Select **Query** from the Create menu to display the Create Query dialog.

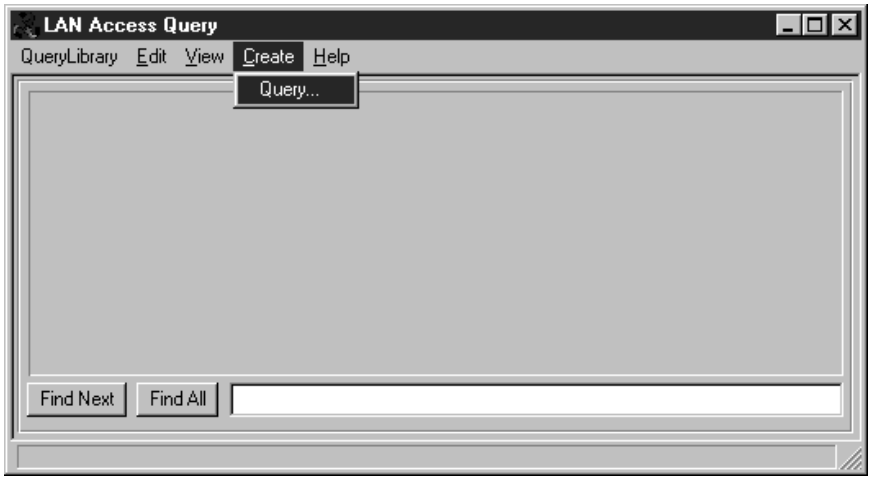


Figure 299. Create Query

- Enter a name for the query in the Query Name field.
- Enter a brief description of the query in the Description field.
- Add properties to the query in the Where Clause section of the dialog by creating an SQL search clause.
- Click the **Create & Close** button to create the query and return to the query library window.

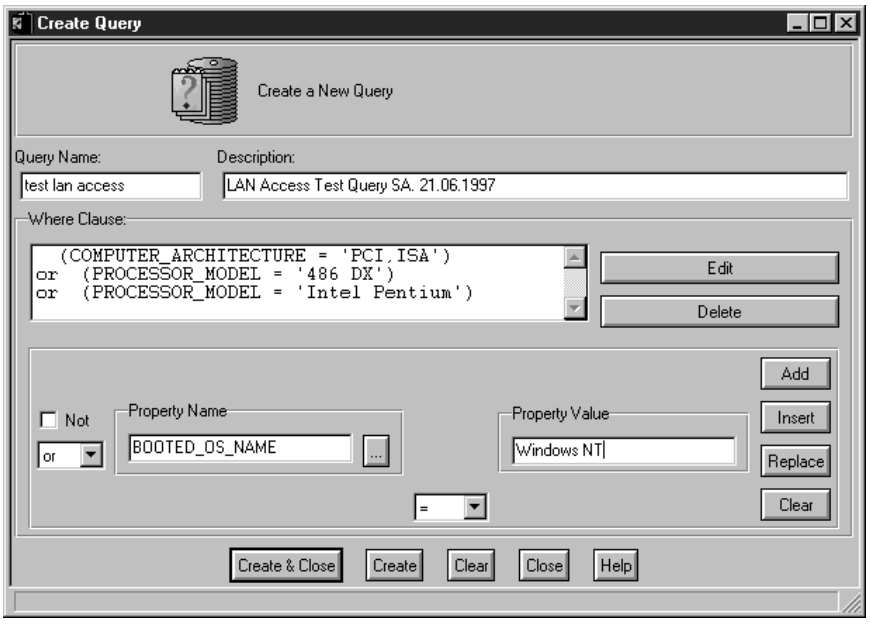


Figure 300. Create Query Dialog

5.4.2.3 Querying the Database

From the Profile Manager window, select **Subscribers..** to display the Subscribers dialog.

Click the **Query** button to display the Execute a Query dialog.

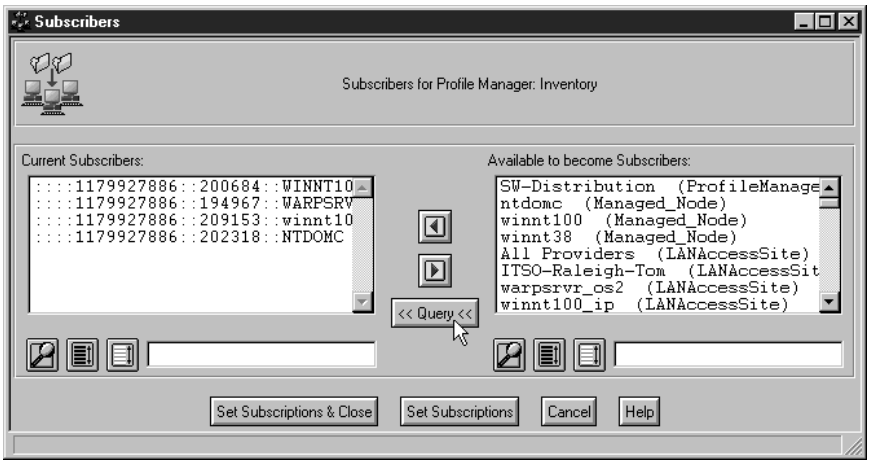


Figure 301. Start Query

Select the query library that contains the query from the Query Libraries scrolling list.

Select the query from the Queries scroll list.

Click the **Execute** button. The framework queries the database according to what was specified in the Where Clause box and returns the names of the systems that meet the query.

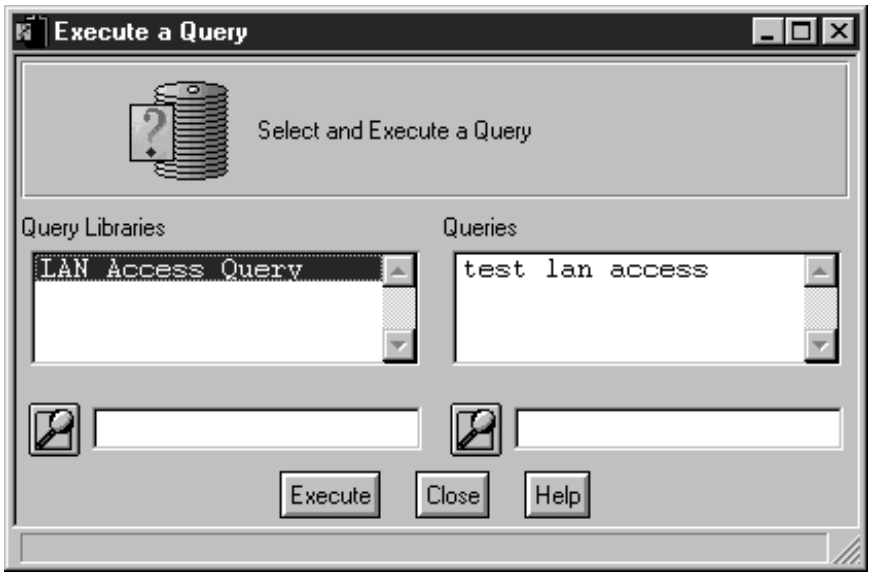


Figure 302. Execute a Query

5.4.3 Restrictions on Using Tivoli Inventory

The following restrictions apply to Tivoli Inventory profile options for LAN resources accessed through an MPM provider:

- Inventory MIF File Generation
  - MIF files are not used by LAN Access.

    When you select Yes, LAN Access instructs MPM providers to refresh inventory database information (if the provider supports the refresh command). Following the refresh, LAN Access reads the inventory information from the provider.

    When you select No, LAN Access reads the inventory information from the provider without a refresh.
- Return Data Results
  - Select the **All data** option only. The Differences of data option can return unpredictable results.
- File Duplicates
  - This option is not supported by LAN Access because the MPM specification does not include information about duplicates.
- Software Discovery Mode Match
  - This option is not supported by LAN Access because the MPM specification for software inventory is not based on matching file signatures.
- Retrieve PC Config Files
  - This option is not supported by LAN Access.

Errors that occur during the distribution of inventory profiles are posted in the LAN Access notice group.

5.4.4 Configuring the TEC Event Server

During LAN Access installation several files that are needed to configure the TEC event server for use with LAN Access are copied to the NT managed node and the TMR server.

Next we are going to show how to configure TEC to enable it to receive alerts sent from the LAN Access event adapter using the graphical interface (GUI). This can also be done using the command line interface (CLI). This way is described in 1.9, “Importing LAN Access Event Classes” on page 64 as well as in the *LAN Access User's Guide*.

