



Nortel Communication Server 1000

Telephony Manager 3.1 Installation and Commissioning

Document status: Standard
Document version: 01.07
Document date: 3 June 2009

Copyright © 2003-2009, Nortel Networks
All Rights Reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Nortel, the Nortel Logo, the Globemark, SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.

Microsoft, MS-DOS, Windows, Windows NT, and Personal Web server are registered trademarks of Microsoft Corporation.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

HP and OpenView are trademarks of Hewlett-Packard Corporation.

Intel and Pentium are trademarks of Intel Corporation.

Novell and NetWare are trademarks of Novell, Inc.

Java is a trademark of Sun Microsystems, Inc.

pcANYWHERE is a trademark of Symantec Corp.

Regular expression library, Author: Henry Spencer, Copyright (c) 1986, 1993, 1995 by University of Toronto.

CToolbarEx - a flat toolbar, Copyright (C) 1997,'98 by Joerg Koenig FooWare Java FTP client. Covered by GNU General Public License.

SNMP Construction Kit (SCK) : Copyright (C) 1998 Yves Soun. Covered by GNU General Public License.

The asterisk after a name denotes a trademarked item.

All other trademarks are the property of their respective owners.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

This product includes the following software:

The Purdue Compiler Construction Tool Set, written by Russell Quong June 30, 1995. Adapted by Terence Parr to ANTLR stuff. Parr Research Corporation with Purdue University and AHPARC, University of Minnesota, 1989-1995.

SNMP Development Kit, written by James R. Davin, Advanced Network Architecture group, M.I.T Laboratory for Computer Science 45 Technology Square Cambridge, MA 02139 Copyright 1988, 1989 Massachusetts Institute of Technology. Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of M.I.T. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

SAX Parser for XML from Apache, Version 1.1 for SAX (Simple API for XML). Copyright (c) 1999-2000 The Apache Software Foundation (<http://www.apache.org/>). All rights reserved.

W3C DOM implementation for Java: Copyright 2000 World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. <http://www.w3.org/Consortium/Legal/>

Cryptix MD5 (RFC 1321) and SHA-1 (NIST FIPS 180-1) message digest algorithms: Copyright (c) 1997 Systemics Ltd on behalf of the Cryptix Development Team.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks Inc. Telephony Manager software license agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying Telephony Manager software or installing the hardware unit with pre-enabled Telephony Manager software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. **License grant.** Nortel Networks Inc. ("Nortel Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.
2. **Restrictions on use; reservation of rights.** The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and

included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. **Limited warranty.** Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date the Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.
4. **Limitation of liability.** IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.
5. **Government licensees.** This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.
6. **Use of software in the European Community.** This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.
7. **Term and termination.** This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will

automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. **Export and re-export.** Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.
9. **General.** If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks Inc., 2375 N. Glenville Dr., Richardson, TX 75082.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Revision History

June 2009

Standard 01.07. This document is up-issued to add an attention for the Installing Telephony Manager 3.1 software procedure.

March 2008

Standard 01.06. This document is up-issued add information to Upgrading to Telephony Manager 3.1, list the versions of IIS supported on the OS platform, and add attention information to Remote Desktop and Terminal Server.

July 2007

Standard 01.05. This document is up-issued to add added attention information to procedure for adding a user.

June 2007

Standard 01.04. This document is up-issued update information in Converting Systems in Telephony Manager and ELAN subnet information in Appendix A, "Typical configurations".

June 2007

Standard 01.03. This document is up-issued edit information in Configuring security for Telephony Manager 3.1.

June 2007

Standard 01.02. This document is up-issued updated information in Configuring security for Telephony Manager 3.1.

May 2007

Standard 01.01. This document is up-issued to support Nortel Communication Server Release 5.0.

July 2006

Standard 5.00. This document is up-issued from Telephony Manager 3.0 to Telephony Manager 3.1.

March 2006

Standard 4.00. This document is up-issued to support Telephony Manager 3.0.

August 2005

Standard 3.00. This document is up-issued to support Communication Server 1000 Release 4.5.

September 2004

Standard 2.00. This document is up-issued for Communication Server 1000 Release 4.0.

October 2003

Standard 1.00. This document is a new NTP for Succession 3.1. It was created to support a restructuring of the Documentation Library. This document contains information previously contained in the following legacy document, now retired: *Using Optivity Telephony Manager (553-3001-330)*.

Contents

How to get help	17
New in this release	19
New in Telephony Manager 3.1	19
Related information	19
NTPs	19
Online	22
CD-ROM	22
Overview	23
Contents	23
Subject	23
Note about legacy products and releases	23
Applicable systems	24
System migration	24
Intended audience	25
Conventions	25
Terminology	25
Text	26
Acronyms	27
Preparing for installation	29
Contents	29
Overview	29
Telephony Manager 3.1 installation tasks	30
Supported systems	30
Supported upgrade paths	32
Telephony Manager 3.1 server and clients overview	32
Telephony Manager 3.1 hardware requirements	33
Telephony Manager 3.1 software requirements	36
Installing Telephony Manager 3.1 server software	43
Contents	43
Overview	43
Installation program features	44
Checking local security settings	44

Installing Telephony Manager 3.1 software	47
Installing Telephony Manager 3.1 client software	61
Contents	61
Overview	61
Installing the client software	64
Performing a keycode upgrade	75
Contents	75
Keycode upgrade	75
Performing migrations	79
Contents	79
Upgrades and migration	79
Upgrading to Telephony Manager 3.1	80
Operating system migration	80
Configuring Secure Sockets Layer (SSL)	85
Contents	85
Overview	85
Installing a server certificate in IIS	85
Configuring SSL on the Telephony Manager 3.1 server platform	86
Enabling SSL for Telephony Manager 3.1 Web logon	86
Importing Telephony Manager 3.1 Root Certificate	87
Setting up CND SSL	87
License management	89
Contents	89
Serial number and keycode	89
TN license	89
RU license	90
Client license	91
Security device (dongle)	91
Before configuring Telephony Manager 3.1	93
Contents	93
Overview	93
Testing the connection	94
Windows Server 2003 configuration	103
Contents	103
Windows Server 2003 configuration and restrictions	103
Adding Telephony Manager 3.1 Web users	135
Contents	135
Overview	135
Capabilities	135
User logon and security	136
Access permissions	137
User authentication	138

User groups	140
Installing and configuring desktop services	147
Configuring a modem for Telephony Manager 3.1 applications	149
Contents	149
Using installation tools	149
Configuring high-speed smart modems	150
Troubleshooting modem connections	151
Security Management	157
Security for upgrades and re-installations	158
Administrators	159
Users	159
Authentication	160
User management	162
Logon process	163
User groups	164
User management recommendations	166
Installation	166
Configuring Telephony Manager 3.1 Navigator users	167
Creating a user group	170
Adding a user	173
Authenticating users	175
Initial logon	177
Setting up the CND server and Terminal server	179
CND server	179
Terminal server	179
Configuring the Web browser client	185
Configure Windows® XP SP2 to work with Telephony Manager 3.1	185
Accessing the Telephony Manager 3.1 Web server from a Web browser	186
Integrating Telephony Manager 3.1 with ENMS	187
Contents	187
Overview	188
Integration requirements	188
Telephony Manager 3.1: ENMS integration	189
Telephony Manager OIT files	190
About oitInstall	191
Using ENMS InfoCenter	192
Viewing Telephony Manager 3.1 server object properties	196
Modifying Telephony Manager 3.1 server object properties	197
Starting Telephony Manager 3.1 Web applications	197
JRE release specific to Apache Tomcat	199
Using FaultSummary	200
Configuring Telephony Manager 3.1	203

Removing a Telephony Manager 3.1 server	203
Troubleshooting	204
Integrating Telephony Manager 3.1 with HP OpenView	207
Contents	207
Overview	207
Limitations	208
Hardware and software requirements	208
System integration	209
Installation and configuration	211
Converting Systems in Telephony Manager	231
Contents	231
Overview	231
Uninstalling Telephony Manager 3.1	235
Contents	235
Overview	235
Uninstalling Telephony Manager 3.1	235
Uninstallation of Telephony Manager Client or Telephony Manager Server	237
Windows 2000 Server reference	243
Contents	243
Overview	243
Installing Telephony Manager 3.1 on Windows 2000 Server	243
Installing Network Adapter software	246
Testing network cards	253
Setting up Metabase Editor utility	255
Contents	255
Overview	255
Setting up the Metabase Editor utility	255
Appendix A Telephony Manager 3.1 engineering guidelines	257
Contents	257
Overview	257
Capacity factors	258
Hardware and software comparisons	259
Software limits	260
IIS support on the Telephony Manager server	273
PC hardware	274
Network bandwidth	277
Telephony Manager 3.1 system performance	285
Telephony Manager 3.1 port usage	291
Telephony Manager 3.1 language support	294
FTP Server configuration	295
Appendix B Installation checklist	297
Contents	297

Overview	297
Installation requirements	297
Programming the switch	298
PC/server installation requirements	298

Appendix C Configuring a USB modem 299

Contents	299
Overview	299
Checking for a virtual COM port	299
Changing the virtual COM port to USB modem association	300

TBS to CND file header conversion 303

Index 305

Procedures

Procedure 1	Checking local security settings	45
Procedure 2	Workarounds for installation of PostgreSQL	46
Procedure 3	Installing Telephony Manager 3.1 software	47
Procedure 4	Installing the client software	64
Procedure 5	Re-enabling the DCOM service	73
Procedure 6	Upgrading the keycode	75
Procedure 7	Operating system migration	81
Procedure 8	Creating the employee csv file	82
Procedure 9	Configuring SSL on the Telephony Manager 3.1 server platform	86
Procedure 10	Enabling SSL for Telephony Manager 3.1 Web logon	86
Procedure 11	Importing Telephony Manager 3.1 Root Certificate	87
Procedure 12	Setting up CND SSL	87
Procedure 13	Setting up communications information	94
Procedure 14	Setting up customer information	97
Procedure 15	Setting up Telephony Manager 3.1 applications	99
Procedure 16	Setting up system data	101
Procedure 17	Enabling Web Service extensions in IIS 6.0	105
Procedure 18	Adding a New ISAPI Web Service extension to IIS 6.0	106
Procedure 19	Enabling parent paths	107
Procedure 20	Configuring IIS 5.0 isolation mode	109
Procedure 21	Adjusting Internet Explorer security settings	110
Procedure	Disable Terminal Services on the Telephony Manager Server	112
Procedure 22	Configuring client authentication on the server side	114
Procedure 23	Configuring security for Telephony Manager 3.1	118
Procedure 24	Configuring authentication	139
Procedure 25	Configuring telephone access options	144
Procedure 26	Configuring the Telephone: Keys page	145
Procedure 27	Configuring the Telephone: Features page	147
Procedure 28	Installing and Configuring Desktop Services	147
Procedure 29	Changing the factory INIT string	150
Procedure 30	Verifying that the modem is properly configured	151
Procedure 31	Testing the COM port	151
Procedure 32	Verifying the COM port	152

Procedure 33	Viewing the Communications profiles	153
Procedure 34	Verifying the modem connection	153
Procedure 35	Resolving a failed session	154
Procedure 36	Resolving COM port error	155
Procedure 37	logon process	164
Procedure 38	Configure authentication	168
Procedure 39	Creating a user group	171
Procedure 40	Adding a user	174
Procedure 41	Configure Windows XP SP2 to work with Telephony Manager 3.1	185
Procedure 42	Accessing the Telephony Manager 3.1 Web server from a Web browser	186
Procedure 43	Downloading the OIT files	189
Procedure 44	Checking the current configuration	190
Procedure 45	Configuring ENMS InfoCenter for Telephony Manager 3.1	192
Procedure 46	Logging in to InfoCenter	194
Procedure 47	Viewing Telephony Manager 3.1 server Object Properties	196
Procedure 48	Modifying Telephony Manager 3.1 server Object Properties	197
Procedure 49	Updating Apache Tomcat path	199
Procedure 50	Setting up FaultSummary	201
Procedure 51	Launching FaultSummary	202
Procedure 52	Removing a Telephony Manager 3.1 server	203
Procedure 53	Accessing the Telephony Manager 3.1 server from NNM	210
Procedure 54	Installing Telephony Manager 3.1 Alarm MIB	211
Procedure 55	Configuring an event	213
Procedure 56	Setting up a Telephony Manager 3.1 server object on the Network Map	219
Procedure 57	Configuring Telephony Manager 3.1 Web server Access	228
Procedure 58	Converting a CS 1000S to CS 1000E CPPM	232
Procedure 59	Converting a CS 1000M Cabinet/Chassis to CS 1000E CPPM	232
Procedure 60	Converting a Meridian 1 system to CS 1000M/E system	233
Procedure 61	Converting a Branch Media gateway CS 1000M Cabinet/Chassis system to CS 1000E CPPM	233
Procedure 62	Uninstalling Telephony Manager Server with no clients associated	237
Procedure 63	Uninstalling Telephony Manager Server with clients associated	239
Procedure 64	Uninstalling Telephony Manager Client if able to access Common Data path of Telephony Manager Server	239
Procedure 65	Uninstalling Telephony Manager Client if unable to access Common Data path of Telephony Manager Server	240
Procedure 66	Deleting client information on the server manually	241
Procedure 67	Installing the Windows server by using the Windows setup program	243
Procedure 68	Installing Windows server components	244
Procedure 69	Allowing Telephony Manager 3.1 client access without constant server log on (optional)	246
Procedure 70	Installing Network Adapter software	246

Procedure 71	Configuring TCP/IP settings on a Windows server	247
Procedure 72	Configuring Telephony Manager 3.1 Dual Network Interface	249
Procedure 73	Installing a modem on a Windows server	251
Procedure 74	Installing Remote Access Service (RAS) on a Windows server	251
Procedure 75	Testing the Nortel server subnet interface	253
Procedure 76	Testing the Embedded LAN interface	253
Procedure 77	Setting up the Metabase Editor utility	255
Procedure 78	Creating an LMHOSTS file	288
Procedure 79	Configuring TCP/IP to use LMHOSTS on a Windows PC	290
Procedure 80	Checking for a virtual COM port	299
Procedure 81	Changing the virtual COM port to USB modem association	301

How to get help

This section explains how to get help for Nortel products and services.

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. More specifically, the site enables you to:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the telephone from a Nortel Solutions Center

If you don't find the information you require on the Nortel Technical Support Web site, and have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or re-seller

If you purchased a service contract for your Nortel product from a distributor or authorized re-seller, contact the technical support staff for that distributor or re-seller.

New in this release

New in Telephony Manager 3.1

This document incorporates new changes in Telephony Manager 3.1

To configure and manage the PBX release 5.0, Telephony Manager (TM) software must be upgraded to Telephony Manager 3.1.

Telephony Manager 3.1 features the following installation and upgrade enhancements:

- License Agreement available upon installation reflects the modified version and copyright year.
- All migration and upgrade limitations for Telephony Manager 3.0 are applicable to Telephony Manager 3.1.
- As a part of the Telephony Manager 3.1 upgrade, the IP telephones that are present in older releases are rebranded to new corresponding telephone types.
- New functionality is added to the installation application, permitting uninstallation of Telephony Manager Client and Telephony Manager Server separately when they are not accessible to each other. For more information, see ["Uninstalling Telephony Manager 3.1" \(page 235\)](#).
- CND 2.1 is the minimum supported level of CND for Telephony Manager 3.1 For more information on CND, see *Common Network Directory 2.1 Administration Guide (NN43050-101)*.

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *Telephony Manager 3.1 System Administration (NN43050-601)*
Provides information about using the applications and features available with Telephony Manager 3.1 on systems.
- *Telephony Manager 3.1 Telemanagement Applications (NN43050-602)*

Provides information about the following optional telemanagement applications:

- Telecom Billing System (TBS)
- TBS Web Reporting
- General Cost Allocation System (GCAS)
- Consolidated Reporting System (CRS)
- Consolidated Call Cost Reports (CCCR)

- *Common Network Directory 2.1 Administration Guide (NN43050-101)*

The Common Network Directory 2.1 Administrator Guide provides information on the CND Service and the CND management utilities and tools.

- *Features and Services (NN43001-106-B1, NN43001-106-B2, NN43001-106-B3)*

Describes features associated with systems. For each feature, information is provided on feature implementation, feature operation, and interaction between features.

- *Software Input/Output: Administration (NN43001-611)*

Describes the prompts and responses for a system's command line interface (CLI). This guide includes information about overlay programs that are classified as administration overlays.

- *IP Trunk: Description, Installation, and Operation (NN43001-563)*

Describes configuration and maintenance of the Voice Gateway Media card. This card appears as a 24-port trunk card with ISDN Signaling Link (ISL) and D-channel signaling.