Edit the context menu of the EventServer icon in the Tivoli desktop and choose the option **Rules Bases...**

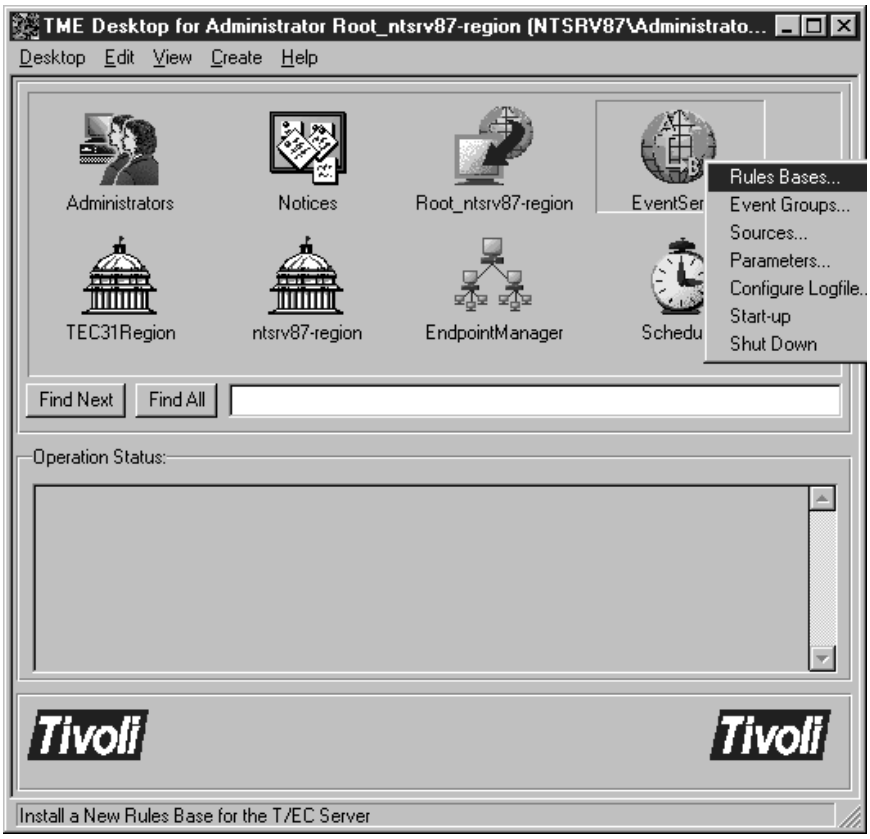


Figure 303. Edit Rule Bases

Select **Create Rule Base...**. If you still only have the default rule, you will have to create a new rule base since the default rule cannot be modified.

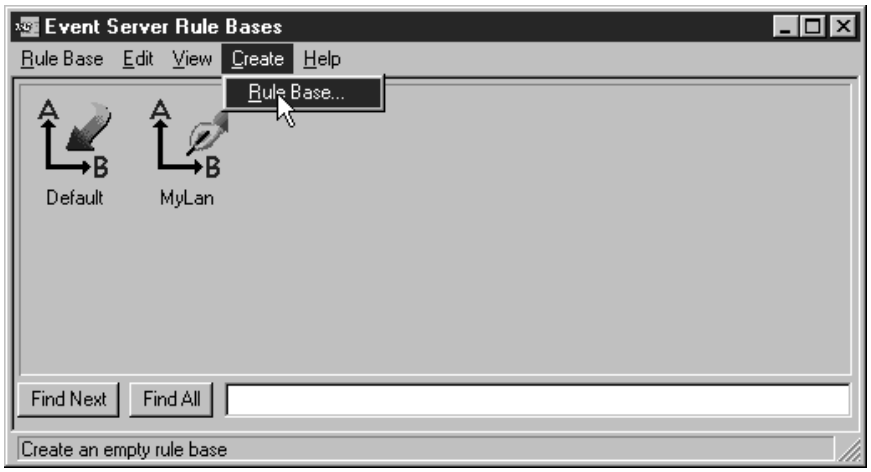


Figure 304. Event Server Rules Bases Window

Enter a name for the new rule base and the directory where you want to create it, including the complete path. If the directory does not yet exist, it will be created for you.

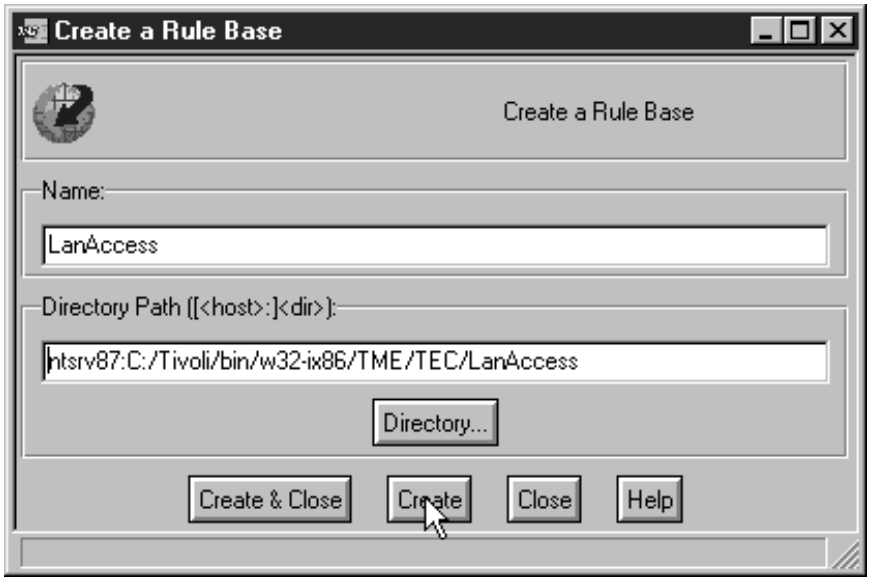


Figure 305. Creation of Rule Base

Copy the contents of the default rule to the newly created rule base. This process is shown in the next two figures. First you have to select the option **Copy...** from the Context menu of the default rule base icon in the Event Server Rules Bases window.

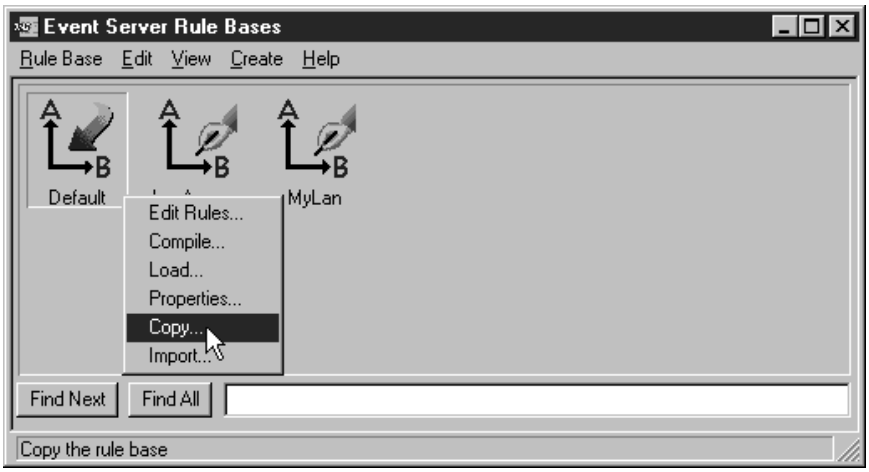


Figure 306. Copying Default Rule Base

In the Copy Rule Base window select the rule base you just created as the Destination rule base and check the boxes **Copy rules** and **Copy classes**.

Click on **Copy & Close**.

Figure 307. Copying Default Rule Base

Now you have to import the LAN Access event class files to the new rule base. To do so, select **Import...** from the Context menu of the appropriate rule base icon in the Event Server Rules Bases window.

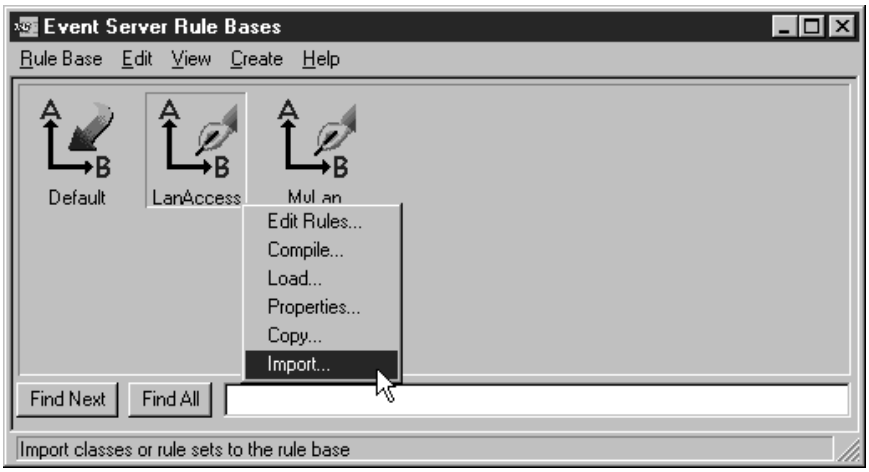


Figure 308. Importing LAN Access Event Class Files

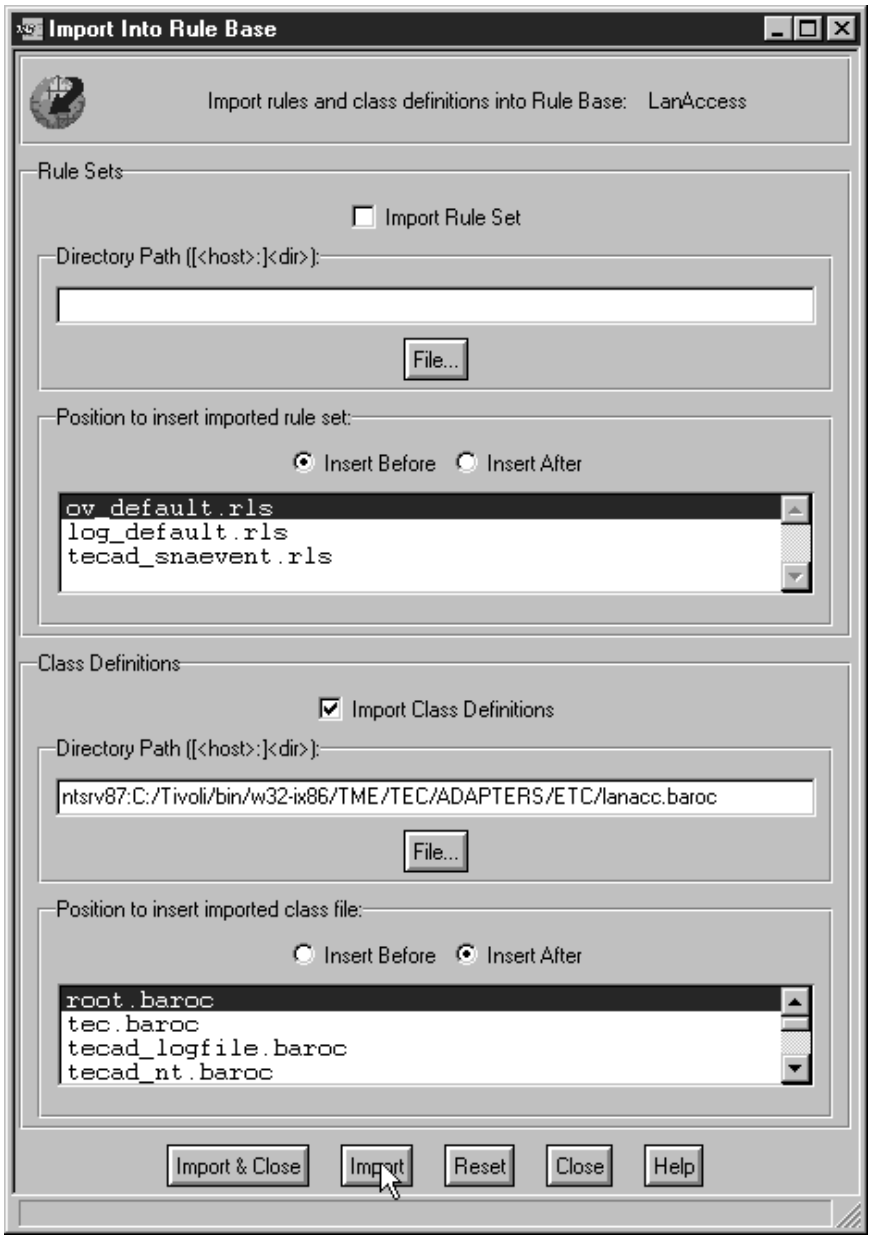


Figure 309. Importing lanacc.baroc File

We need to import the files lanacc.baroc and la_sms.baroc. You must first import the lanacc.baroc and insert it after the root.baroc file as shown in Figure 309.

Then import the la_sms.baroc file and insert it after lanacc.baroc as shown in Figure 310 on page 255.

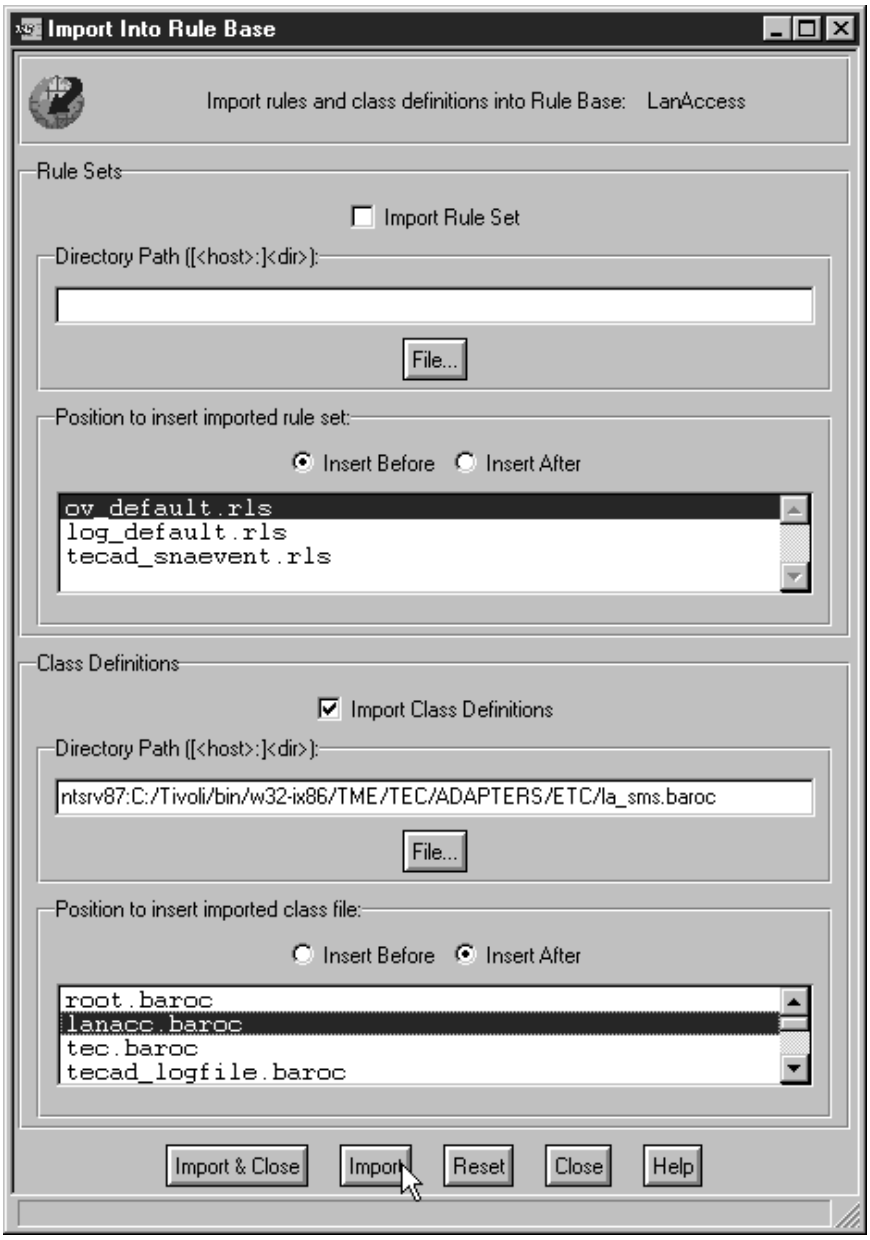


Figure 310. Importing la_sms.baroc File

The next thing to do is to compile the rule base. To do this select **Compile...** from the rule's Context menu.

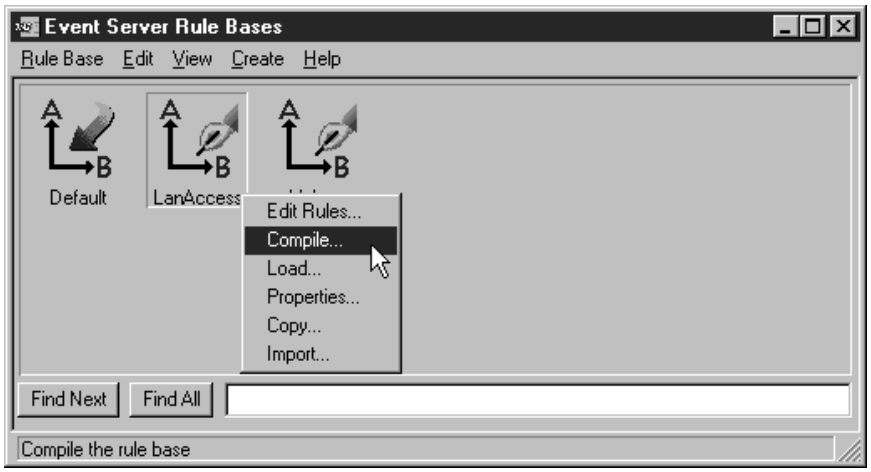


Figure 311. Compiling Rule Base

You can check the box **Trace rules** to have a record of the compilation before clicking on **Compile**. When the compilation is done, click on **Close** to exit.