- *IP Line: Description, Installation, and Operation (NN43100-500)*

Describes configuration and maintenance of gateway cards.

- *Telephones and Consoles: Description (NN43001-567)*

Describes telephones and related features. The telephones provide access to a Telephony Manager-generated Corporate Directory.

- *DECT: Description, Planning, Installation, and Operation (NN43120-114)*

Provides an overview of Telephony Manager for Nortel Integrated DECT (DECT) systems.

- *Software Input/Output: Administration (NN43001-611)*

Describes the meaning of system messages.

- *Software Input/Output: Maintenance (NN43001-711)*

Describes the prompts and responses for a system's command line interface (CLI). This guide includes information about overlay programs that are classified as maintenance overlays.

- *Communication Server 1000M and Meridian 1: Large System Installation and Configuration (NN43021-310)*

Provides information about the Survivable IP Expansion (SIPE) feature for a Meridian 1 Large System.

- *Communication Server 1000S: Installation and Configuration (NN43031-310)*

Provides information about the Survivable IP Expansion (SIPE) feature for CS 1000S systems.

- *Data Networking for Voice over IP (553-3001-160)*

Provides information for Data Networking about Communication server 1000 and Meridian 1 systems.

- *Security Management (NN43001-604)*

Provides information about the OAM Security Phases I and II

- *SRG Configuration Guide (Survivable Remote Gateway): SRG software version 1.0 (P0609195)*

Provides information on how to setup and configure a Survivable Remote Gateway (SRG) system for an IP network.

- *Main office configuration guide for Survivable Remote Gateway 50 (NN43001-307)*

Describes the Main Office Configuration for the Survivable Remote Gateway 50. Information in this document complements information found in documents in the Communication Server 1000 documentation suite.

- *Branch Office: Installation and Configuration (NN43001-314)*

Describes the Branch Office feature and contains information on planning, installation, configuration, and maintenance.

- *Emergency Services Access (NN43001-613)*

Describes the Emergency Services Access feature.

- *What's New for Communication Server 1000 Release 5.0 (NN43001-115)*

Contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 5.0 software.

- *Succession 1000/M Main Office Configuration for SRG: Succession software version 3.1 (P0609617)*

Provides an overview of Succession programming to support Survivable Remote Gateway (SRG) as a branch office.

Online

To access Nortel documentation online, click the Technical Documentation link under Support on the Nortel home page:

www.nortel.com

CD-ROM

To obtain Nortel documentation on CD-ROM, contact your Nortel customer representative.

Overview

Contents

This chapter contains information about the following topics:

["Subject" \(page 23\)](#)

["Applicable systems" \(page 24\)](#)

["Intended audience" \(page 25\)](#)

["Conventions" \(page 25\)](#)

Subject

This document is up-issued to incorporate information in the Telephony Manager 3.1 Feature Specification document.

Telephony Manager 3.1 (TM 3.1) is designed for managers of telecommunications equipment and authorized Nortel* distributors. Telephony Manager 3.1 provides a single point of access for management of Nortel systems. Telephony Manager 3.1 uses internet protocol (IP) technology to target:

- single point of connectivity to systems and related devices
- data collection for traffic and billing records
- collection, processing, distribution, and notification for alarms and events
- data entry and propagation (employee names and telephone numbers shared in multiple databases)
- Windows® and Web-based management applications

Note about legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Nortel Communication server 1000 Release 4.0 software.

For more information about legacy products and releases, click the Technical Documentation link under Support on the Nortel home page:

www.nortel.com

Applicable systems

This document applies to the following systems:

- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet
- Meridian 1 PBX 51C
- Meridian 1 PBX 61C
- Meridian 1 PBX 81
- Meridian 1 PBX 81C
- Communication server 1000S (CS 1000S)
- Communication server 1000M Chassis (CS 1000M Chassis)
- Communication server 1000M Cabinet (CS 1000M Cabinet)
- Communication server 1000M Half Group (CS 1000M Half Group)
- Communication server 1000M Single Group (CS 1000M Single Group)
- Communication server 1000M/E Multi Group (CS 1000M/E Multi Group)
- Communication server 1000E CPPM (CS 1000E CPPM)

Take note that when upgrading software, memory upgrades can be required on the Signaling Server, the Call Server, or both.

System migration

After particular Meridian 1 systems are upgraded to run CS 1000 Release 4.0 software and configured to include a signaling server, they become CS 1000M/E systems.

"Meridian 1 systems to CS 1000M/E systems" (page 24) lists each Meridian 1 system that supports an upgrade path to a CS 1000M/E system.

Meridian 1 systems to CS 1000M/E systems

This Meridian 1 system...	Maps to this CS 1000M/E system...
Meridian 1 PBX 11C Chassis	CS 1000M Chassis/Cabinet
Meridian 1 PBX 11C Cabinet	CS 1000M Chassis/Cabinet
Meridian 1 PBX 51C	CS 1000M Half Group
Meridian 1 PBX 61C	CS 1000M Single Group

Meridian 1 PBX 81	CS 1000M/E Multi Group
Meridian 1 PBX 81C	CS 1000M/E Multi Group

For more information, refer to one or more of the following NTPs:

- *Communication Server 1000M and Meridian 1: Small System Upgrade Procedures (NN43011-458)*
- *Communication Server 1000M and Meridian 1: Large System Upgrade Procedures (NN43021-458-B1, -B2, -B3)*
- *Communication Server 1000E: Upgrade Procedures (NN43041-458)*
- *Communication Server 1000S: Upgrade Procedures (NN43031-458)*

Intended audience

This document is intended for Communication Server 1000 and Meridian 1 system administrators using a Microsoft Windows®-based PC for management activities. It assumes that you have the following background:

- working knowledge of the Windows® 2000 server, Windows Server 2003, Windows 2000 Professional, and Windows XP Professional operating systems
- familiarity with Communication Server 1000 and Meridian 1 system management activities
- knowledge of general telecommunications concepts
- experience with window systems or graphical user interfaces (GUI)
- knowledge of Internet Protocol (IP)

Conventions

Terminology

In this document, the following systems are referred to generically as system:

- Meridian 1
- Communication server 1000S (CS 1000S)*
- Communication server 1000M/E (CS 1000M/E)*
- Communication server 1000E CPPM (CS 1000E CPPM)*

The following systems are referred to generically as Small System:

- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet
- Communication server 1000M Chassis (CS 1000M Chassis)*

- Communication server 1000M Chassis (CS 1000M Cabinet)*

The following systems are referred to generically as Large System:

- Meridian 1 PBX 51C
- Meridian 1 PBX 61C
- Meridian 1 PBX 81
- Meridian 1 PBX 81C
- Communication server 1000M Half Group (CS 1000M Half Group)*
- Communication server 1000M Single Group (CS 1000M Single Group)*
- Communication server 1000M/E Multi Group (CS 1000M/E Multi Group)*

*Systems that are referred to as CS 1000.

Text

In this document, the following text conventions are used:

angle brackets (< >) Indicates that you must input some command text. You choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command.

Example: If the command syntax is

chg suppress_alarm <n>

where n is 0 = all, 1 = minor, 2 = major, 3 = critical, you enter

chg suppress_alarm 3

to suppress all alarms except critical alarms

bold

Courier text

Indicates command names, options, and text.

Example:

Enter prt open_alarm

.

Italic text

Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore.

Example: For additional information, refer to *Using Telephony Manager*.

plain Courier text	Indicates command syntax and system output, for example, prompts and system messages. Example: Open Alarm destination #0 is 47.82.40.237
separator (>)	Shows menu paths. Example: Select Utilities > Backup in the Navigator window.

Acronyms

The following are some of the acronyms used in this document:

API	application programming interface
ASP	active server page
CCCR	consolidated call cost reports
CLAN	customer local area network (see Nortel server subnet*)
CLI	command line interface
CND	Common Network Directory
CRS	Consolidated Reporting System
DBA	Data Buffering and Access
DEP	Data Execution Prevention
DN	directory number
ELAN	embedded local area network
ENMS	Enterprise Network Management System
FTP	file transfer protocol
GCAS	General Cost Allocation System
GUI	graphical user interface
IIS	internet information services
I/O	input/output
IP	Internet Protocol
ITG	Internet Telephony Gateway
LAN	local area network
LDAP	lightweight directory access protocol
MAT	Meridian Administration Tools
MIB	management information base
NIC	Network Interface Card

TM	Telephony Manager
PTY	pseudo-TTY (network port)
RAS	remote access server
RU	reporting unit
SNMP	simple network management protocol
SSL	secure sockets layer
TBS	Telecom Billing System
TLAN	telephony local area network
TN	terminal number
TTY	teletype (serial port)
uid	unique identifier in LDAP synchronization
VPN	Virtual Private Network
VLAN	virtual local area network
WAN	wide area network

*Nortel server subnet, formerly known as the CLAN, is the subnet to which the Telephony Manager Network interface is connected.

Preparing for installation

Contents

This chapter contains information about the following topics:

["Overview" \(page 29\)](#)

["Telephony Manager 3.1 installation tasks" \(page 30\)](#)

["Supported systems" \(page 30\)](#)

["Supported upgrade paths" \(page 32\)](#)

["Telephony Manager 3.1 server and clients overview" \(page 32\)](#)

["Telephony Manager 3.1 hardware requirements" \(page 33\)](#)

["Telephony Manager 3.1 software requirements" \(page 36\)](#)

Overview

Telephony Manager 3.1 combines with the Enterprise Network Management System (ENMS) to give an integrated data, voice, and video network, as part of the Nortel Unified Networking system. The resulting integration provides converged LAN, WAN, and voice management, and the capacity to monitor Telephony Manager 3.1 server activity through the ENMS.

For installation recommendations to create a secure environment for your Telephony Manager 3.1 data and users, see *Telephony Manager 3.1 System Administration (NN43050-601)*.

To configure modems for use with Telephony Manager 3.1, refer to ["Configuring a modem for Telephony Manager 3.1 applications" \(page 149\)](#).

When planning Telephony Manager 3.1 installations, consider detailed hardware and software guidelines in Appendix A.

Telephony Manager 3.1 installation tasks

Installing Telephony Manager 3.1 involves performing tasks related to:

- new Telephony Manager 3.1 server (standalone) software
- new client software
- upgrades
- migrations
- Web Help
- license management

These tasks are covered in detail in the coming chapters.

Supported systems

Telephony Manager 3.1 supports the following machine types and managed system software releases:

Table 1
Machine types and switch software releases supported in Telephony Manager 3.1

System type = Meridian 1				System type = Communication Server	
Hardware type	Machine type	X11 Switch software releases supported	X21 Switch software releases supported	Machine type	X21 Switch software releases supported
11C Cabinet/11C Chassis *	11C Cabinet/11C Chassis	24, 25	3, 4, 4.5, 5	Communication Server 1000M Cabinet/Chassis	3, 4, 4.5
51C 060	51C 060	24, 25	3, 4, 4.5	Communication Server 1000M Half Group 060	3, 4, 4.5
51C 060E	51C 060E	24, 25	3, 4, 4.5	Communication Server 1000M Half Group 060E	3, 4, 4.5
61C 060	61C 060	24, 25	3, 4, 4.5	Communication Server 1000M Single Group 060	3, 4, 4.5
61C 060E	61C 060E	24, 25	3, 4, 4.5	Communication Server 1000M Single Group 060E	3, 4, 4.5

61C PII	61C PII		3, 4, 4.5, 5	Communication Server 1000M Single Group PII	3, 4, 4.5, 5
61C CPPIV	61C CPPIV		4.5, 5	Communication Server 1000M Single Group CPPIV	4.5, 5
81, 81C 060	81, 81C 060	24, 25	3, 4, 4.5	Communication Server 1000M/E Multi Group 060	3, 4, 4.5
81, 81C 060E	81, 81C 060E	24, 25	3, 4, 4.5	Communication Server 1000M/E Multi Group 060E	3, 4, 4.5
81C PII	81C PII	25	3, 4, 4.5, 5	Communication Server 1000M/E Multi Group PII	3, 4, 4.5, 5
81C CPPIV	81C CPPIV		4.5, 5	Communication Server 1000M/E Multi Group CPPIV	4.5, 5
CS 1000S				Communication Server 1000S	2, 3, 4, 4.5
1000E PII				Communication Server 1000M/E Multi Group PII	4, 4.5, 5
1000E CPPIV				Communication Server 1000M/E Multi Group CPPIV	4.5, 5
1000E CPPM **				Communication Server 1000E CPPM	5

*The 11C Cabinet/11C Chassis was originally called 11C/Mini. The 11C/Mini was rebranded in Telephony Manager 3.0.

**Both Standard Availability and High Availability options share the same machine type, for example 1000E CPPM. This is consistent with the manner in which Telephony Manager handles redundant systems in PII and CPPIV.

Telephony Manager 3.1 supports the following systems and components:

- Meridian ITG Trunk 2.0 to 2.2 (Telephony Manager Services/ ITG ISDN IP Trunks application)
- Meridian IP Trunk 3.0/3.01 (Telephony Manager Services/ ITG ISDN IP Trunks application)

- Meridian ITG Line 1.0 (Telephony Manager Services/ ITG IP Telecommuter/Wireless IP Gateway application)
- Meridian ITG Line 2.0 to 2.2 (Telephony Manager Services/ ITG IP Phones application)
- Meridian IP Line 3.0, 3.1, 4.X, and 5.0 (Telephony Manager Services/ Telephony)
- MDECT (DMC8 card, and DMC4 with updated loadware)
- Meridian 802.11 Wireless IP Gateway (Telephony Manager Services/ ITG IP Telecommuter/Wireless IP Gateway application)

Telephony Manager 3.1 concurrence follows the life cycle plans of the Meridian 1 and CS 1000 systems and components with which it interworks. Some CPU/X11 release/system configurations that have reached their end-of-life cycle, and thus are not supported by Nortel, are also not supported by Telephony Manager 3.1.

Supported upgrade paths

Telephony Manager supports a one-step direct upgrade from OTM 2.2 or Telephony Manager 3.0 to Telephony Manager 3.1. An upgrade from OTM 2.2 to Telephony Manager 3.1 will take longer because it also involves the migration of the database.

Direct upgrades are not supported for customers migrating from OTM releases prior to 2.2. A two-step upgrade is required, first to OTM 2.2 and then to Telephony Manager 3.1. Refer to *Telephony Manager 3.0 Installation and Configuration (553-3001-230)* for details of the upgrade from OTM 2.2 to Telephony Manager 3.0.

Telephony Manager 3.1 server and clients overview

Telephony Manager 3.1 supports both Web and Windows® clients. The Windows GUI interface has different functionality than the Web browser interface. The Windows GUI interface can be used directly on the Telephony Manager 3.1 server, or on an Telephony Manager 3.1 Windows® client.

The Telephony Manager 3.1 client accesses and modifies data that is stored on the Telephony Manager 3.1 server. This data is made available by sharing the Telephony Manager 3.1 folder on the Telephony Manager 3.1 server with all Telephony Manager 3.1 clients. Due to the large amounts of data transferred between the Telephony Manager 3.1 server and the Telephony Manager 3.1 clients, high network bandwidth is consumed. Response time and performance degrade significantly unless the Telephony Manager 3.1 client and Telephony Manager 3.1 server are on the same LAN. In general, a WAN connection is not suitable. Consult [Appendix "Telephony Manager 3.1 engineering guidelines" \(page 257\)](#) in this

document for further details on bandwidth and other network requirements for the Telephony Manager 3.1 client communicating with the Telephony Manager 3.1 server. The appendix also provides information about the different network configurations that are possible.

The Web clients operate as thin clients connecting directly to a Web server running on the Telephony Manager 3.1 server. All operations performed using a Web client are executed on the Telephony Manager 3.1 server. The Telephony Manager 3.1 server requires connectivity to the ELAN subnets of the systems managed.

Telephony Manager Windows and Web client require that an administrator account is logged onto the server at all times, because the server uses the identity of the logged-in user for access. To allow Telephony Manager 3.1 client access without logging in to the server at all times, see [Procedure 69 "Allowing Telephony Manager 3.1 client access without constant server log on \(optional\)" \(page 246\)](#) for Windows 2000 Server and Windows Server 2003.

A typical client-server architecture

The Telephony Manager 3.1 client is a thick client that runs on a Windows PC. It does not operate in a traditional client-server model. Rather, the Telephony Manager 3.1 client runs similar software to that running on the Telephony Manager 3.1 server. The Telephony Manager 3.1 client communicates directly with the managed systems, and therefore:

- requires connectivity to the ELAN subnets of those systems
- must be operational at the time any operations performed on the client are scheduled to run
- if a site or system defines a serial profile for Station Admin, physical serial connections must be present between the switch and the server, and between the switch and the client PCs. Communications profiles are defined on a site/system basis and are shared by a server and its clients.

Telephony Manager 3.1 hardware requirements

Refer to [Appendix "Telephony Manager 3.1 engineering guidelines" \(page 257\)](#) for more information about Telephony Manager 3.1 hardware requirements.

Use correct information

The information in this document is subject to change. For the latest system requirements, see the Telephony Manager 3.1 General Release Bulletin.

Ask the network card manufacturer about the type of network card and the availability of the required software driver.

Response-time testing is based upon and supported on the minimum configuration as listed in [Table 2 "Telephony Manager 3.1 hardware requirements" \(page 34\)](#).

For a Windows client some variables are:

- amount of RAM on the Telephony Manager 3.1 client PC
- the Operating System (OS) on the Telephony Manager 3.1 client PC
- number of TNs managed through the Station Administration application
- other applications that can run on the Telephony Manager 3.1 client PC, including those that run in the background, such as antivirus software
- amount of traffic on the LAN
- NIC on the Telephony Manager 3.1 client PC
- deployment in the network architecture (topology and placement of the Telephony Manager 3.1 client PC with respect to the Telephony Manager 3.1 server)

The minimum and recommended CPU and RAM configurations are specified. Some Telephony Manager 3.1 applications can run with less than the recommended configurations, but performance can be degraded.

The Telephony Manager 3.1 server requires the following minimum hardware specifications listed in [Table 2 "Telephony Manager 3.1 hardware requirements" \(page 34\)](#).

Table 2
Telephony Manager 3.1 hardware requirements

Requirement	Server configuration	Single (stand-alone) configuration	Client configuration
Minimum CPU - See Note 1	Intel Pentium IV Processor 2 GHz	Intel Pentium IV Processor 1 GHz	Intel Pentium III Processor 600 MHz
Minimum RAM	1 GB	1 GB	512 MB
Minimum Hard Drive Space (May increase depending on number of telephones)	2 GB (1 GB plus customer data storage)	2 GB (1 GB plus customer data storage)	500 MB
Custom Help	512 MB	512 MB	512 MB
Web Help (all languages - excluding custom help)	400 MB	400 MB	400 MB
SVGA Color Monitor and interface card	1024x768 or higher resolution	1024x768 or higher resolution	1024x768 or higher resolution

Requirement	Server configuration	Single (stand-alone) configuration	Client configuration
3 1/2-inch 1.44 MB floppy disk drive	Required	Required	Required
CD-ROM drive	Required	Required	Required
Ethernet Network Interface Card - See Note 2	1 or 2	1	1
Hayes- compatible modem is optional for connection to remote sites, required for polling configurations. Please note: WinModems are incompatible and are not supported.	56K BPS recommended	56K BPS recommended	56K BPS recommended
PC com port with 16550 UART is required. USB serial adapters and USB modems are not supported.	Required	Required	Required
PC COM port with 16550 UART - See Note 3	Required	Required	Required
Parallel Port Dongle or USB dongle	Required	Required	Not required
	Supports one USB dongle only	Supports one USB dongle only	
	USB dongles are not supported through a USB hub	USB dongles are not supported through a USB hub	
Parallel printer port (configured) or USB port (required for dongle)	Required	Required	Required
Two-button Windows-compatible mouse or positioning	Required	Required	Required
Note 1: Telephony Manager 3.1 is supported on Intel Xeon CPU or Hyper-threading configurations.			

Requirement	Server configuration	Single (stand-alone) configuration	Client configuration
Note 2: An Ethernet Network Interface Card is required to support connection with the Meridian 1 using Ethernet. A second Ethernet Network Interface Card is optional depending on configuration.			
Note 3: For external modems or direct connection, the PC must have an available serial port (that is, one not used by a mouse or other serial device). The number of on-board PC COM ports required depends on the number of external modems or direct connections required.			

Telephony Manager 3.1 software requirements

Novell

The Telephony Manager 3.1 server is not supported on a Novell server. TCP/IP communication is supported. IPX/SPX communication is not supported.

General restrictions

The following general restrictions apply to Telephony Manager 3.1:

- The user is responsible to ensure that selection of **Signaling server present** check box is completed. Telephony Manager 3.1 cannot automatically determine if a system has a signaling server.
- For CS 1000M Cabinet and CS 1000M Chassis systems, both appear in Telephony Manager 3.1 as a Communication Server 1000M Cabinet/Chassis. Existing fields are used to differentiate the hardware. The user can:
 - name the system to reflect the hardware when adding the system
 - add information into the comments field to describe the hardware
- The Meridian 1 PBX 11C Chassis (Option 11C Mini) system appears in Telephony Manager 3.1 as a Meridian 1 PBX 11C Cabinet (Option 11C) system after the update system data operation. It is the user's responsibility to select the proper machine type in the system properties page.
- In the **System Data** tab, those systems with **Signaling server present** (that is **Signaling server present** checkbox in Network Tab is selected) cannot be downgraded to non-CS 1000 software releases, for example, X11 Release 25.37. The applicable releases displayed in the release combo box is based on the Machine Type and for the CS 1000 machine types only CS 1000 releases are applicable.
- The **Signaling server present** check box must be cleared to downgrade the system to non-CS 1000 software releases.
- If a Meridian 1 system running CS 1000 Release 4.0 in Telephony Manager 3.1 Navigator connects to a system running X11 release

software, the non-applicable associated hardware is deleted, and a message for each deleted hardware (Survivable Cabinet and Media Gateways 1000B) is logged in the Event Log.

Multisession is not supported. Two users cannot be concurrently logged into the same PC at the same time and have Telephony Manager 3.1 running.

Operating System and application requirements for Telephony Manager 3.1 PC configurations

Table 3 "Telephony Manager 3.1 configuration OS requirements" (page 37), Table 4 "OS Service Packs" (page 38), Table 6 "Application software requirements" (page 38), and Table 7 "Third-party software requirements" (page 40) list the required and supported software that run on Telephony Manager 3.1 PC configuration types.

Table 3
Telephony Manager 3.1 configuration OS requirements

Telephony Manager 3.1 PC Configuration				
Supported OS software	Telephony Manager 3.1 as a server (supporting Telephony Manager 3.1 Windows clients)	Telephony Manager 3.1 as a stand-alone (supporting no Telephony Manager 3.1 Windows client)	Telephony Manager 3.1 as a Windows client	Telephony Manager 3.1 Web clients
Windows Server 2003, Enterprise Edition	Yes (only supported in a non-clustered environment)	Yes (only supported in a non-clustered environment)	No	Yes
Windows Server 2003, Standard Edition	Yes	Yes	No	Yes
Windows 2000 Server	Yes	Yes	No	Yes
Windows XP Professional	No	Yes	Yes	Yes
Windows 2000 Professional	No	Yes	Yes	Yes

Telephony Manager 3.1 cannot be installed on Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000 Advanced Server, or Datacenter Server. For Windows Server 2000, only the Standard Edition is supported. For Windows Server 2003, only the Standard Edition and the Enterprise Edition are supported.

Windows Server 2003 R2 is not supported. Refer to Product Bulletin *Windows Server 2003 R2 Support on TM 3.0 (P-2006-0260-Global-Rev1)* for details.

Table 4
OS Service Packs

OS software	OS PC service packs
Windows Server 2003, Enterprise Edition	SP1 or SP2
Windows Server 2003, Standard Edition	SP1 or SP2
Windows 2000 Server	SP4
Windows XP Professional	SP2
Windows 2000 Professional	SP4

Table 5
Web browser support

OS	Web browser
Windows Server 2003	IE 6.0 + SP1 IE 7.0
Windows 2000 Server	IE 6.0 + SP1
Windows XP Professional	IE 6.0 + SP2 IE 7.0
Windows 2000 Professional	IE 6.0 + SP1

Table 6
Application software requirements

Telephony Manager 3.1 PC configuration			
Application software	Server	Single (stand-alone)	Windows client
Internet Explorer 6.0 SP1 (Windows only)	Minimum Required	Minimum Required	Minimum Required
TCP/IP Protocol	Required	Required	Required
RAS (Remote Access Service)	Required	Required	Required
Java 1.5.0_02 run time environment	Required	Required	Required

Telephony Manager 3.1 PC configuration			
Application software	Server	Single (stand-alone)	Windows client
Microsoft Active server Page (ASP)	Required	Required	n/a
IIS WWW Publishing Service	Required	Required	n/a
Microsoft Windows Script 5.6	Required	Required	Required
IIS FTP Service	Required	Required	n/a
ATTENTION Nortel does not recommend running more than one Web client from Windows 2000 Professional or Windows XP Professional standalone platforms.			

Regional Operating System support

The Windows 2000 Server and Windows Server 2003 Operating Systems (OS) are supported for the following languages:

- Japanese
- Simplified Chinese

The Windows 2000 Professional and Windows® XP Professional clients are supported for the following languages:

- Spanish
- French
- German
- Brazilian Portuguese
- Japanese
- Simplified Chinese

Third-party software requirements

Table 7 "Third-party software requirements" (page 40) lists the third party software or firmware included as part of the Telephony Manager 3.1 application.

Table 7
Third-party software requirements

	Software and version	Comments
1	MDAC & Jet Engine 4.0 SP7	MDAC is included in all the supported platforms.
2	Crystal Reports 10.0 Runtime	
3	JRE 1.5	
4	MsXML 4.0 SP2	Telephony Manager 3.1 uses version 4.0 with Service Pack 2 which is supported on Windows 2000 and XP. It is the latest version available
5	Sentinel Driver 5.41 used for dongle support.	This version is supported on Windows 2000 and XP.
6	Netscape Directory SDK version 5.0 for Telephony Manager CND services and SDK version 5.0 for SSL connection.	
7	Windows Installer 2.0	This is used before we install Telephony Manager on a freshly formatted PC. This is the latest version and it is installed for Windows 2000. It is not installed for Windows XP since it is included with the OS.
8	ARL (for SNMP) Version 15.3	The Asynchronous Request Library (ARL) provides an API for building SNMP manager applications or for integrating SNMP manager capabilities into an existing application. ARL is the SNMP stack for Telephony Manager 3.1 (for all applications).
9	Microsoft Access 97/2000 Runtime	
10	PostgreSQL 8.1	PostgreSQL 8.1 is an open source SQL based relational database. This is Telephony Manager's telephone database back end.
11	Apache Tomcat 5.5	Apache Tomcat 5.5 is an open source Web Server required to deliver JSP pages, the technology used for Telephony Manager pages.

System software release and package requirements

Table 8 "Meridian 1 X11 system software release and packages" (page 41) lists Telephony Manager 3.1 software releases and required packages for Telephony Manager 3.1 applications.

Table 8
Meridian 1 X11 system software release and packages

Telephony Manager 3.1 application	X11 pkgs required
Alarm Management	Pkg 164, 242, 243, and 296
Additional packages for Alarm Notification	Pkg 55 and 315
Maintenance Windows	Pkg 164, 242, 243, and 296
System Terminal - Overlay Passthru	Pkg 164, 242, and 296
Ethernet connection (for Station Administration, Traffic Analysis, and ESN ART)	Pkg 164, 242, and 296
SNMP Alarms (Open Alarms)	Pkg 315
Data Buffering and Access - Ethernet	Pkg 351
Data Buffering and Access - Serial	N/A
Database Disaster Recovery	Pkg 164, 242, 296, and 351
Virtual Terminal server	Pkg 164, 242, and 296
Emergency Service for Client Mobility	Pkg 336 and 337

Table 9 "CS 1000 and Meridian 1 software requirements" (page 41) lists CS 1000 and Meridian 1 software requirements.

Table 9
CS 1000 and Meridian 1 software requirements

Telephony Manager 3.1 Functionality	Connection Type ¹
Alarm Management	Ethernet/PPP
System Terminal	Ethernet/PPP
ESN Art	Ethernet/PPP/Serial
Traffic Analysis	Ethernet/Serial ²
Telecom Billing System (TBS)	Serial Ethernet (DBA)
Call Tracking	Serial
Web Alarm Viewing	Ethernet/PPP
Virtual Terminal server	Ethernet/Serial ³
Maintenance Pages/Inventory	Ethernet/PPP
Telephone Manager/List Manager	Ethernet/Serial
Access server	Ethernet/PPP/Serial
DECT	Ethernet/PPP

1. Ethernet and PPP connections require the MAT Management Interface software package 296.
For version 4.5 and beyond, **unsecure shells must be enabled**.

Telephony Manager 3.1 Functionality	Connection Type ¹
2. If traffic is collected through a buffer box, only a serial connection is supported.	
3. Only direct serial connections are supported. Modems are not supported.	

Installing Telephony Manager 3.1 server software

Contents

This chapter contains information about the following topics:

["Overview" \(page 43\)](#)

["Installation program features" \(page 44\)](#)

["Installing Telephony Manager 3.1 software" \(page 47\)](#)

Overview

This chapter contains information about:

- Installation program features and restrictions
- Troubleshooting
- Installation of new Telephony Manager 3.1 servers

An installation checklist is provided. [Appendix "Installation checklist" \(page 297\)](#).



CAUTION

Installing Telephony Manager from the desktop or from a folder that has a longer path name will cause unexpected error messages during the Telephony Manager Server or Telephony Manager Client installation.

To install the program from a hard drive instead of from a CD, create a folder in the root of the drive and name it "CD". Copy the contents of the CD or unzip the files from the archive into this folder. Run the installation program.

Web Help

Web Help can be installed at the same time as the Telephony Manager 3.1 software installation; however the Web Help installation is time consuming. The user can install only the Telephony Manager 3.1 software first, and then run setup again in Maintenance Mode to install WebHelp later (see ["Maintenance mode" \(page 57\)](#)).

Installation program features

Telephony Manager 3.1 server (standalone) software installation uses the standard Windows® installation wizard.

Users and groups

During the installation process, Telephony Manager 3.1 adds the Default, EndUser, and HelpDesk user groups to the server. User groups cannot have the same name as a local user on the Telephony Manager 3.1 server. If the installation program detects a local user with the same name as one of the user groups that it is attempting to add, you are given the option of renaming or deleting the local user or canceling the creation of the user group.



CAUTION

Service Interruption

Telephony Manager 3.1 is not supported on a Windows Server system that is configured as a Primary Domain Controller (PDC). DO NOT install Telephony Manager 3.1 on a PDC.

Checking local security settings

Ensure the Users group has the **access this computer from network** and **log on locally** policies set before the Telephony Manager 3.1 installation is started.

This can be checked and changed using the following procedure.

ATTENTION

If Telephony Manager 3.1 is to be installed on a computer that is within a domain, you must check the policies on the primary Domain Controller. In such cases, contact your domain administrator to set the required policies. Insufficient permissions results in PostgreSQL error during installation, and the only means of recovery is to uninstall Telephony Manager and reinstall Telephony Manager again with the proper permissions.

Procedure 1

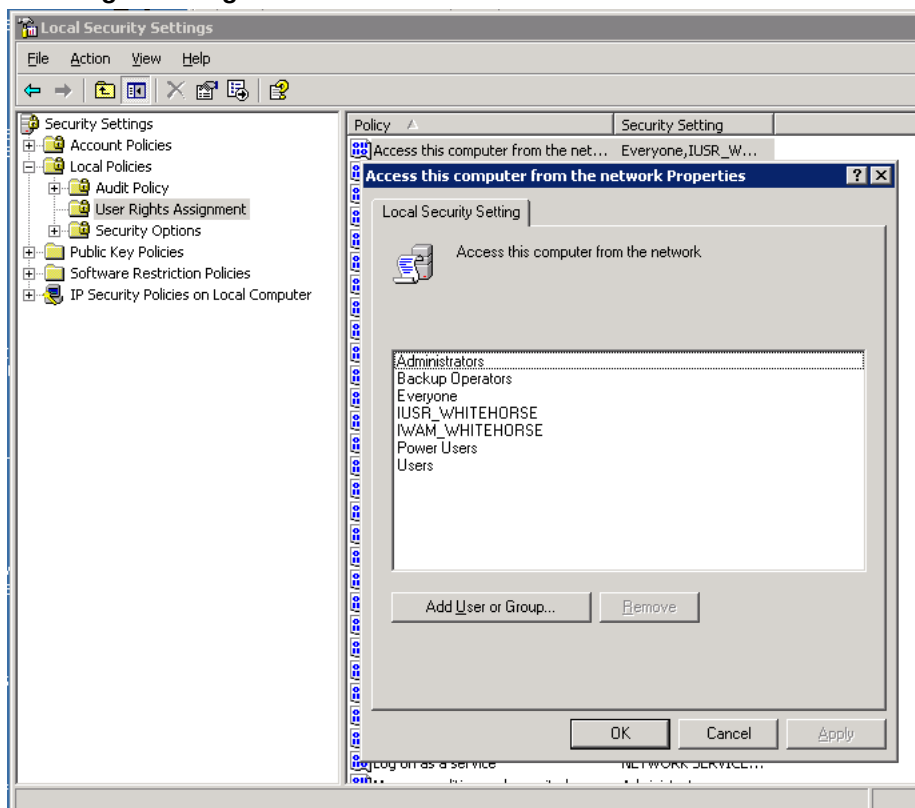
Checking local security settings

Step	Action
------	--------

- | | |
|---|---|
| 1 | From the Administrative Tools window, launch the Local Security Settings.