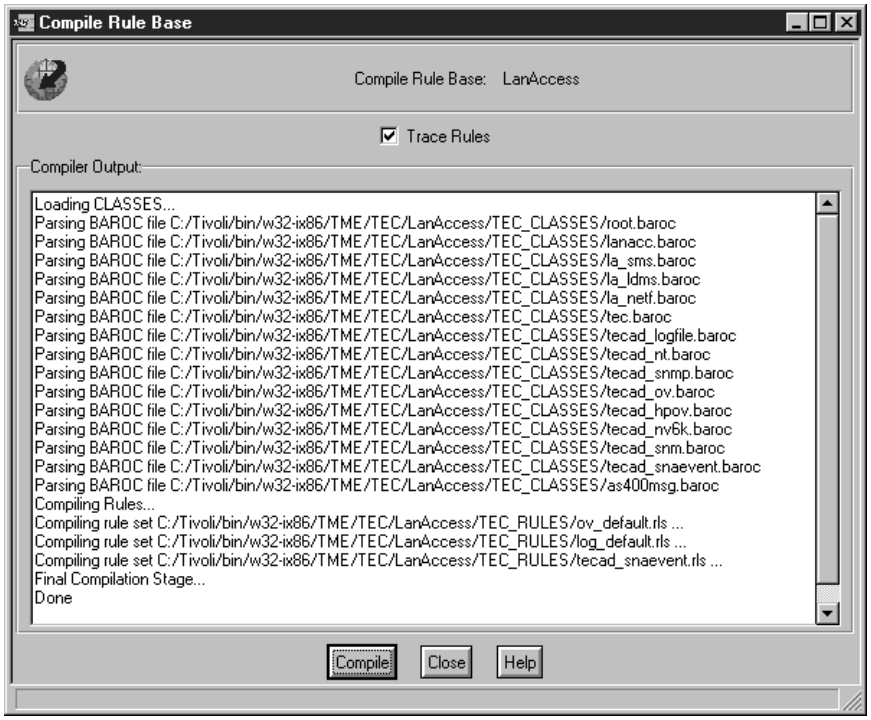


Figure 312. Compile Rule Base Window

Finally, you have to load and activate the new rule base to make the TEC event adapter work with it.

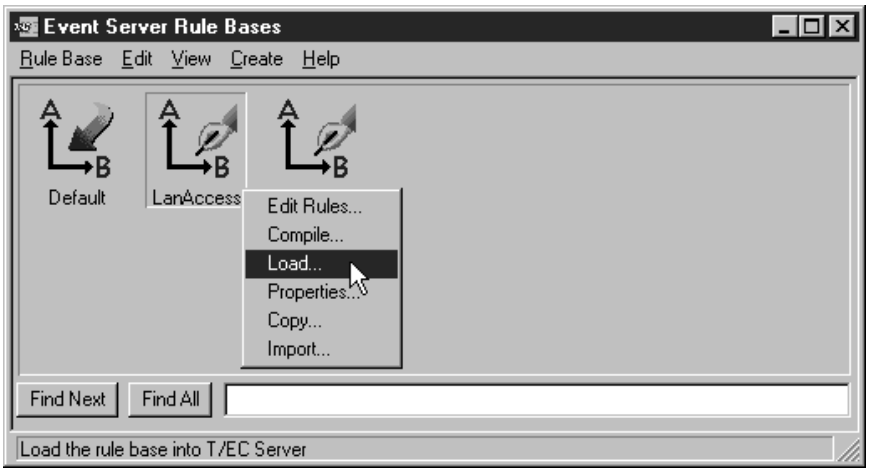


Figure 313. Loading the Rule Base

Select either of the two options in the next window and click on **Load & Close**.

Figure 314. Load Rule Base Window

If you choose the option Load and activate the rule base you should see the red arrow appear on the new rule. The rule with the red arrow is the actual active rule on the TEC event server. If you choose the other option, you would have to restart the event server for the change to take effect. This can either be done on the Tivoli desktop or through the command line interface. The commands are:

- wstopesvr
- wstartesvr

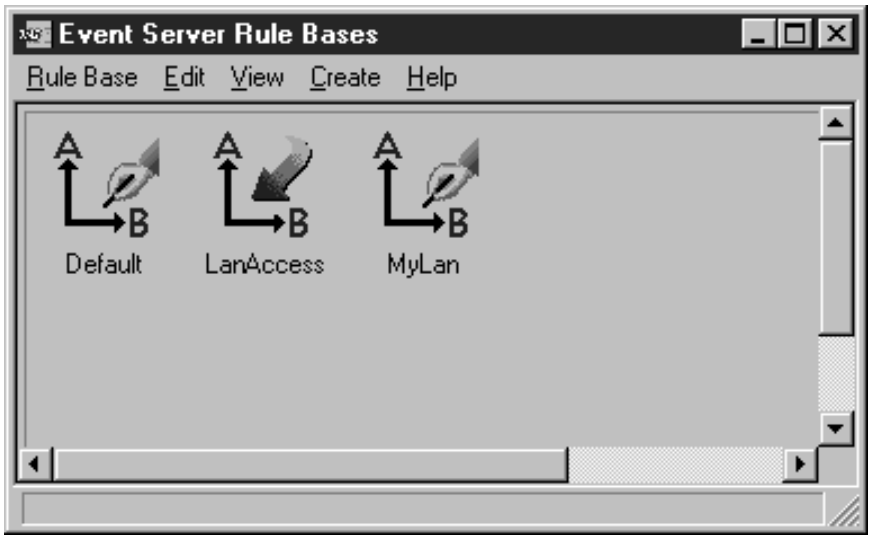


Figure 315. Event Server Rules Bases Window

Appendix A. Configuration Files

The following BAROC files are shipped with Tivoli LAN Access:

A.1 LA_LDMS.BAROC

A copy of the event adapter for the Intel LANDesk code follows:

```
#*********************************************************************
#  Tivoli Event Classes for Management Services Broker
#  Date:        Feb  27, 1997
#  Version:     Version 0.1
#
#  Copyright (c) 1996, Tivoli Systems, Inc.  All rights reserved.
#   Licensed Materials - Property of Tivoli Systems
#
# LA_LDMS.baroc - TME 10 LAN Access event classes for
#                 the LanDesk Management Suite V2.51 MPM Provider
#*********************************************************************
# LanDesk Management Suite V2.51 Alerts
#*********************************************************************
TEC_CLASS :
        LDMSV251_EVENT ISA PROVIDER_EVENT
        DEFINES {
            origin:                                 default = "MPM Provider for Intel LANDesk";
            architecture_code:                      default = "IntelAMSV1";
            name:                   STRING;
            description:            STRING;
            location:               STRING;
            alert_id:               INTEGER;
            application_name:       STRING;
            alert_server:           STRING;
            contact_person:         STRING;
            building_name:          STRING;
            room_number:            STRING;
            street_address:         STRING;
            city:                   STRING;
            state:                  STRING;
            zip:                    STRING;
            phone_number:           STRING;
            contact:                STRING;
            current_time:           STRING;
            database_name:          STRING;
            component:              STRING;
            event_name:             STRING;
            solution:               STRING;
            system:                 STRING;
            subsystem:              STRING;
            group:                  STRING;
            message:                STRING;
            data:                   STRING;
            statekey:               STRING;
            alert_origin:           STRING;
            product_id:             STRING;
            device_id:              STRING;
            alias:                  STRING;
            app_code_version:       STRING;
            rbl_version:            STRING;
            rom_version:            STRING;
            network_type:           STRING;
            up_time:                STRING;
            server_name:            STRING;
            user_name:              STRING;
            file_name:              STRING;
            node_address:           STRING;
            generic_name:           STRING;
            generic_description:    STRING;
            generic_location:       STRING;
            ethernet_address:       STRING;
            ipx_address:            STRING;
            ip_address:             STRING;
            token_ring_address:     STRING;
            appication_data:        STRING;
            date_and_time:          STRING;

        };
END
```

Figure 316 (Part 1 of 4). Event Class for LANDesk Management Suite V2.51 MPM Provider

```
TEC_CLASS :

        LDMS_25_LINE_MESSAGE ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "Alert Converter.25 Line Message";
        };
END

TEC_CLASS :

        LDMS_ALERTS_FROM_ASP_CLIENTS ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "Alert Converter.Alerts from ASP Clients";
        };
END

TEC_CLASS :

        LDMS_PRINT_STATUS_ALERTS ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "Alert Converter.Print Status Alerts";
        };
END

TEC_CLASS :

        LDMS_LDISCAN ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "Alert Converter.LDIScan";
        };
END

TEC_CLASS :

        LDMS_VIRUS_FOUND ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "Alert Converter.Virus Found";
        };
END
TEC_CLASS :

        LDMS_USER-DEFINED_TEST_ALERT ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "Alert Converter.User-defined Test Alert";
        };
END

TEC_CLASS :

        LDMS_METER_NLM_IS_LOADED ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "LDMETER.Meter NLM is loaded";
        };
END
TEC_CLASS :

        LDMS_SERVER_MANAGER-AMS_ALERT_FAILURE ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "LNADesk Server Manager.Server Manager-AMS alert failure";
        };
END
```

Figure 316 (Part 2 of 4). Event Class for LANDesk Management Suite V2.51 MPM Provider

```
TEC_CLASS :

        LDMS_APPLICATION_IS_DELETED_FROM_METERED_LIST ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "LDMETER.Application is deleted from Metered List";
        };
END

TEC_CLASS :

        LDMS_METER_NLM_IS_UNLOADED ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "LDMETER.Meter NLM is unloaded";
        };
END

TEC_CLASS :

        LDMS_RELAY_NLM_IS_UNLOADED ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "LDMETER.Relay NLM is unloaded";
        };
END

TEC_CLASS :

        LDMS_INVENTORY_CHANGED ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "Desktop Manager.Inventory Changed";
        };
END
TEC_CLASS :

        LDMS_SERVER_MANAGER-OUT_OF_BAND_ALERT ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "LANDesk Server Manager.Server Manager-out of band alert";
        };
END
TEC_CLASS :

        LDMS_DISTRIBUTE_STATUS ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "Distribute Console.Distribute Status";
        };
END

TEC_CLASS :

        LDMS_PRINTER_READY ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "Printer Manager.Printer Ready";
        };
END
```

Figure 316 (Part 3 of 4). Event Class for LANDesk Management Suite V2.51 MPM Provider

```
TEC_CLASS :

        LDMS_PRINTER_PRINTING ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "Printer Manager.Printer Printing";
        };
END

TEC_CLASS :

        LDMS_PRINTER_OFFLINE ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "Printer Manager.Printer Offline";
        };
END

TEC_CLASS :

        LDMS_PRINTER_OUT_OF_PAPER ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "Printer Manager.Printer Out of Paper";
        };
END
TEC_CLASS :

        LDMS_PRINTER_ERROR ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "Printer Manager.Printer Error";
        };
END
TEC_CLASS :

        LDMS_PRINTER_WAITING_FOR_FORM ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "Printer Manager.Printer Waiting for Form";
        };
END

TEC_CLASS :

        LDMS_PRINTER_NOT_CONNECTED ISA LDMSV251_EVENT
        DEFINES {
            unique_id:                          default = "Printer Manager.Printer Not Connected";
        };
END

# Generic event class for non-predicated alerts

TEC_CLASS :

        INTELAMSV1_EVENT ISA LDMSV251_EVENT
        DEFINES {
        };
END
```

Figure 316 (Part 4 of 4). Event Class for LANDesk Management Suite V2.51 MPM Provider

A.2 LA_NETF.BAROC

A copy of the event adapter for the IBM Netfinity code follows:

```
#*********************************************************************
#
#  Tivoli Event Classes for Management Services Broker
#
#  Date:        Feb  27, 1997
#  Version:     Version 0.1
#
#  Copyright (c) 1996, Tivoli Systems, Inc.  All rights reserved.
#   Licensed Materials - Property of Tivoli Systems
#
# Netfinity.baroc - TME 10 LAN Access event class for
#                   the NetFinity MPM Provider
#
#
#*********************************************************************
#
# NetFinity Alerts
#
#*********************************************************************

TEC_CLASS :
        NETFIN_EVENT ISA PROVIDER_EVENT
        DEFINES {
            origin:                                     default = "MPM Provider for IBM NetFinity";
            architecture_code:                          default = "NETFINITY";
            alert_text:             STRING;
            standard_alert_type:    STRING;
            application_id:         STRING;
            application_alert_type: INT32;
            time_and_date:          STRING;
            system_name:            STRING;
            sender_path:            STRING;
            system_unique_id:       STRING;
            appication_data:        STRING;
            p1:                     STRING;
            p2:                     STRING;
            p3:                     STRING;
            p4:                     STRING;
            p5:                     STRING;
            p6:                     STRING;
            p7:                     STRING;
            p8:                     STRING;
            p9:                     STRING;
            p10:                    STRING;
        };
END
```

Figure 317 (Part 1 of 4). Event Class for Netfinity MPM Provider

```
TEC_CLASS :

        NF_POED_ERROR_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "POED.0201";
        };
END

TEC_CLASS :

        NF_POED_INFO_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "POED.0200";
        };
END

TEC_CLASS :

        NF_PFA_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "PFA.0000";
        };
END

TEC_CLASS :

        NF_FILE_CHANGED_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "MonCritF.0000";
        };
END

TEC_CLASS :

        NF_FILE_DELETED_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "MonCritF.0001";
        };
END

TEC_CLASS :

        NF_FILE_CREATED_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "MonCritF.0002";
        };
END

TEC_CLASS :

        NF_PROCESS_TERM_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "ProcMgr.0901";
        };
END

TEC_CLASS :

        NF_PROCESS_START_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "ProcMgr.0900";
        };
END

TEC_CLASS :

        NF_PROCESS_NOT_START_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "ProcMgr.0902";
        };
END
```

Figure 317 (Part 2 of 4). Event Class for Netfinity MPM Provider

```
TEC_CLASS :

        NF_SYS_ONLINE_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "NetMgr.000A";
        };
END

TEC_CLASS :

        NF_SYS_OFFLINE_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "NetMgr.000B";
        };
END

TEC_CLASS :

        NF_ACCESS_GRANT_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "SecMgr.0014";
        };
END

TEC_CLASS :

        NF_PUBLIC_ACCESS_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "SecMgr.0015";
        };
END

TEC_CLASS :

        NF_ACCESS_DENIED_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "SecMgr.0016";
        };
END

TEC_CLASS :

        NF_RESTART_INIT_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "SecMgr.0041";
        };
END

TEC_CLASS :

        NF_RESTART_REJECT_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "SecMgr.0040";
        };
END

TEC_CLASS :

        NF_SERVICE_START_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "SvcMgr.0900";
        };
END
```

Figure 317 (Part 3 of 4). Event Class for Netfinity MPM Provider

```
TEC_CLASS :

        NF_SERVICE_REJECT_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "SvcMgr.0901";
        };
END

TEC_CLASS :

        NF_THRESH_ERROR_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "MonitorB.0000";
        };
END

TEC_CLASS :

        NF_THRESH_NORM_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "MonitorB.0010";
        };
END

TEC_CLASS :

        NF_PHYS_RAID_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "MonitorB.0130";
        };
END

TEC_CLASS :

        NF_LOG_RAID_ALERT ISA NETFIN_EVENT
        DEFINES {
            unique_id:                                  default = "MonitorB.0131";
        };
END


# Generic event class for non-predicated alerts

TEC_CLASS :

        NETFINITY_EVENT ISA NETFIN_EVENT
        DEFINES {
        };
END
```

Figure 317 (Part 4 of 4). Event Class for Netfinity MPM Provider

A.3 LA_SMS

We did not attach a copy of the SMS event adapter since it was very large. See the product installation CD for this.

A.4 LANACC.BAROC

A copy of the Tivoli LAN Access event classes follows:

```
#*********************************************************************
#
#  Tivoli Event Classes for Management Services Broker
#
#  Date:        Feb  27, 1997
#  Version:     Version 0.1
#
#  Copyright (c) 1996, Tivoli Systems, Inc.  All rights reserved.
#   Licensed Materials - Property of Tivoli Systems
#
# lanacc.baroc - TME 10 LAN Access event classes.
#
#
#
#*********************************************************************
TEC_CLASS :
        LAN_ACCESS_EVENT ISA EVENT
        DEFINES {
            source:                                     default = "TME 10 LAN Access";
            severity:                                   default = UNKNOWN;
            target_mpm_location:         STRING;
            hostname:                                   default = "Unknown";
        };
END

TEC_CLASS :
        LA_CONNECTION_LOST ISA LAN_ACCESS_EVENT
        DEFINES {
            msg:                                        default = "Connection to MPM location lost";
        };
END

TEC_CLASS :
        LA_CONNECTION_ESTABLISHED ISA LAN_ACCESS_EVENT
        DEFINES {
            msg:                                        default = "Connection to MPM location established";
        };
END

TEC_CLASS :
        LA_ACCESS_DENIED ISA LAN_ACCESS_EVENT
        DEFINES {
            msg:                                        default = "Access to MPM location was denied";
        };
END

TEC_CLASS :
        LA_CONNECTION_TIMED_OUT ISA LAN_ACCESS_EVENT
        DEFINES {
            msg:                                        default = "Connection to MPM location timed out";
        };
END
TEC_CLASS :
        LA_CONNECTION_FAILED ISA LAN_ACCESS_EVENT
        DEFINES {
            msg:                                        default = "Connection to MPM location failed";
        };
END

TEC_CLASS :
        PROVIDER_EVENT ISA LAN_ACCESS_EVENT
        DEFINES {
            architecture_code:           STRING;
            unique_id:                   STRING;
        };
END

# This event is for provider-based alerts that are not explicitly supported
# by the LAN_ACCESS TEC adapter's map file (ie. the architecture is not represented).

TEC_CLASS :
        GENERIC_PROVIDER_EVENT ISA PROVIDER_EVENT
        DEFINES {
        };
END
```