The Local Security Settings window appears, as shown in Figure 1 "User Rights Assignment" (page 45). |
| 2 | Select the Local Policies > User Rights Assignment . |
| 3 | Double-click the policies Log on as a Service and Access this computer from the network . Ensure the Users group is present. If it is not, add Users to the policy. |

Figure 1
User Rights Assignment

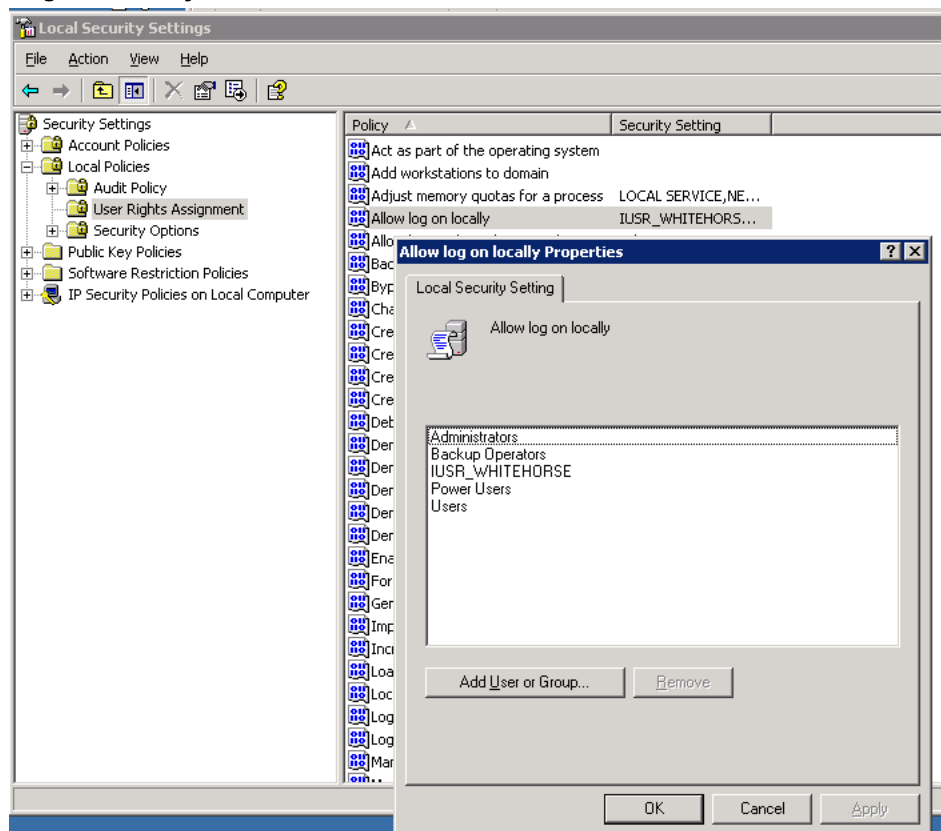


- | | |
|---|--|
| 4 | Double-click the policy Log on locally .

See Figure 2 "Log on Locally" (page 46) The Users group should be granted this policy.

For Windows Server 2003, the policy name is Allow log on locally . |
|---|--|

Figure 2
Log on Locally



—End—

If the computer is within a domain, the policy settings of the domain can override the local security policies. The following are possible workarounds so the user can install PostgreSQL. If these solutions do not work, it is possible the problem may be specific to the particular domain, and Nortel recommends that you contact your domain administrator.

Procedure 2

Workarounds for installation of PostgreSQL

Step	Action
1	Log off the domain.
2	Log on to the PC as the local administrator.
3	Check the policies prior to installing Telephony Manager.

- 4 Move the PC out of the domain.
- 5 Check the policies prior to installing Telephony Manager.
- 6 Move the PC back into the domain.

—End—

Installing Telephony Manager 3.1 software

The following procedure will install the Telephony Manager 3.1 software.

ATTENTION

CND 2.1 is a mandatory requirement to ensure the proper functioning of Telephony Manager 3.1.

If a previous version of CND already exists on your server or network, follow the instruction in the CND 2.1 Administration Guide to upgrade your CND.

The Telephony Manager installation setup contains a folder with the CND setup & installation files. The file is **<TM_Installation_Setup_Root_Directory>\CND\Setup.exe**.

When the CND is installed on the same server as Telephony Manager (either after or before the Telephony Manager installation) to store database information, it must be installed **separately**. When the CND is installed on another server, Telephony Manager can connect with the CND via the network.

For detailed information about installing and synchronizing the CND, see *Telephony Manager 3.1 System Administration (NN43050-601)* and the *Common Network Directory 2.1 Administration Guide (NN43050-101)*.

Procedure 3

Installing Telephony Manager 3.1 software

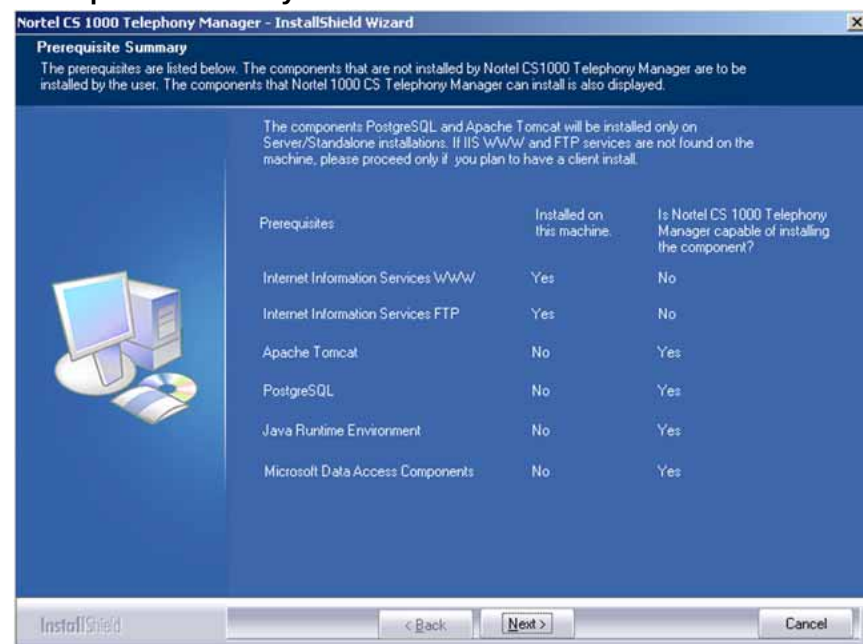
Step	Action
1	Configure the Windows® OS for Telephony Manager 3.1 installation by completing the following steps: a. Log on to Windows as Administrator. b. Exit all Windows programs. c. Install security patches as advised through Product Bulletins available on the Partner Information Center Web site.
2	Double-click Setup.exe on the Telephony Manager 3.1 CD-ROM. Click Next .

The following prerequisites are checked:

- if the operating system is supported by Telephony Manager 3.1
- if the PC has the appropriate software components installed (for details, see "Preparing for installation" (page 29)).

The Prerequisite Summary page appears [Figure 3 "Prerequisite Summary" \(page 48\)](#), listing the mandatory software components needed to continue installation.

Figure 3
Prerequisite Summary



If a prerequisite component that Telephony Manager cannot install is unavailable on the computer, the following message is displayed:

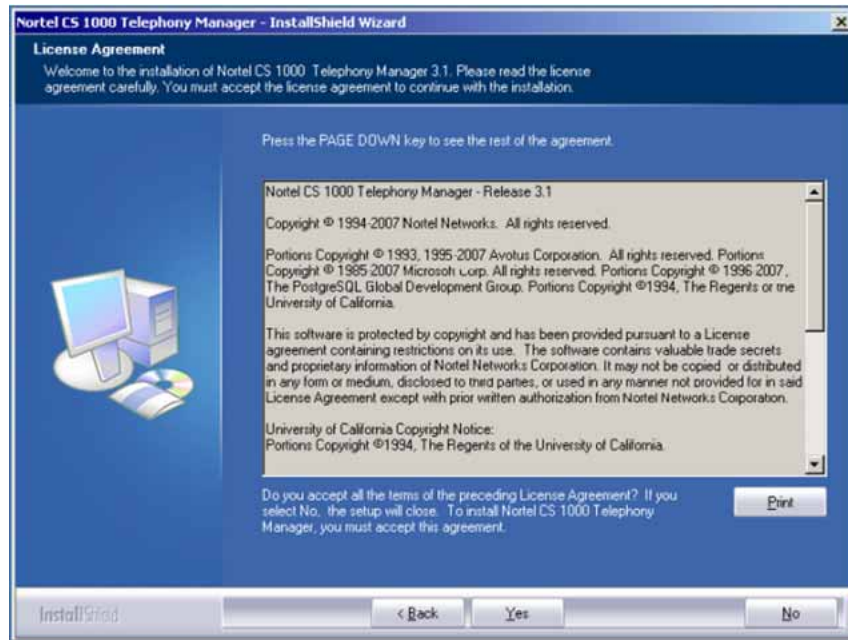
Figure 4
Prerequisite uninstalled components message



3 Click **Next** to continue.

- 4 The Welcome and Licence Agreement window appears (see [Figure 5 "Welcome and License Agreement window" \(page 49\)](#)). Read the Licence Agreement and click **Yes** to accept and continue.

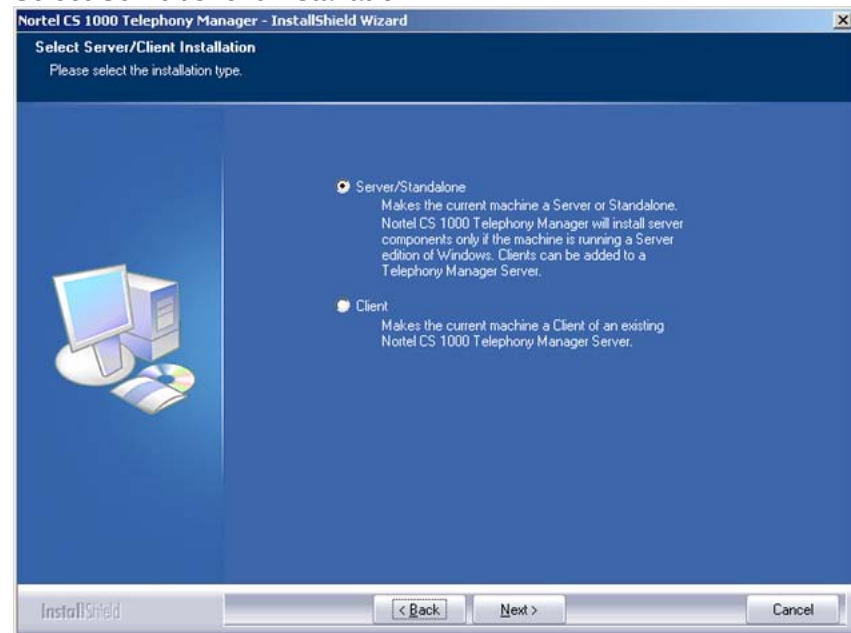
Figure 5
Welcome and License Agreement window



- 5 The Server/Client installation selection page appears (See [Figure 6 "Select Server/Client Installation" \(page 50\)](#)). Select **Server/Standalone** and click **Next**. If all prerequisites are not met, installation cannot continue beyond this point. Some prerequisites are automatically installed by Telephony Manager 3.1.

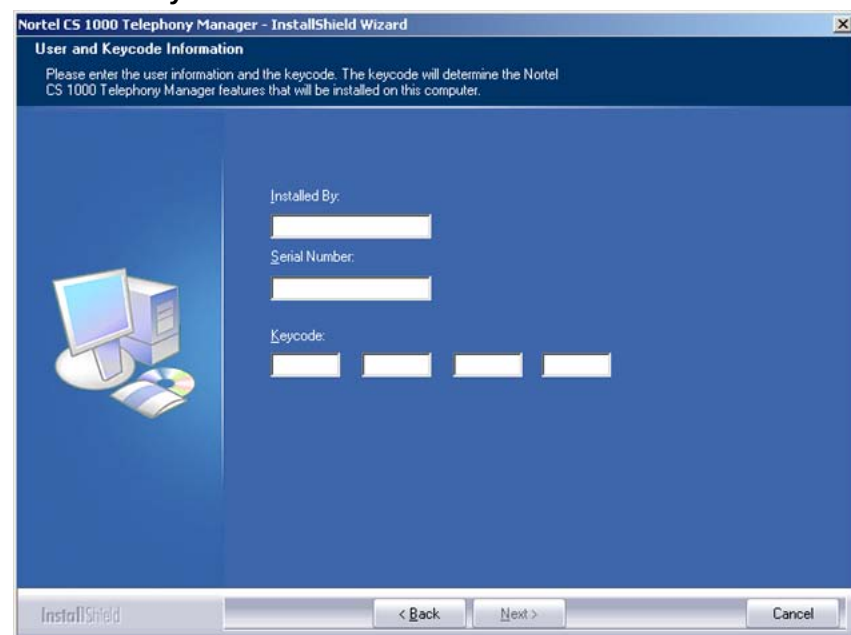
Note that installation types cannot be changed for upgrades. It is preselected based on the existing installation.

Figure 6
Select Server/Client Installation



- 6 The User and Keycode information screen appears (see [Figure 7 "User and Keycode Information"](#) (page 50)).

Figure 7
User and Keycode Information



Enter the user information and keycode. Click **Next** to continue.

At this point the installation decides which applications to install based on the keycode entered. If the keycode is invalid, an error message appears (see [Figure 8 "Invalid keycode error" \(page 51\)](#)).

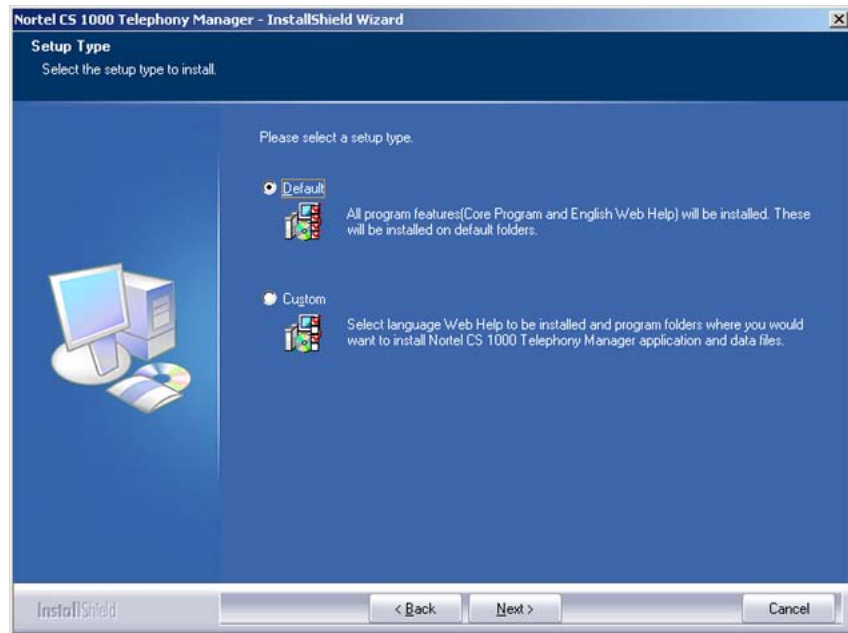
There are no restrictions on the number of keycode entry attempts.

Figure 8
Invalid keycode error



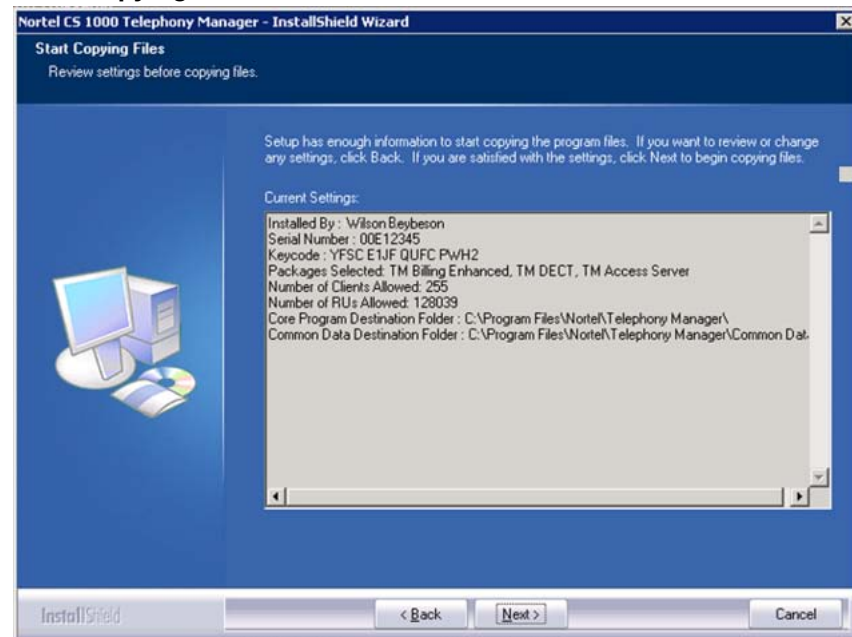
- 7 The Setup Type page screen appears ([Figure 9 "Setup Type" \(page 51\)](#)), providing a choice of either default or custom installation options.

Figure 9
Setup Type



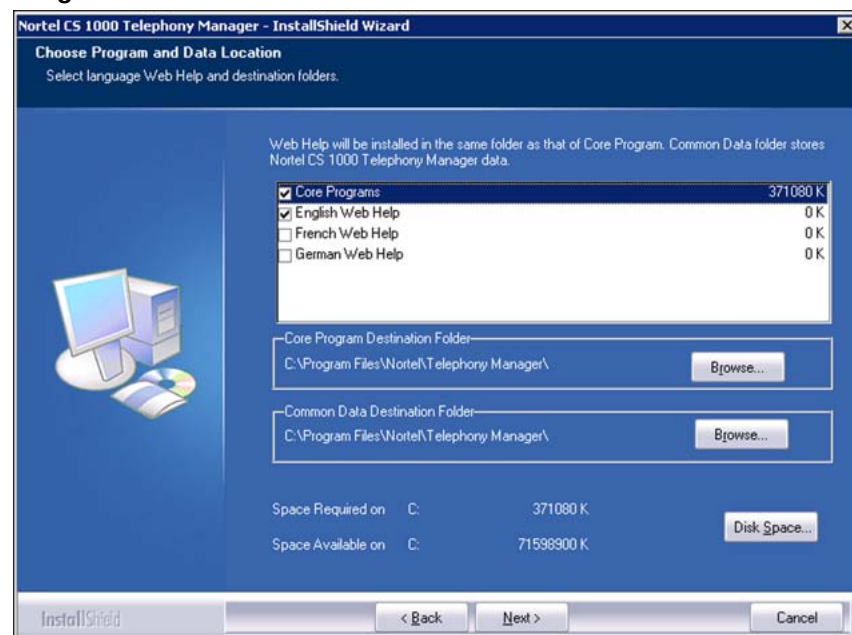
If **Default** is selected and **Next** is clicked, the Start Copying Files screen appears ([Figure 10 "Start Copying Files screen" \(page 52\)](#)) which provides a summary of the installation which can be reviewed.

Figure 10
Start Copying Files screen



If **Custom** is selected and **Next** is clicked, the Choose Program and Data Location screen appears (Figure 11 "Program and Data Location" (page 52)).

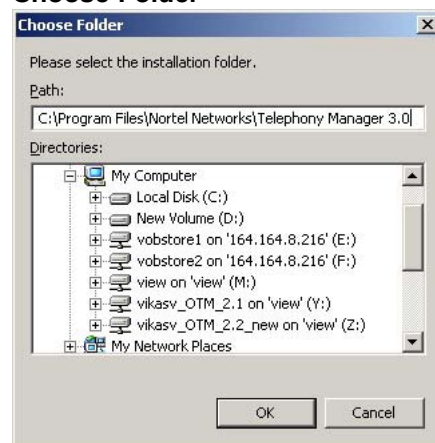
Figure 11
Program and Data Location



The Choose Program and Data Location screen lists the features to be installed on the PC. The list includes:

- Core Program. This cannot be deselected by the user. However, the folder selection option displayed within the Core Program Destination Folder group box allows the user to select the destination folder where the Core Program is to be installed. Web Help files and Local Data are also installed in this folder.
- English Web Help. Installs the English Web Help files. These are installed in the default folder or the folder selected for Core Program.
- French Web Help. Installs the French Web Help files. These are installed in the default folder or the folder selected for Core Program.
- German Web Help. Installs the German Web Help files. These are installed in the default folder or the folder selected for Core Program.
- Core Program Destination Folder Browse button allows the user to select the folder where the Core Program files are to be installed.
- Common Data Destination Folder Browse button allows the user to select the destination folder for the Common Data.
- Clicking either Browse button displays the Choose Folder dialog box (see [Figure 12 "Choose Folder" \(page 53\)](#)).

Figure 12
Choose Folder



8 Specify a destination directory and click **OK**.

ATTENTION

You must not install Telephony Manager 3.1 in the root directory (for example, C:\). During the installation process, you must specify a folder (for example, C:\Nortel).

- 9 Clicking the Disk Space button in [Figure 11 "Program and Data Location" \(page 52\)](#) displays the Available Disk Space dialog box (see [Figure 13 "Available Disk Space" \(page 54\)](#)), showing the available disk space in each of the drives on the PC.

If the selected drive doesn't have enough disk space to accommodate the selected options, an error message appears asking the user to select another drive.

Figure 13
Available Disk Space



Click **OK**.

- 10 The Installation Summary screen appears (See [Figure 14 "Installation Summary" \(page 55\)](#)), listing the options chosen during the installation. To change settings, there are two choices:
- Click **Back** to return to the previous screen
 - Click **Next** to begin the Installation process. The Setup Status screen appears. (See [Figure 15 "Setup Status" \(page 55\)](#)).

Figure 14
Installation Summary

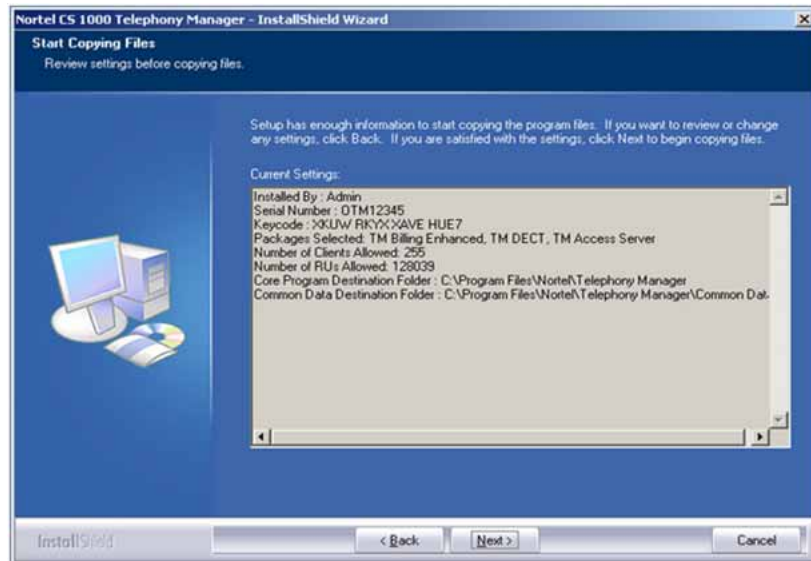
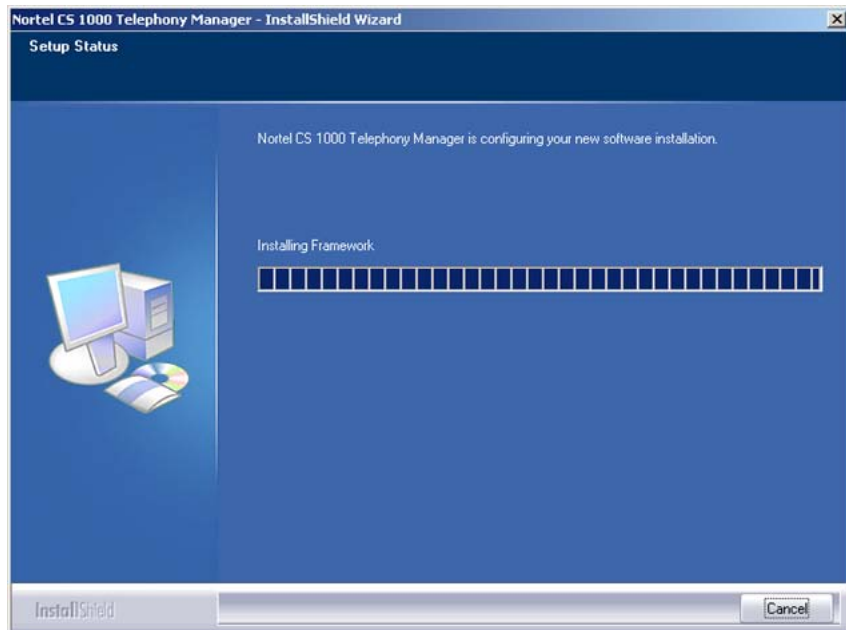


Figure 15
Setup Status



- 11** If **Cancel** is clicked at any time during the installation, the Exit Setup dialog box (Figure 16 "Exit Setup" (page 56)) prompts for confirmation before terminating and rolling back the installation. If **Yes** is clicked (see Figure 17 "Install interrupted" (page 56)), the

system is restored to its original state. If **No** is clicked, the installation continues.

Figure 16
Exit Setup

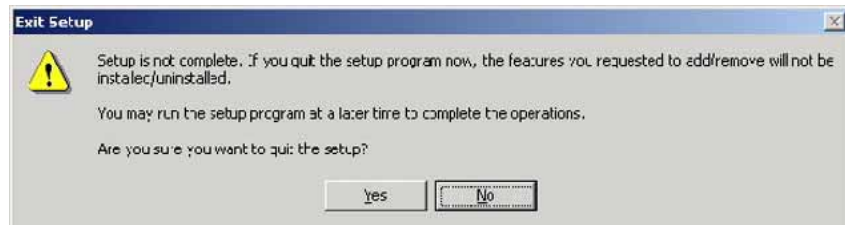
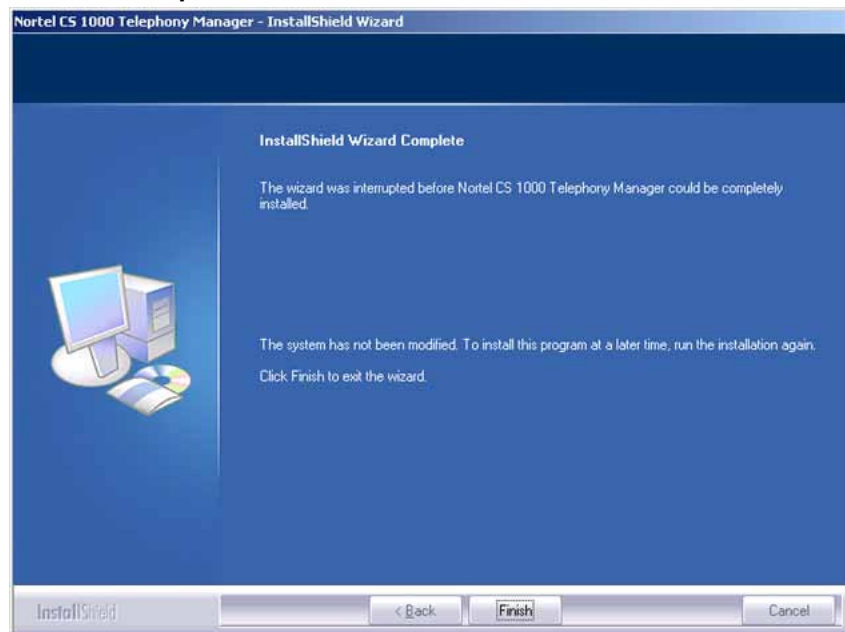
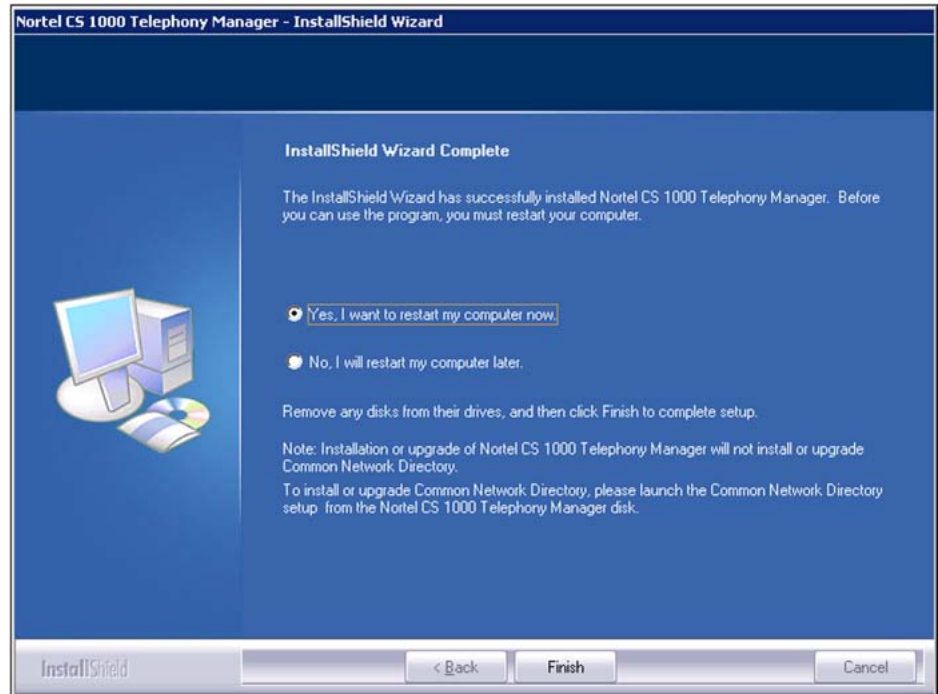


Figure 17
Install interrupted



- 12 Upon completion, the installation Wizard Complete screen appears, prompting the installer to restart the PC now or at a later time. See [Figure 18 "Installation Wizard Complete" \(page 57\)](#).

Figure 18
Installation Wizard Complete



- 13** Click **Finish** to restart the computer.

Once the computer restarts, the installation finishes, and the Telephony Manager logon screen appears.

ATTENTION

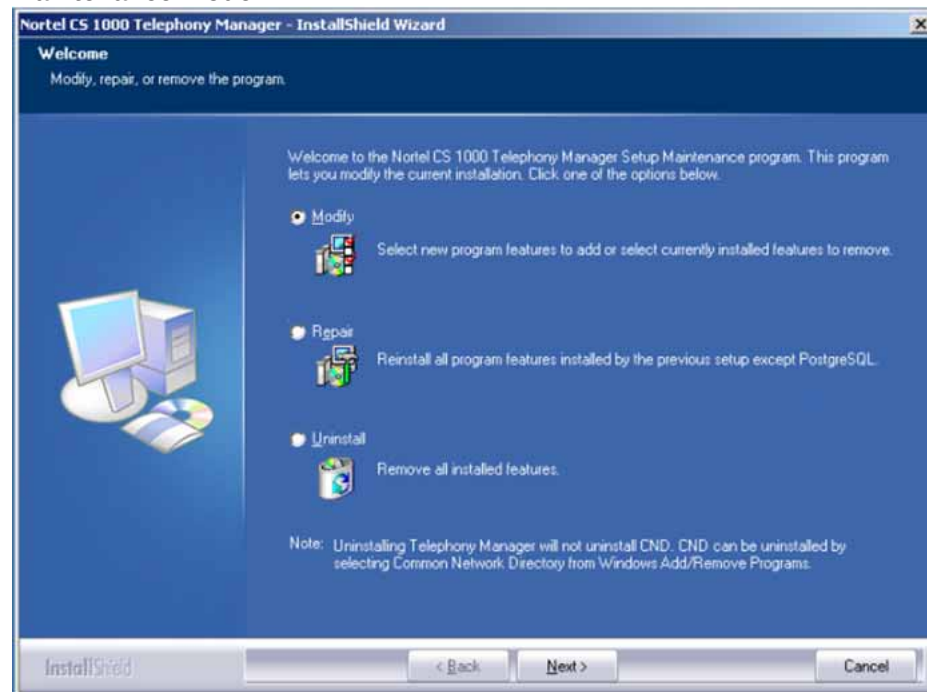
User may see HTTP 400 error on attempting to log on to Web Navigator after performing an upgrade from one TM version to another, due to issues related to Tomcat. Performing a Repair operation on Telephony Manager will resolve the HTTP 400 error.