Figure 318. Tivoli Event Classes for Management Services Broker

A.4.1 readme File

The readme file follows:

```
*****************************************************************
* Release Notes text for TME 10 LAN Access Version 1.1          *
*                                                               *
* README.TXT    07/21/97  1:02pm                               *
Contents
I. Prerequisites
        1. NetFinity
        2. LANDesk Management Suite
        3. SMS
        4. LAN Access Site

II.  Installation and Configuration of TME 10 LAN Access
        1. LAN Access Transport Layer Configuration
        2. Patch for NetFinity V5.0 Base (NETFBASE.EXE)
        3. Patch for NetFinity V4.0x Manager and Services
        4. Installation and Configuration Window Note
        5. UNINSTALL Instructions for NetFinity OS/2 Provider

III. Additional Information/Known Problems/Limitations
        1. Distributing a file package via the Profile Manager menu
        2. Referencing cli utilities in a Windows V3.1, Windows
           V3.11, or Windows for Workgroups batch file
        3. Configuration Execution log file name
        4. SMS Provider Software Inventory
        5. SMS Provider File Operations and Remote Execution
        6. Passing SMS Alerts through the MPM Alert architecture
        7. Alert Mappings for SMS detected SNMP traps
        8. Important SNA configuration information
        9. Distributing to multiple LANAccessCollections
       10. Creating configuration programs for OS/2
-----------------------------------------------------------------
I. Prerequisites

1. The NetFinity Provider is currently only supported in the
   following NetFinity Manager platforms and versions:
   - NetFinity Manager for OS/2 version 5.0
   - NetFinity Manager for Windows NT version 5.0
   - NetFinity Manager for Windows NT version 4.0

2. The LANDesk Management Suite Provider requires the following:
   - LANDesk Management Suite version 2.51
   - BTRIEVE Database version 6.15 with latest patches on the
     NetWare Server (See ftp://ftp.pervasive-sw.com/bin/patches/
     BTRNW615.EXE for patches)
   - LANDesk Management Console installed on a Windows 95 system
     configured to use the Windows 95 / Microsoft NetWare client.
     - In an NDS environment, you need to use Novell's Netware
       Client32
```

Figure 319 (Part 1 of 6). readme

```
       Special Requirements for the NDS environment
       -------------------------------------------
       - In a NetWare 4.x environment using NDS, the provider must
         be installed on a system connected via Novell's NetWare
         Client 32 which must be installed prior to installing
         LANDesk's Management Console.  In addition, it is
         recommended that all LANDesk clients connect using either
         Client 32 or Microsoft's Service for Novell Directory
         Services even if connected in bindery emulation mode.

       - All of the Btrieve DLLs, both 16-bit and 32-bit, must be
         correct version.  The following dates and sizes were used
         during LAN Access testing:

         Date      Time    Size     Filename
         --------  -----   -------  ------------
         10/20/94  11:56   147,616  NWCALLS.DLL
         10/18/94  14:55    41,456  NWIPXSPX.DLL
         11/02/93  18:12    38,576  NWLOCALE.DLL
         10/12/95  15:28    10,784  W16NR.DLL
          2/13/97  13:15    42,496  W32BTICM.DLL
         10/12/95  15:49    18,944  W32NR.DLL
          2/21/97   3:04    23,040  W32RQCFG.EXE
          1/30/97  14:45    41,980  WBTICOMM.DLL
          2/04/97  13:59    43,472  WBTRCALL.DLL
          7/15/96  10:43     5,824  WBTRTHNK.DLL
         11/07/96  18:49    65,536  WBTRV32.DLL
          4/19/95  15:16     4,192  WBTRVRES.DLL

         Make sure that all copies of the files are the correct
         version.  In particular, on the provider check the
         directories:
         C:\LANDESK
         C:\WINDOWS\SYSTEM

         and on the management server check the directories:
         LANDESK
         PUBLIC
         SYSTEM\WIN32\BIN
         SYSTEM\WIN\BIN

       - When using Novell's NetWare Client 32, modifications that
         the installation program makes to the path statement in
         AUTOEXEC.BAT do not always take effect.  If that happens
         the LANDesk Provider will not be able to find the Btrieve
         DLLs and consequently will not be able to load.  To fix
         this problem, the directory containing the 32-bit Btrieve
         DLLs must be mapped to a search drive on the provider.

       - It is recommended that this search drive be mapped in the
         login script for the context containing the LANDesk groups.
         For example, if the LANDESKADMINGROUP exists in organization
         TIVOLI, and the Btrieve DLLs are located in
         \\server-name\sys\system\win32\bin, you would make the
         following addition to the login script:

          IF MEMBER OF ".CN=LANDESKADMINGROUP.O=TIVOLI" THEN
             map ins s16:=server-name\sys\system\win32\bin
          END
3. The SMS Provider requires:
   - SMS version 1.2 installed a Windows NT system (X86 version)

4. The LAN Access Site requires:
   - Windows NT system installed as Managed Node using the TME 10
     Framework version 3.1 with the 3.1.2 patch
   - The Windows NT Managed Node must NOT be currently configured
     as a TME Repeater.
   - The TMR can be running any Tier 1 operating system with the
     TME 10 Framework version 3.1 with the 3.1.2 patch.
```

Figure 319 (Part 2 of 6). readme

```
II. Installation and Configuration of TME 10 LAN Access
1. When the final dialog box appears for configuring the Network
   Driver (LAN Access Transport Layer)on the Windows NT Managed
   Node, a timeout setting is required.  The dialog box defaults
   to 15 seconds.  This value may have to be adjusted according
   to the performance of your network.

2. Patch for NetFinity V5.0 Base (NETFBASE.EXE)
   The NetFinity provider will replace the NETFBASE.EXE file
   dated 4-10-97, with a fixed version dated 4-30-97.  If
   persistent communication errors occur during the Remote
   Systems Manager group operations or exceptions occur during
   NetFinity shutdown, verify that NETFBASE.EXE is the fixed
   version.

   If you are attempting to install a TME 10 Managed Node or SMS
   Provider on a NetFinity system and are experiencing exceptions
   during NetFinity shutdowns, you will need to do the following
   BEFORE executing the LAN Access install:
     - stop the NetFinity service from the
       Settings\Control Panel\Services window
     - copy NETFBASE.EXE from the US\W32 directory on the LAN
       Access CD to your NetFinity installation directory
       (WNETFIN is the default NetFinity installation directory).
     - restart the NetFinity service from the
       Settings\Control Panel\Services window

   You may now proceed with the LAN Access installation.

3. Patch for NetFinity V4.0x Manager and Services
   NetFinity V4.0x Manager and Services systems running windows
   3.x or Windows 95 require a patch for the file RCSHD.EXE.
   This patch should be applied to all clients to allow proper
   function of the software distribution function.  The patch
   can be found in the \W32\NF40FIX directory on the LAN Access
   CD.

4. Installation and Configuration Window Note
   The Windows Provider and LAN Access Transport Install
   procedure executes several Provider and Transport specific
   configuration routines.  The windows associated with these
   routines are displayed in front of the Install window.
   If, while a configuration routine is displayed, you give the
   input focus to another window, you must remember to return to
   the configuration routine and not to the Install window.
   The Install window will not respond to input until the
   configuration routine is closed.  Likewise, if you display
   the help for a configuration routine, you must remember to
   return to the configuration routine and not the Install
   window when you close the help window.

5. UNINSTALL Instructions for NetFinity OS/2 Provider
```

Figure 319 (Part 3 of 6). readme

```
Here are the steps needed to uninstall the OS/2 NetFinity
Provider.
  1. Stop the NetFinity Network Interface by going to the
     NetFinity directory and enter the following:
           NETFBASE SHUTDOWN

  2. Remove the following files from the Netfinity
     directory:
      - msbrmt.exe
      - rmtresrc.dll
      - mpm2nf.dll
      - mpmact.alt
      - mpmactin.exe
      - mpmexp.dbi
      - mpminst.cmd
      - mpm_br.dll
      - nfmpm.exe
      - nfprvcfg.exe
      - nfprvcfg.hlp

  3.  Delete all the files and remove the directory where the
      provider keeps inventory files (C:\NETFIN\NFMPMDB).

  4.  Delete the LAN Access folder on the desktop.
----------------------------------------------------------------
III. Additional Information/Known Problems/Limitations
1. Distributing a file package via the Profile Manager menu

   You must install one of the following patches to allow
   distribution from the Profile Manager menu:

      3.0-COU-0004  -  Courier V3.0
      3.1-COU-0004  -  TME 10 Software Distribution V3.1

2. Referencing cli utilities in a Windows V3.1, Windows V3.11, or
   Windows for Workgroups batch file

   You must code the fully qualified path to the cli utility in your
   batch file.  All of the cli utilities are located in the
   c:\tmelacli subdirectory.

   For example, if your batch file issues the following command:
         wseterr -1

   Modify it so it appears as follows:
         c:\tmelacli\wseterr -1

3. Configuration Execution log file name

   Appendix B - Software Distribution Error Logging mentions a
   configuration program/execution log file.  The name of this
   log file is labarc.log
4. SMS Provider Software Inventory
   In order for software inventory information to be picked up by
   the MPM SMS provider, an SMS Software Audit must be run by the
   SMS Administrator. After a Software Audit has been performed, any
   information in the SMS database under the AUDITED_SOFTWARE group
   will be returned by the MPM SMS provider.
```