—End—

Maintenance mode

With Telephony Manager 3.1 successfully installed, run Setup.exe from the installation CD ROM to enter the InstallShield Wizard Maintenance mode (see [Figure 19 "Maintenance mode" \(page 58\)](#)). Telephony Manager 3.1 can also be uninstalled by using the Add/Remove Programs window. For details, see ["Uninstall using Add/Remove Programs" \(page 241\)](#).

Figure 19
Maintenance mode



Maintenance mode provides the following options:

- **Modify:** The Modify option lets the user perform install and uninstall of Telephony Manager 3.1 components such as Web Help.
- **Repair:** The Repair option performs a reinstall of the existing installation, overwriting the existing installation's application files without modifying the data files.

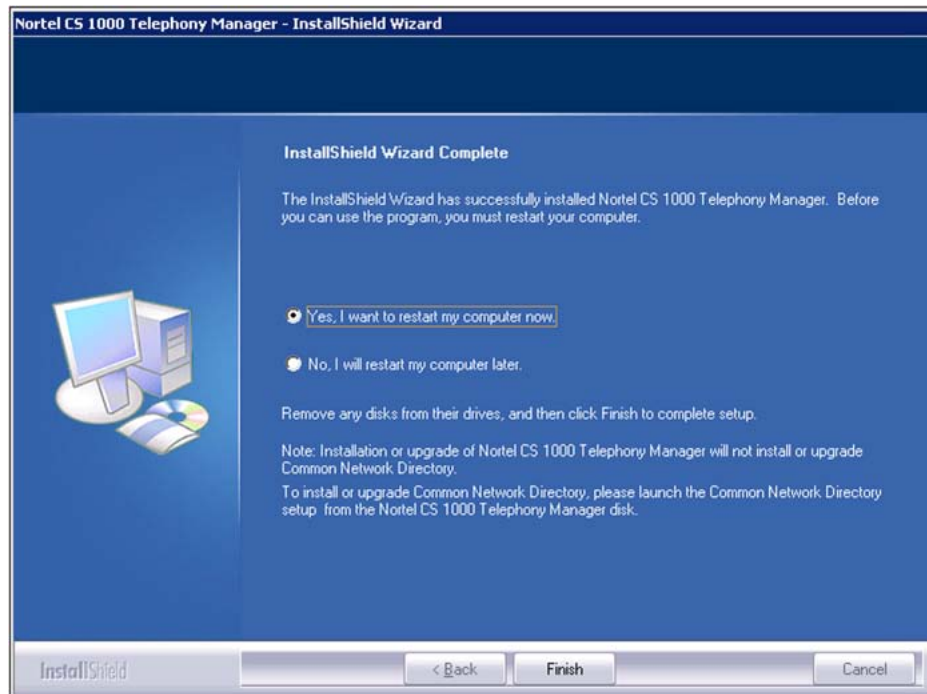
ATTENTION

The Repair option of Telephony Manager does not repair PostgreSQL.

- **Uninstall:** The Uninstall option performs an uninstall of the Telephony Manager 3.1 installation. A warning is issued and the user is prompted to proceed. Upon completion, the Uninstall Complete window appears. For more information about uninstalling Telephony Manager 3.1, see [Figure 138 "Telephony Manager InstallShield wizard" \(page 238\)](#).

Upon completion of the selected Maintenance operation, the Maintenance Complete window appears (see [Figure 20 "Maintenance Complete" \(page 59\)](#)),

Figure 20
Maintenance Complete



Installing Telephony Manager 3.1 client software

Contents

This chapter contains information about the following topics:

["Overview" \(page 61\)](#)

["Installing the client software" \(page 64\)](#)

Overview

This chapter contains information about installing Telephony Manager 3.1 client software.

Telephony Manager 3.1 client software installation is similar to the Telephony Manager 3.1 server installation. The steps are summarized in this chapter.



CAUTION

Installing Telephony Manager from the desktop or from a folder that has a longer path name will cause unexpected error messages during the Telephony Manager Server or Telephony Manager Client installation.

To install the program from a hard drive instead of from a CD, create a folder in the root of the drive and name it "CD". Copy the contents of the CD or unzip the files from the archive into this folder. Run the installation program.

Telephony Manager 3.1 server and client overview

Telephony Manager 3.1 supports both Web and Windows clients. The Windows GUI interface has different functionality than the Web browser interface. The Windows GUI interface can be used directly on the Telephony Manager 3.1 server, or on an Telephony Manager 3.1 Windows client.

The Web clients operate as thin clients connecting directly to a Web server running on the Telephony Manager 3.1 server. All operations performed using a Web client are executed on the Telephony Manager 3.1 server. The Telephony Manager 3.1 server requires connectivity to the ELAN subnets of the systems managed.

The Telephony Manager 3.1 client is a thick client that runs on a Windows PC. It does not operate in a traditional client-server model. Rather, the Telephony Manager 3.1 client runs similar software to that running on the Telephony Manager 3.1 server. The Telephony Manager 3.1 client communicates directly with the managed systems, and therefore requires connectivity to the ELAN subnets of those systems. The Telephony Manager 3.1 client must be operational at the time any operations performed on the client are scheduled to run.

The Telephony Manager 3.1 client accesses and modifies data that is stored on the Telephony Manager 3.1 server. This data is made available by sharing the Telephony Manager 3.1 folder on the Telephony Manager 3.1 server with all Telephony Manager 3.1 clients. Due to the large amounts of data transferred between the Telephony Manager 3.1 server and the Telephony Manager 3.1 clients, high network bandwidth is consumed. Response time and performance degrade significantly unless the Telephony Manager 3.1 client and Telephony Manager 3.1 server are on the same LAN. In general a WAN connection is not suitable.

Consult the Engineering Guidelines in [Appendix "Telephony Manager 3.1 engineering guidelines" \(page 257\)](#) in this document for further details on bandwidth and other network requirements for the Telephony Manager 3.1 client communicating with the Telephony Manager 3.1 server. The appendix also provides information about the different network configurations that are possible.

Windows XP client install and mapped drives

After a Telephony Manager client installation reboot, files are copied from the server. Windows XP does not save the logon account information of a mapped drive. If the mapped drive is unavailable, this operation fails and causes logon problems, which can be avoided in the following 2 ways:

- Ensure the account used to map the drive is the same account (same logon id and password) used to logon to the client PC for installation. In other words, the logon id and password for accessing both Server and Client machines must be the same.
 - If **administrator** is the logon id to map the drive, **administrator** must also be the logon id for accessing the client PC.
 - If **xyz123** is the password to map the drive, the same **xyz123** must be the password for accessing the client PC.

- Save the logon account credentials from a command line. The **net use** command provides the **/savecred** switch, used when the user is prompted for a username and/or password.

Table 10
Formatting legend

Format	Meaning
<i>Italic</i>	Information that the user must supply
Bold	Elements that the user must type exactly as shown
Between Brackets ([])	Optional items
Between braces ({ }); choices separated by pipe (). Example: {even odd}	Set of choices from which the user must choose only one

The syntax for this command is:

```
net use [{DeviceName|*}] [\\{ComputerName|IP}\ShareName] [/savecred]
```

OR

```
net use [{DeviceName|*}] [\\{ComputerName|IP}\ShareName[{Password|*}]] [/user:[DomainName\]UserName] [/savecred]
```

The parameters are:

- **DeviceName**: Assigns a name to connect to the resource. The device name can be disk drives (that is, D: through Z:) or type an asterisk (*) instead of a specific device name to assign the next available device name.
- **\\ComputerName\ShareName**: Specifies the name of the server or its IP address and the shared resource. If ComputerName contains spaces, use quotation marks around the entire computer name from the double backslash (\\) to the end of the computer name (for example, \\ComputerName\ShareName).
- **/savecred**: Stores the provided credentials for reuse.
- **Password**: Specifies the password needed to access the shared resource. Type an asterisk (*) to produce a prompt for the password. The password is not displayed when typed in at the password prompt.
- **/user**: Specifies a different user name with which the connection is made.
- **DomainName**: Specifies another domain. If you omit DomainName, net use uses the current logged on domain.
- **UserName**: Specifies the user name with which to log on.

Figure 21
Mapped drive from command line window

```

C:\WINNT\system32\cmd.exe

C:\>net use * \\192.168.201.31\Nortel /savecred
Drive Z: is now connected to \\192.168.201.31\Nortel.

The command completed successfully.

C:\>net use
New connections will be remembered.

Status          Local        Remote               Network
-----
OK              Z:          \\192.168.201.31\Nortel  Microsoft Windows Network
Disconnected    \\192.168.55.181\IPC$  Microsoft Windows Network
The command completed successfully.

C:\>_

```

The initially mapped drive is the drive that must always be mapped for Telephony Manager to function.

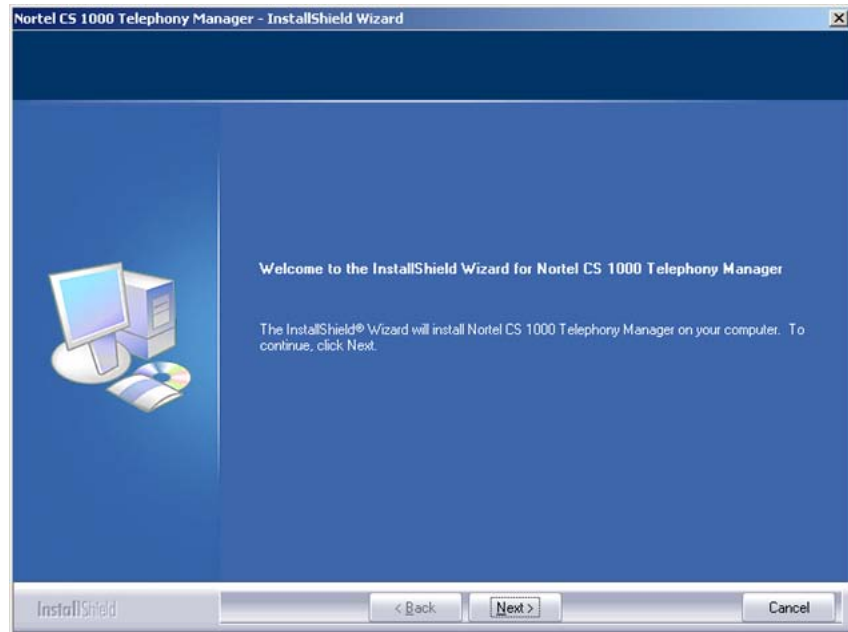
Installing the client software

Procedure 4 Installing the client software

Step	Action
1	Before installation: - On client PC, exit all Windows programs. - Ensure Distributed COM is enabled. For DCOM to work, the Telephony Manager 3.1 client must be able to reach the Telephony Manager 3.1 server by its actual IP address. If Network Address Translation (NAT) is used on the server, the Telephony Manager 3.1 client is not able to reach the server: - From Control Panel>Administrative Tools>Component Services, right-click My Computer under the Computers folder of the Console tree. - Click on Properties > Default Properties, ensuring the Enable Distributed COM on this computer check box is selected. - On the Telephony Manager 3.1 server, grant users full control permissions to the shared directory <tmroot>\Telephony Manager. - On the client PC, map the shared directory located on the Telephony Manager 3.1 server. Ensure that the mapped drive is available upon reboot of the client PC.

- 2 Double-click **Setup.exe** on the Telephony Manager 3.1 CD-ROM, [Figure 22 "InstallShield Wizard - Preparing to Install"](#) (page 65) appears.

Figure 22
InstallShield Wizard - Preparing to Install



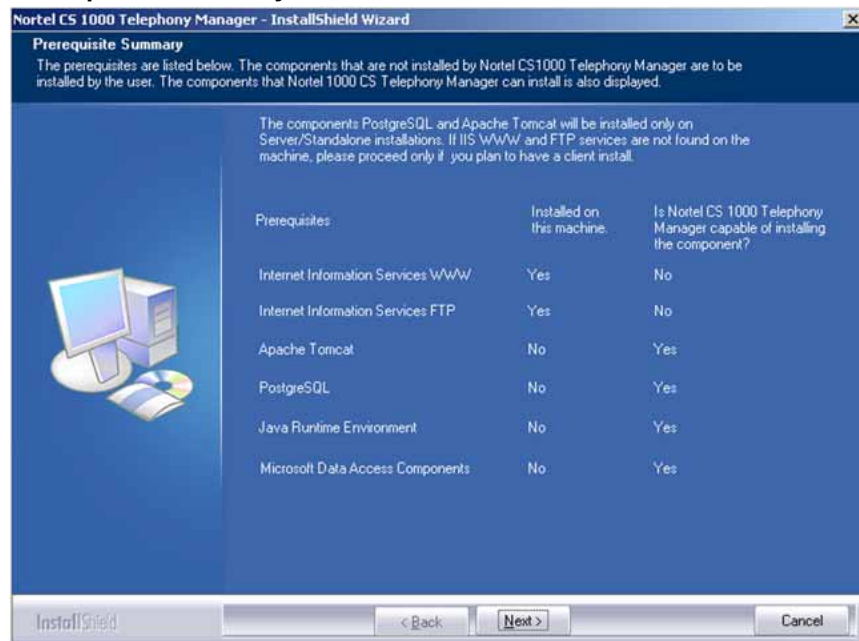
The following prerequisites are checked:

- if the operating system is supported by Telephony Manager 3.1
- if the PC has the appropriate software components installed (for details, see ["Preparing for installation"](#) (page 29)).

The Prerequisite Summary page appears ([Figure 23 "Prerequisite summary"](#) (page 66)), listing the mandatory software components needed to continue installation.

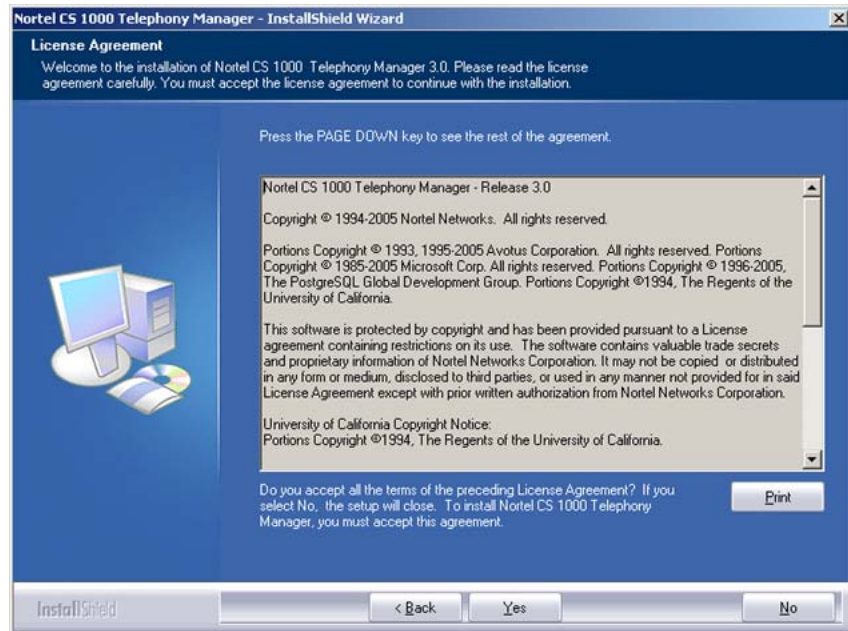
Although the prerequisite summary appears during a client install, it is only relevant to a server install.

Figure 23
Prerequisite summary



- 3 Click **Next** to continue.
- 4 The Welcome screen and Licence Agreement appears (see [Figure 24 "Welcome screen and Licence Agreement" \(page 67\)](#)). Read the Licence Agreement and Click **Yes** to accept and continue.

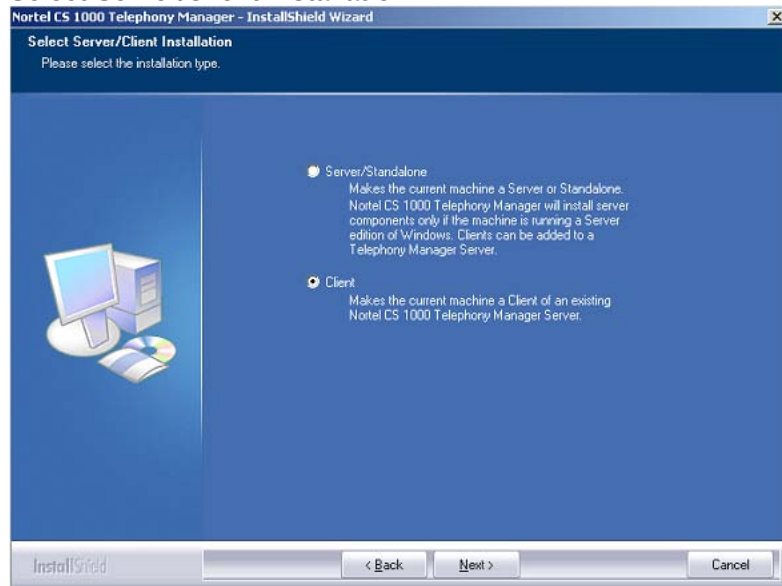
Figure 24
Welcome screen and Licence Agreement



- 5 The Server/Client installation selection page appears (See [Figure 25 "Select Server/Client Installation"](#) (page 67)). Select **Client**.

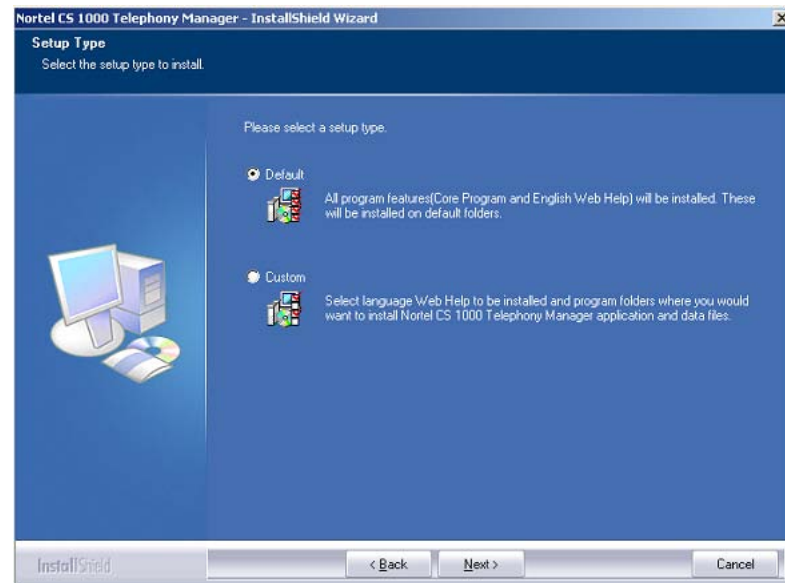
Installation types cannot be changed for upgrades. It is preselected based on the existing installation.

Figure 25
Select Server/Client Installation



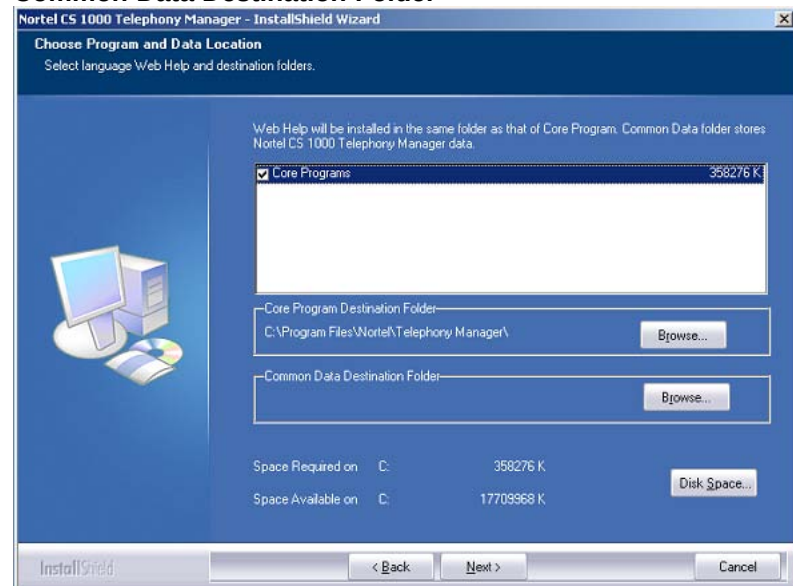
- 6 The Setup Type page screen appears (Figure 26 "Setup Type" (page 68)), providing a choice of either Default or Custom installation options. Select **Default**.

Figure 26
Setup Type



If Default is chosen, the Installation Summary page appears and the installation proceeds with default values. If Custom is chosen, the following pages appear.

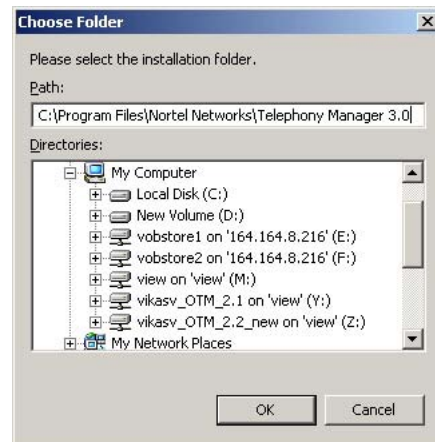
Figure 27
Common Data Destination Folder



Ensure that you browse to the Common Data folder that is stored on the actual Telephony Manager Server, using the mapped drive.

Figure 27 "Common Data Destination Folder" (page 68) shows the Common Data Destination Folder screen. The Common Data Destination Folder Browse button allows the user to select the destination folder for the Common Data. Clicking the Browse button displays the Choose Folder dialog box (see Figure 28 "Choose Folder" (page 69)).

Figure 28
Choose Folder



- 7 Specify a destination directory and click **OK**.

ATTENTION

You must not install Telephony Manager 3.1 in the root directory (for example, C:\). During the installation process, you must specify a folder (for example, C:\Nortel).

- 8 Clicking the Disk Space button in Figure 11 "Program and Data Location" (page 52) displays the Available Disk Space dialog box (see Figure 29 "Available Disk Space" (page 70)), showing the available disk space in each of the drives on the PC.

If the selected drive doesn't have enough disk space to accommodate the selected options, an error message appears asking the user to select another drive.

Figure 29
Available Disk Space



- 9 The Installation Summary screen appears (See [Figure 30](#) "Installation Summary" (page 70)), listing the options chosen during the installation.

Figure 30
Installation Summary

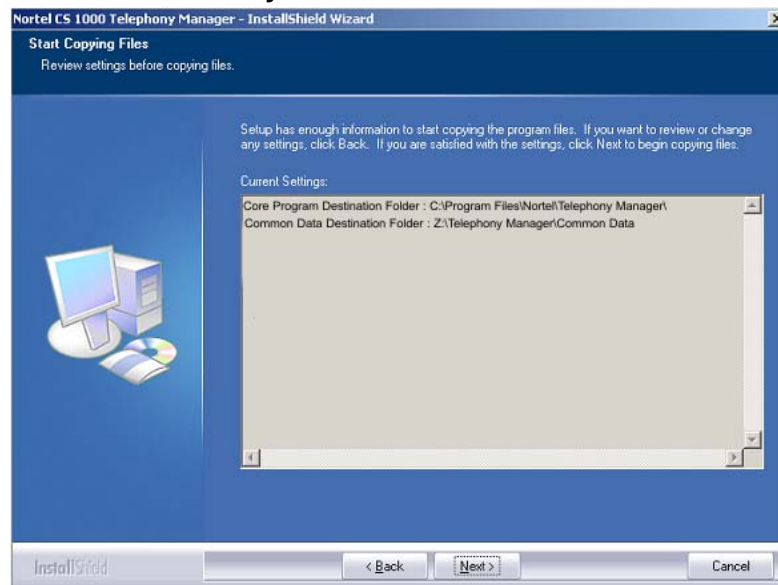
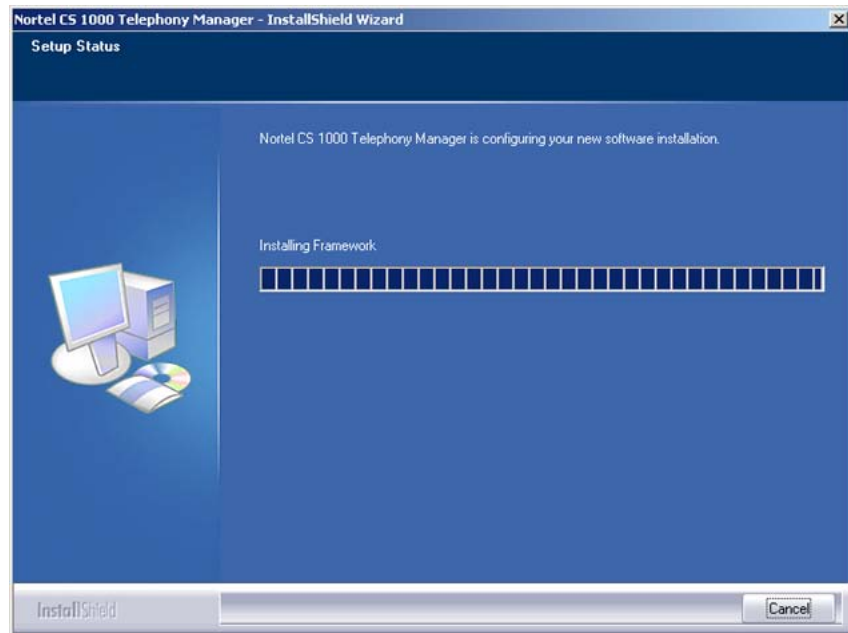


Figure 31
Setup Status



- 10 If **Cancel** is clicked at any time during the installation, the Exit Setup dialog box (Figure 32 "Exit Setup" (page 71)) prompts for confirmation before terminating and rolling back the installation. If **Yes** is clicked (see Figure 33 "Install interrupted" (page 72)), the installation is interrupted and the system is restored to its original state. If **No** is clicked, the installation continues.

Figure 32
Exit Setup

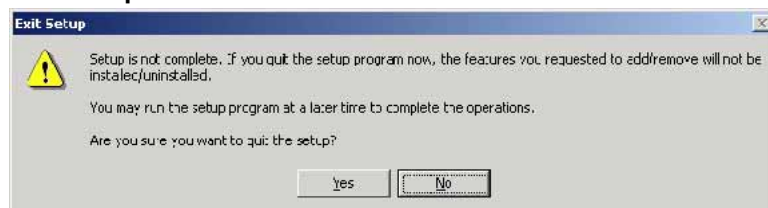
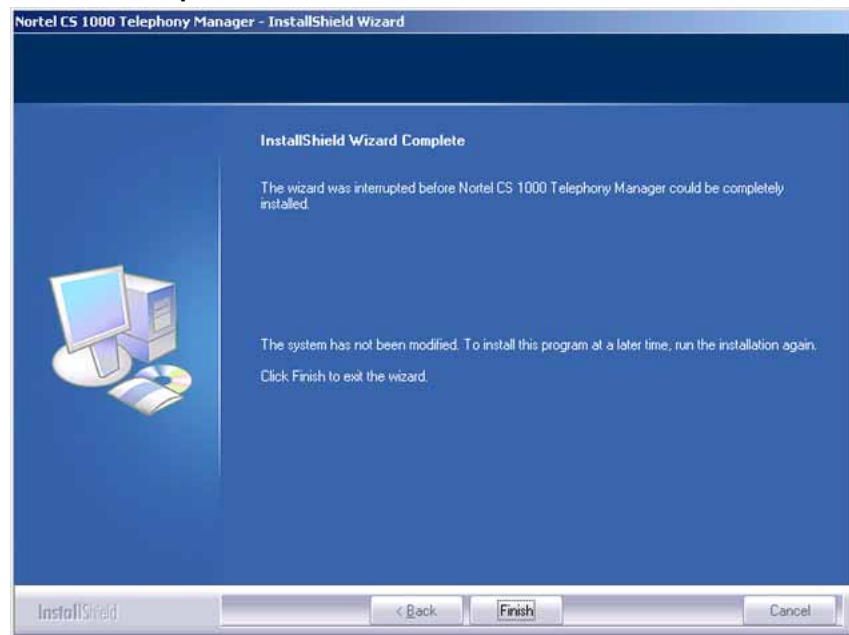
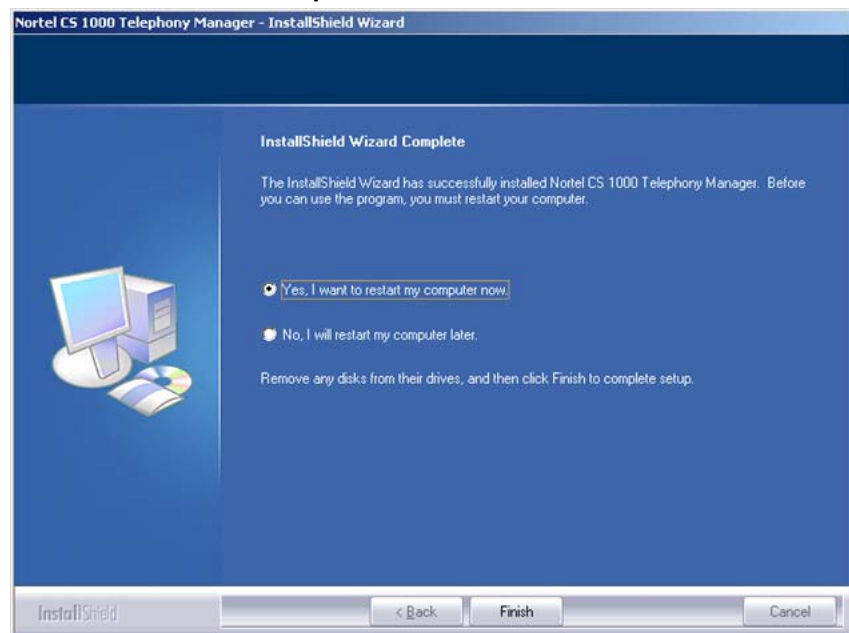


Figure 33
Install interrupted



- 11 Upon completion, the installation Wizard Complete screen appears, prompting the installer to restart the PC now or at a later time. See [Figure 34 "Installation Wizard Complete"](#) (page 72).

Figure 34
Installation Wizard Complete



—End—

pcAnywhere uninstallation

When pcAnywhere version 11.0 is installed on a system and later it is uninstalled, DCOM service is disabled by the uninstall process. Telephony Manager 3.1 logon will fail.

To enable Telephony Manager 3.1 logon, complete the following procedure:

When the pcAnywhere version 11.0 is uninstalled, re-enable the DCOM service.

Procedure 5

Re-enabling the DCOM service

Step	Action
1	Go to Control Panel->Administrative Tools->Component Services
2	Click Computers folder
3	Right-click on My Computer .
4	Select Properties .
5	Select Default Properties tab.
6	Place a check next to Enable Distributed COM on this computer .
7	Click OK and close the Component Services window.
8	Reboot the machine for the changes to take effect.

—End—

Performing a keycode upgrade

Contents

This chapter contains information about the following topics:

["Keycode upgrade" \(page 75\)](#)

Keycode upgrade

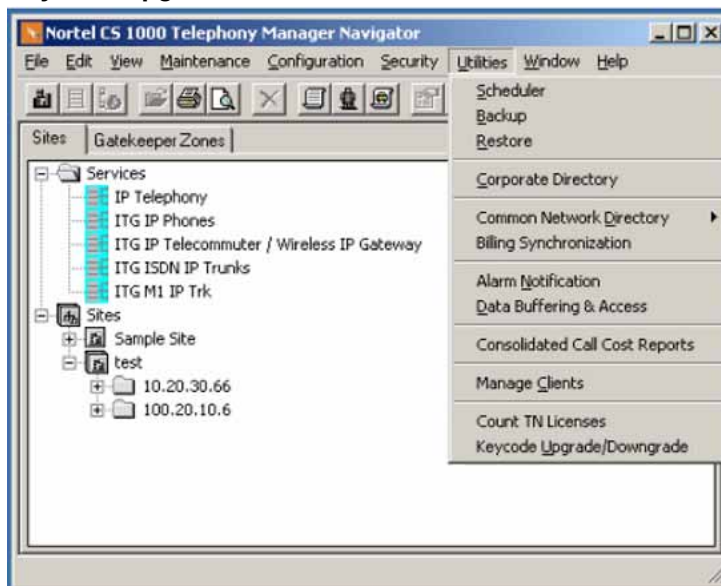
For keycode upgrades that do not involve applications, a separate license upgrade utility is incorporated into the Telephony Manager Navigator under the Utilities menu.