Figure 319 (Part 4 of 6). readme

```
5. SMS Provider File Operations and Remote Execution
   An MPM file operation or remote execution request results in
   two SMS jobs and one SMS query being created. Two SMS packages
   will also be created, if not previously done.

   To improve response time for these SMS jobs, you should minimize
   the PCM polling interval on all targeted systems. To change the
   PCMSVC32.EXE polling interval on a system, edit its C:\SMS.INI
   file and modify the ffPackage Command Manager“ "PollingInterval"
   field appropriately. An additional consideration would be to set
   the services response to "Very Fast" on all affected SMS sites
   via the SMS Administrator site properties window.

   The "Shared Working" directory specified on the "MPM Provider
   For SMS Configuration" window should not be the same share as
   the one used by SMS for package distributions - i.e.
   \\<server name>\SMS_PKGD<drive letter>.

   If the MPM SMS Provider generated SMS jobs are not being executed
   on a targeted system running NT Server. Please refer to Microsoft
   Knowledge Base Article ID: Q164657(SMS: Psmwin32.exe Prevents PCM
   Service from Running Package) for a possible workaround. SMS
   Service Pack 2 may or may not have fixed this problem. If SMS
   Service Pack 2 is installed and the problem still exists, then
   set the following registry entries

     "SMS Package ID (W32)"      = ""
     "SMS Background Jobs"       = 0

   located under

     "My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\MPM2SMS
        Provider"

   Then reboot your system. This will result in packages created by
   the MPM SMS Provider to be run in the foreground. As a result,
   they will be handled by the PCM application and hence distribution
   to SMS Primary Sites will no longer be possible.
6. Passing SMS Alerts through the MPM Alert architecture
   The support for MPM alerts from SMS uses the event database and
   the SNMP trap database.  If you wish to also track the occurrence
   of an SMS Alert you need to:

   1) Bring up the Properties dialog for the alert.
   2) Select the 'Actions' pushbutton to bring up the Alert Actions
      dialog.
   3) make sure the 'Log an Event' check box is checked.
   4) click 'OK' button to dismiss the dialogs.

   Now whenever the Alert occurs an Event will be added to the SMS
   Event database.  This event will be processed by the MPM
   Alert subsystem and forwarded to the MPM Alert subscriber that
   subscribes to the enumerated alert SMSEVENT_380.

7. Alert Mappings for SMS detected SNMP traps
   For SNMP Traps Detected by SMS and reported via the MPM alert
   architecture 0the following mappings will be used:

      AlertArchitectureCode = "Microsoft.SMS.SNMP.V1"
      AlertUID = Enterprise OID + ":" + Generic Trap type
      AlertLabel =  "SMSSnmp_NonPredicated"
```

Figure 319 (Part 5 of 6). readme

```
   The remaining items that may be returned as cooked data are:
elementLabel                  elementArchitectureCode       elementValue
-------------------------------------------------------------------------------
ComponentName                 Component Name                MPM_OCTET
Machine ID                    Machine ID                    MPM_ULONG
Instance Key                  Instance Key                  MPM_ULONG
IP Address                    IP Address                    MPM_OCTET
Enterprise                    Enterprise                    MPM_OCTET
NT Event Source               NT Event Source               MPM_OCTET
Generic Trap Type             Generic Trap Type             MPM_ULONG
Specific Trap ID              Specific Trap ID              MPM_ULONG
Time Ticks                    Time Ticks                    MPM_OCTET
Time Date Received            Time Date Received            MPM_DATETIME
Number of Variables Trap Type Number of Variables Trap Type MPM_ULONG
Variable 0...Number Variables Variable 0...Number Variables MPM_OCTET

8. Important SNA Configuration Information

   Important SNA configuration information can be found on this CD in
   subdirectory \us\readme.sna Please read this file prior to configuring
   your SNA protocol for use with TME 10 LAN Access.

   A change to the SNA configuration requires a restart of the affected
   LAN Access Sites.

9. Distributing to multiple LANAccessCollections
   When distributing to multiple LANAccessCollections, if a failure
   occurs on a LANAccessNode or multiple LANAccessNodes, the error
   dialog displayed by Software Distribution may not accurately report
   the collection that owns the node or nodes where the failure occurred.
   When  messages appear in the error dialog referencing a
   LANAccessCollection, always view the LAN Access Notice Group which
   lists individual failures for each LANAccessNode.  This circumstance
   may also occur when distributing to multiple LANAccessSites.  Always
   view the LAN Access Notice Group if this is the case.

10. Creating configuration programs for OS/2
   Use .cmd files rather than .bat files when creating a configuration
   program for OS/2.
****************************************************************
Copyright 1997 Tivoli Systems, Inc.
All rights reserved.
Tivoli is a registered trademark of Tivoli Systems Inc.
TME 10 and Tivoli Management Environment are trademarks of
Tivoli Systems Inc.  All other brand or product names are
trademarks or registered trademarks of their respective holders.
```

Figure 319 (Part 6 of 6). readme

Appendix B. Microsoft Information

The following information is from the Microsoft Knowledgebase:

```
Microsoft Knowledgebase ARTICLE-ID: Q166244
SQL Server Tuning Parameters for Systems Management Server

The information in this article applies to:
 - Microsoft SQL Server, versions 4.2a, 6.0, and 6.5
 - Microsoft Systems Management Server, versions 1.0, 1.1, and 1.2

SUMMARY
=======
Systems Management Server requires several SQL Server configuration options
to be set correctly to perform at maximum efficiency. This article
summarizes the recommended configuration options for a SQL Server running a
Systems Management Server database.

MORE INFORMATION
Network Support
---------------
Named Pipes network support is required for Systems Management Server to
use to communicate with the Systems Management Server database. You can
change SQL Server network support by running SQL Server setup, selecting
the Change Network Support option, and then selecting Named Pipes as an
installed network.

Recommended Options for Tempdb and the Systems Management Server Database

TempDB should be 20% of the size of the largest database on the SQL server.

Tempdb database options enabled:
   Select Into/ Bulk Copy
     Truncate Log on CheckPoint

Tempdb database options disabled:
   Columns Null by Default
   No CheckPoint on Recovery
   Single User
   DBO Use Only
   Read Only
Systems Management Server database options enabled:
   Truncate Log on CheckPoint

Systems Management Server database options disabled:
   Select Into/ Bulk Copy
   Columns Null by Default
   No CheckPoint on Recovery
   Single User
   DBO Use Only
   Read Only

In SQL Server 6.0 and 6.5, you can change the database options through the
SQL Enterprise Manager user interface by clicking Databases on the Manage
menu. From there, double-click the database to edit, and click the Options
tab. It is also possible to double-click the database name in the Server
Manager window.

In SQL Server 4.2a, 6.0, and 6.5, you can change the database options by
using the SP_DBOPTION stored procedure.
```

```
Recommended SQL Server Configuration Options
SQL Server Memory:
Set the SQL Server memory appropriately. This is the amount of RAM
dedicated to SQL Server. This setting depends on the amount of physical RAM
in the computer and the usage and performance requirements of SQL Server.
Memory is designated in 2-KB blocks. For example, for a dedicated SQL
Server with 128 megabytes (MB) of RAM, you may want to set the memory to
64 MB of RAM (32,768 2-KB blocks) to SQL Server. On a SQL Server and
Systems Management Server site server with 128 MB of RAM, you may only want
to dedicate 40 MB of RAM (20,480 2-KB blocks) to SQL Server.

SQL Server open Objects:
Set open objects to 5,000-7,000, depending on the size of your site and the
child sites below it. The SQL Server default for open objects is 500, which
is not adequate for a small SQL Server running Systems Management Server.
Symptoms of open objects being set too low on a SQL Server include poor
Systems Management Server or SQL Server performance, a backlog of deltamifs
or .mif files in the Systems Management Server directory structure, or
delays in inventory, package distribution, and job status MIF processing.

SQL Server User Connections:
Set user connections appropriately. Each user connection takes 40 KB of
RAM, so this value is determined by the amount of memory dedicated SQL
Server and the number of concurrent connections required. Each Systems
Management Server site server reporting to a SQL Server requires at least
10 connections. Each running instance of the Systems Management Server
Administrator program and the SQL Enterprise Manager requires at least one
more connection.
Tempdb in RAM:
Microsoft does not recommend placing tempdb in RAM on a SQL Server running
Systems Management Server.

In SQL Server 6.0 and 6.5, you can change the SQL Server configuration
options through the SQL Enterprise Manager user interface by clicking SQL
Server Configure on the Server menu. From there, click the Configuration
tab.

In SQL Server 4.2a, 6.0, and 6.5, you can change the configuration options
by using the SP_CONFIGURE stored procedure.

Additional Information
If you make any changes to these parameters, stop and restart the
MSSQLServer service.

Please refer to your SQL Server documentation or online Help for more
information on these settings.

A regularly scheduled database dump, along with backup of the Systems
Management Server registry and directory structure, is a mandatory part of
a good backup and recovery procedure.
 THE INFORMATION PROVIDED IN THE MICROSOFT KNOWLEDGE BASE IS PROVIDED "AS
IS" WITHOUT WARRANTY OF ANY KIND. MICROSOFT DISCLAIMS ALL WARRANTIES, EITHER
EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS
FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL MICROSOFT CORPORATION OR ITS
SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT,
INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN
IF MICROSOFT CORPORATION OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OR
LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES SO THE
FOREGOING LIMITATION MAY NOT APPLY.
```

Figure 320 (Part 2 of 2). Knowledgebase Article Q166244

Appendix C. Special Notices

This publication is intended to help expand the technical knowledge of LAN and systems management professionals who have used the Tivoli Framework in the Intel environment. It will show them how Tivoli LAN Access integrates into that framework, as well as how other LAN Management suites integrate into Tivoli LAN Access. The information in this publication is not intended as the specification of any programming interfaces that are provided by Tivoli LAN Access. See the PUBLICATIONS section of the IBM Programming Announcement for Tivoli LAN Access 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 use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

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:

AIX
AS/400
DB2
Netfinity
OS/2
RISC System/6000
RS/6000
System/390
Trouble Ticket
IBM®
AnyNet
Client Access
IBM
NetView
PS/2
RMONitor
SystemView
ThinkPad
ValuePoint

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

Java and HotJava are trademarks of Sun Microsystems, Incorporated.

Microsoft, Windows, Windows NT, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

Pentium, MMX, ProShare, LANDesk, and ActionMedia are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be trademarks or service marks of others.

Appendix D. Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

D.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see “How to Get ITSO Redbooks” on page 281.

- *NT Systems Management Integration*, SG24-2107
- *Netfinity V5.0 Command Line and LMU Support*, SG24-4925
- *Integrating Netware Management into NetView for AIX*, SG24-2532
- *Understanding Tivoli's TME 3.0 and TME 10*, SG24-4948
- *TME 3.0 NT - Automated Processes*, SG24-4793
- *Setting Up a TME 3.0 NT Environment*, SG24-4819

D.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
Lotus Redbooks Collection	SBOF-6899	SK2T-8039
Tivoli Redbooks Collection	SBOF-6898	SK2T-8044
AS/400 Redbooks Collection	SBOF-7270	SK2T-2849
RS/6000 Redbooks Collection (HTML, BkMgr)	SBOF-7230	SK2T-8040
RS/6000 Redbooks Collection (PostScript)	SBOF-7205	SK2T-8041
RS/6000 Redbooks Collection (PDF Format)	SBOF-8700	SK2T-8043
Application Development Redbooks Collection	SBOF-7290	SK2T-8037

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 `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:

- **Redbooks Web Site on the World Wide Web**

  `http://w3.itso.ibm.com/`

- **PUBORDER** — to order hardcopies in the United States
- **Tools Disks**

  To get LIST3820s of redbooks, type one of the following commands:

  ```
  TOOLCAT REDPRINT
  TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET SG24xxxx PACKAGE
  TOOLS SENDTO CANVM2 TOOLS REDPRINT GET SG24xxxx PACKAGE (Canadian users only)
  ```

  To get BookManager BOOKs of redbooks, type the following command:

  ```
  TOOLCAT REDBOOKS
  ```

  To get lists of redbooks, type the following command:

  ```
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
  ```

  To register for information on workshops, residencies, and redbooks, type the following command:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1998
  ```

- **REDBOOKS Category on INEWS**
- **Online** — send orders to: USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL

Redpieces

For information so current it is still in the process of being written, look at "Redpieces" on the Redbooks Web Site (`http://www.redbooks.ibm.com/redpieces.html`). Redpieces are redbooks in progress; not all redbooks become redpieces, and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

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** — 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 North 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	1-403-267-4455
Outside North America	(+45) 48 14 2207 (long distance charge)

- **1-800-IBM-4FAX (United States)** or **(+1)001-408-256-5422 (Outside USA)** — ask for:

Index # 4421 Abstracts of new redbooks
Index # 4422 IBM redbooks
Index # 4420 Redbooks for last six months

- **On the World Wide Web**

Redbooks Web Site	http://www.redbooks.ibm.com/
IBM Direct Publications Catalog	http://www.elink.ibmlink.ibm.com/pbl/pbl

Redpieces

For information so current it is still in the process of being written, look at "Redpieces" on the Redbooks Web Site (`http://www.redbooks.ibm.com/redpieces.html`). Redpieces are redbooks in progress; not all redbooks become redpieces, and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

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.

Index

A
Advanced Tool Configuration 128
attributes 77
Auto-Discovery Interval 30, 60
automatic update 61
Automatic Update check box 38

B
BasicLANAccessSite 21
bibliography 279
Btrieve 6.15 72, 76, 79, 81

C
Character set 144
Client Configuration Utility 106
CLNTCFG.INI 104

D
database schema 237
Desktop Manager 91, 112, 117
Desktop Remote 90
Dictionary File 137
directory replication 148
discovery process 31
Distribute 90
Distribute Console 107, 112, 117
dynamic alerts 164

E
event adapter 2, 11, 25, 62, 70, 139, 164, 197
event adapter log file 63
event class 64

F
file package options 179
File Package Properties 180
filtering categories 34

H
Hardware Inventory 137, 138, 165, 194

I
Include Local MPM Information 30
install_client authority 11, 23
inventory database 236

L
la_ldms.baroc 139
la_netf.baroc 64, 139
la_sms.baroc 139, 254
LAN
  collection 51
  collection object 1, 25, 40
  managed node 2
  node object 1, 25
  object node 43
  objects 24
  site 134
  site location 27
  site object 1, 2, 24
LAN managing station 2
lanacc.baroc 64, 254
LANAccessSite 18
LANDESKADMINGROUP 87
logon server 141

M
management tools 89
Maximum Sockets option 100
Microsoft Visual Test 169
MPM APIs 120
MPM provider sites 13
MPM providers 1, 2, 11, 24, 49, 109, 110, 112, 204, 248
MPM-API 128

N
NetWare Server 80
Network Driver Configuration 116
Network Driver Configuration panel 29
network events 1
notice group 15
NTFS 133

O
ODBC core components 173
OS/2 MPM provider 49

P
Package Command Manager 161, 162
password 50, 132, 143, 146, 172
password protected 32
patch 11, 13, 83, 131

Patch 3.1.1 71
Patch 3.1.2 71
Patch 6.15.440 72
patches 3
polling interval 123

R

real-time 91
Release Notes 12
remote command execution 131
Retrieving the event cache 201
rule 65

S

Server Manager 91
services tools 89
setup.exe 132
setup.exe command 7, 117, 171
Site Code 151
site server 141
SMS events 164
SMS Installer 169
software audit 153
software inventory 153, 190
Software Metering 91
Sort order 144
SYS volume 87
SYS:bti\NetWare 75
SYS:SYSTEM volume 75

T

Target MPM Properties 43
Target MPM Protocol 43
Target MPM Provider 44
TEC event server 64, 70
tecad_msb.cfg 70
tecad_msb.exe 62, 139
tecad_msb.log 139
tecad_msb.map 63, 139
threshold 207
TIVLDW16 188
TIVLDW32 188
Tivoli Enterprise Console 2, 121, 164
Tivoli Framework 1
Tivoli Inventory 1
Tivoli LAN Access objects 1
Tivoli_Admin_Priviledges group 9
TME Event Group 202
TME Event Source 202

U

user connections 145

V

Validation Policy 21

W

wcopmrules command 66
wcprb command 65
wcrtrb command 65
wgetadmin command 23
wimprbclass command 66
wloadrb command 67
wpatch command 12
wstartesvr command 67, 257
wstopesvr command 67, 68, 257

ITSO Redbook Evaluation

Integrating LAN Management Tools with Tivoli LAN Access
SG24-2118-00

Your feedback is very important to help us maintain the quality of ITSO redbooks. **Please complete this questionnaire and return it using one of the following methods:**

- Use the online evaluation form found at http://www.redbooks.ibm.com
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Which of the following best describes you?
__Customer __Business Partner __Solution Developer __IBM employee
__None of the above

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction _____

Please answer the following questions:

Was this redbook published in time for your needs? Yes____ No____

If no, please explain:

_____

_____

_____

_____

What other redbooks would you like to see published?

_____

_____

_____

Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)

_____

_____

_____

_____

_____

SG24-2118-00
Printed in the U.S.A.