Procedure 6

Upgrading the keycode

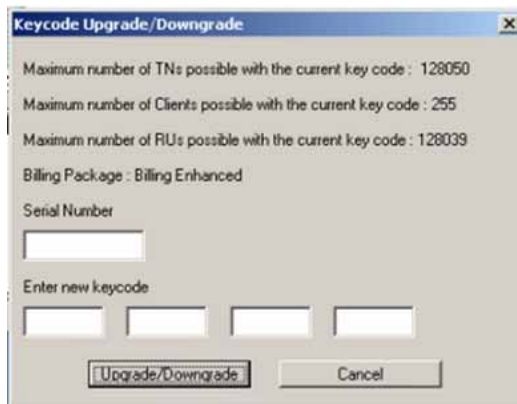
Step	Action
1	From the Utilities menu in Telephony Manager Navigator, select Keycode Upgrade(SeeFigure 35 "Keycode upgrade Utilities menu" (page 76)). The menu items shown in Figure 35 "Keycode upgrade Utilities menu" (page 76) are not available for a Client installation of Telephony Manager 3.1.

Figure 35
Keycode upgrade Utilities menu



- 2 The Keycode Upgrade dialog box appears (see [Figure 36 "Keycode Upgrade dialog box" \(page 76\)](#)), providing details of the currently available licenses and a keycode entry facility to upgrade the keycode. Enter the appropriate information and click Upgrade.

Figure 36
Keycode Upgrade dialog box



- 3 The Confirm Keycode Upgrade dialog box appears (see [Figure 37 "Confirm Keycode Upgrade dialog box" \(page 77\)](#)). Click **yes** to proceed.

Figure 37
Confirm Keycode Upgrade dialog box



—End—

Performing migrations

Contents

This chapter contains information about the following topics:

["Upgrades and migration" \(page 79\)](#)

["Operating system migration" \(page 80\)](#)

Upgrades and migration

ATTENTION

Direct upgrades are not supported for customers migrating from OTM releases prior to 2.2. A two-step upgrade is required, first to OTM 2.2, and then to Telephony Manager 3.1.

Upgrade from MAT to Telephony Manager 3.1 is not supported. The upgrade must be done as a new purchase and a new install.

Custom reports created in OTM 2.2 are lost after migration to Telephony Manager 3.1. The Telephony Manager 3.1 Corporate Directory does not support customized reports.

Windows Server 2003 migration

Direct migration is not supported in Windows Server 2003.

To migrate from Windows 2000 Server (OTM 2.2) to Windows Server 2003 (Telephony Manager 3.1) you must first upgrade from OTM 2.2 to Telephony Manager 3.1 on the Windows 2000 Server system. The database migration utility then migrates all data to Telephony Manager 3.1. Complete the following steps to perform this migration:

- Perform a full backup of the Telephony Manager 3.1 data on the Windows 2000 Server system, using the Telephony Manager 3.1 backup utility.
- Install Telephony Manager 3.1 on the Windows Server 2003 system.
- Transfer the backed up data from the Windows 2000 Server system to the Windows Server 2003 system.

- Restore the backed up data to the Windows Server 2003 system using the Telephony Manager 3.1 restore utility.

Upgrading to Telephony Manager 3.1

To configure and manage PBX Release 5.0, the OTM or Telephony Manager software must be upgraded to Telephony Manager 3.1.

Migration is supported from OTM 2.2 to Telephony Manager 3.1. The upgrades can be conducted either by direct upgrade or a two-step upgrade (upgrading from previous OTM releases to OTM 2.2), as indicated by the following actions.

The data migration is performed as part of the upgrade from OTM 2.2 to Telephony Manager 3.1.

Note: Do not attach the USB dongle until Telephony Manager 3.1 is installed.

The direct upgrade is a one-step upgrade, as follows:

- Telephony Manager 3.0 to Telephony Manager 3.1: Telephony Manager 3.1 uses the same database as the one used for Telephony Manager 3.0, therefore there is no requirement to migrate database.
- OTM 2.2 to Telephony Manager 3.1: This operation involves migration and upgrade of databases.

Telephony Manager 3.1 provides the option to upgrade from OTM 1.20, 2.0, 2.01, and 2.1, involving two steps.

1. Upgrade from OTM 1.20, 2.0, 2.01, or 2.1 to OTM 2.2.
2. Upgrade from OTM 2.2 to Telephony Manager 3.1.

Operating system migration



WARNING

Back up the Alarm Notification control and script files separately. The script files can be replaced during a software upgrade.

Complete the following steps to migrate from OTM 2.2 installed on one operating system to Telephony Manager 3.1 on a different operating system.

Procedure 7

Operating system migration

Step	Action
1	Upgrade OTM 2.2 to Telephony Manager 3.1 on the existing operating system.
2	Reboot the system and allow database migration to complete.
3	Launch the Telephony Manager 3.1 navigator (> utilities > Backup utility). Perform a full backup.
4	Install Telephony Manager 3.1 on the new supported operating system.
5	Reboot the system.
6	Launch the Telephony Manager 3.1 navigator (> utilities > Restore utility). Perform the restore operation using the full backup file created on the original operating system.

—End—

ATTENTION

Following the system upgrade and reboot, the Database Migration Utility runs automatically. The utility can be found at the following location:

<tmroot>\Common Services\Program Files\MigrationController.exe

Windows client migration

Because all common data resides on the Telephony Manager 3.1 server, backup and restore of data on the client is not required. If the Telephony Manager 3.1 server is successfully installed, Telephony Manager 3.1 clients can be installed on any new supported operating system.

Migrating employee data

ATTENTION

CND 2.1 is a mandatory requirement to ensure the proper functioning of Telephony Manager 3.1. It is not part of Telephony Manager install, and must be installed separately.

For detailed information about installing and synchronizing the CND, see *Telephony Manager 3.1 System Administration (NN43050-601)* and *Common Network Directory 2.1 Administration Guide (NN43050-101)*.

The Database Migration Utility does not migrate employee data in the Employee Directory. There are 2 possible ways to recreate the employee data in Telephony Manager 3.1:

- Use the CND Sync Utility provided by Telephony Manager 3.1 to automatically add employee records in CND based on CPND name of the telephones.
- Use the Subscriber Import feature provided by the CND Manager to add employee records using a CSV file.

See ["TBS to CND file header conversion" \(page 303\)](#) for the TBS conversion table.

The following procedure describes how to export employee data from OTM 2.2 to a CSV file that can be used to recreate employee data in the CND using the Subscriber Import feature.

Prior to executing these steps, the user must read the *Common Network Directory 2.1 Administration Guide (NN43050-101)* section "Subscriber import" in order to understand the requirements, warnings, and limitations of the CSV file.

Procedure 8

Creating the employee csv file

Step	Action
1	Open the system window and launch the Export Utility.
2	Select Corporate Directory Export and click on the ellipsis button (...) to access the configuration dialog.
3	Select File Type as Text File (comma separated values) .
4	Click on the Format button to select the employee fields that you want to export.
5	For each field selected, make sure the External Column Name matches the supported attribute names in CND (refer to <i>Common Network Directory 2.1 Administration Guide (NN43050-101)</i> , Subscriber Import section, Header Record description).
6	Click OK to save Format settings.
7	Click OK to save Configuration settings.
8	Click Go or Schedule to run report.
9	Repeat the process for each system that you want to have the employee data migrated to CND.

- 10 Consolidate and/or edit the exported csv files as required to conform to the CND Subscriber Import requirements.

ATTENTION

Use of Microsoft Excel for editing is not recommended as it performs automatic conversion that will corrupt the employee data.

—End—

Database Migration Utility logfile

The Database Migration Utility creates a log file that contains information on the systems that have been migrated and any record that could not be migrated. This logfile, named **DataMigration.log**, is found in the following location:

<tmroot>\Common Data\DataMigration.log

Configuring Secure Sockets Layer (SSL)

Contents

This section contains information about the following topics:

["Overview" \(page 85\)](#)

["Installing a server certificate in IIS" \(page 85\)](#)

["Configuring SSL on the Telephony Manager 3.1 server platform" \(page 86\)](#)

["Enabling SSL for Telephony Manager 3.1 Web logon" \(page 86\)](#)

["Importing Telephony Manager 3.1 Root Certificate" \(page 87\)](#)

["Setting up CND SSL" \(page 87\)](#)

Overview

To use Secure Sockets Layer (SSL) in Web applications, a server certificate must be installed in Internet Information Services (IIS). The key-storage file, which contains both private and public keys and is password-protected, must be used for the certificate to become valid. Private and public keys are used by the browser and IIS to negotiate encryption.

Installing a server certificate in IIS

Telephony Manager 3.1 server can be configured to use SSL to protect passwords in network transport during the logon sequence. For the SSL transport to become fully operational, an SSL server certificate must be installed in IIS. You can obtain your own server certificate from a trusted authority (for example, Verisign) or generate your own certificate using a certificate server. This document assumes you have already obtained a server certificate and only describes the steps required to install the certificate.

Configuring SSL on the Telephony Manager 3.1 server platform

The following versions of IIS are supported on the OS platform: 5.0, 5.1, 6.0, and 7.0.

To install the certificate from the Internet Services Manager application on a Windows server, complete the following procedure.

Procedure 9

Configuring SSL on the Telephony Manager 3.1 server platform

Step	Action
1	Launch the application from Programs > Administrative Tools > Internet Information Services (IIS) Manager .
2	From the left navigator pane, select Web Sites > Default Web Site .
3	Right-click on Default Web Site and select Properties .
4	From the Properties window, select Directory Security tab and click Server Certificate under Secure Communications. The Web server Certificate Wizard then walks you through the installation of the certificate.
5	After the certificate installation is completed, go to the Default Website Properties window and select the Web site tab. Ensure the SSL Port is set to 443.

—End—

Enabling SSL for Telephony Manager 3.1 Web logon

Procedure 10

Enabling SSL for Telephony Manager 3.1 Web logon

Step	Action
<i>To enable SSL for Telephony Manager 3.1 Web logon, complete the following procedure.</i>	
1	From Telephony Manager 3.1 Navigator (Windows or Web), launch the User Authentication application.
2	Select the check box Use SSL for Web logon authentication .

—End—

Importing Telephony Manager 3.1 Root Certificate

Enabling SSL for Telephony Manager 3.1 Web logon can cause long delays before the logon page is displayed. When IIS receives an incoming SSL request from a client, it attempts to build its certificate chain before sending its certificate information back to the client. During this time, if the IIS computer does not have the issuing certificate authority's root certificate installed locally, it tries to connect to the certificate authority directly to obtain it. This causes the server to try and resolve the certificate authority's machine name or fully qualified domain name to an IP address.

If the certificate authority (certificate server) is inaccessible from the IIS computer, then IIS continues to resolve the certificate authority's IP address until it times out. These name resolution queries cause SSL connection delays.

To resolve this, the client can import the Telephony Manager 3.1 root certificate into the browser's certificate storage.

To import the Telephony Manager 3.1 root certificate into Internet Explorer certificate storage, complete the following procedure:

Procedure 11

Importing Telephony Manager 3.1 Root Certificate

Step	Action
1	Make the Telephony Manager 3.1 server certificate available to the client PC.
2	From Internet Explorer, select Tools > Internet Options .
3	Select Content tab and click Certificates .
4	Select Trusted Root Certification Authorities tab.
5	Click Import . The Certificate Import Wizard walks you through the import process.

—End—

Setting up CND SSL

Procedure 12

Setting up CND SSL

Step	Action
1	Set up Netscape Communicator 4.79 or above, to trust certificate authorities used by CND servers that have SSL enabled.

If the CND server certificate is issued by well known certificate authorities such as VeriSign, and so on, the certificate authority can already be in the Netscape Communicator certificate database by default.

- a. Verify the certificate authority is included in Netscape Communicator certificate database. To do this, open the Communicator menu, select **Tools > Security Info**, and then click **Signers** on the left side.
 - b. If the certificate authority is not included in the database, consult your system administrator for importing a private certificate authority.
- 2** Locate the certificate database files used by the Netscape Communicator:
- a. From C:\Netscape\userName directory (UserName is the current logon user name), select **cert7.db**, **key3.db**, and **secmod.db**.
 - b. Copy the three files to the Telephony Manager 3.1 Common Data directory (usually under c:\Nortel\Common Data).
- 3** Set up the CND SSL connection in Telephony Manager 3.1 server:
- a. Open **Telephony Manager 3.1 Windows Navigator**, select **Utilities > CND Server Setup**.
 - b. Set the port number to 636 or the specific SSL port number configured by the CND server.
 - c. Select **Use SSL for authentication and synchronization**.
- 4** For detailed instructions on setting up the CND server, as well as an example of importing attributes to the CND Directory, see CND Synchronization in *Common Network Directory 2.1 Administration Guide (NN43050-101)*.

—End—

License management

Contents

This chapter contains information about the following topics:

["Serial number and keycode" \(page 89\)](#)

["TN license" \(page 89\)](#)

["RU license" \(page 90\)](#)

["Client license" \(page 91\)](#)

["Security device \(dongle\)" \(page 91\)](#)

Serial number and keycode

Keycodes supported on previous releases of Telephony Manager do not work in Telephony Manager 3.1.

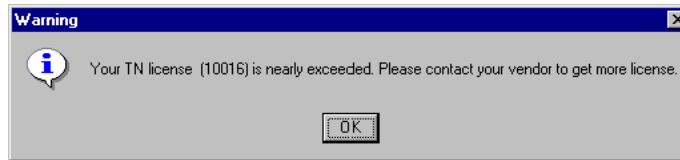
The serial number and keycode you receive with your Telephony Manager 3.1 software package determines the maximum number of terminal numbers (TNs) or telephones, Reporting Units (RUs), and Telephony Manager 3.1 clients that can be configured in your Telephony Manager 3.1 system. To purchase licensing for additional TNs, RUs, or clients, contact your Telephony Manager 3.1 vendor.

TN license

TN license checking

Each time you log on to Telephony Manager 3.1, your TN license is checked. If the number of set TNs (telephone TNs and virtual TNs) configured in your system is approaching the maximum for your license, the TN **Warning** window appears. See [Figure 38 "TN license warning" \(page 90\)](#).

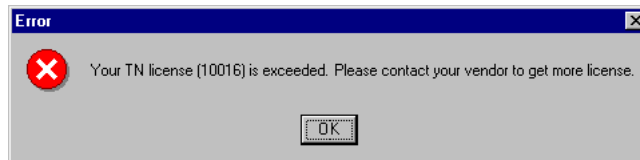
Figure 38
TN license warning



License exceeded

If your TN license is exceeded, an **Error** window appears. See [Figure 39 "TN license error" \(page 90\)](#). This message appears every 15 minutes. Contact your vendor to obtain a license for additional TNs.

Figure 39
TN license error



License reuse

TN checking is performed on bootup and after every 12 hours of operation. If you delete a site, the TN licenses associated with that site becomes available for reuse after the next TN check. If you are unable to wait for the next TN check, you can reboot the Telephony Manager 3.1 server.

RU license

Reporting Units (RUs) are the base used for licensing the telemanagement applications in Telephony Manager 3.1. An RU represents a single entity in the Telephony Manager 3.1 Corporate databases to which costs/usage can be assigned and reported on through the telemanagement applications. An entity can be either an employee in the Employee database, an external party in the External Parties database, or a role or project in the Roles/Projects database.

Each time you launch a telemanagement application in Telephony Manager 3.1, your RU license is checked. If the number of RUs configured in your system is approaching the maximum for your license, a warning dialog box appears.

If your RU license is exceeded, you receive an error message. The TBS application continues to collect data; however, you cannot cost the data and generate reports. The GCAS application launches, but you cannot generate reports. Contact your vendor to obtain a license for additional RUs.

See *Telephony Manager 3.1 Telemanagement Applications (NN43050-602)* for more information.

Client license

When you install an Telephony Manager 3.1 client, the host name of the Telephony Manager 3.1 client is registered on the Telephony Manager 3.1 server database. Each time a user attempts to log on to the Telephony Manager 3.1 client, the Telephony Manager 3.1 software checks the Telephony Manager 3.1 database. If the Telephony Manager 3.1 client is not located in the database, the **TM 3.1 Navigator** dialog box appears.

The clients Hostname and IP are saved to the client database. If the IP is changed while the Hostname stays the same then use the client utility.

The **TM 3.1 Navigator** window appears if the Telephony Manager 3.1 client computer's host name is changed or if the Telephony Manager 3.1 client is removed from the Telephony Manager 3.1 database.

If the host name of an Telephony Manager 3.1 client computer is changed, the Telephony Manager 3.1 Administrator can use the client Utility to update the host name in the Telephony Manager 3.1 database. For information about the client Utility, see *Telephony Manager 3.1 System Administration (NN43050-601)*.

Security device (dongle)

Parallel dongle

A Dongle is a small hardware security device attached to the PC. In Telephony Manager 3.1, the dongle attached to the server enables access for all of the clients configured on the server.

When Telephony Manager 3.1 is launched from a Telephony Manager 3.1 client, the Telephony Manager 3.1 server's dongle is checked. The Telephony Manager 3.1 client cannot launch the Telephony Manager 3.1 System Window if the Telephony Manager 3.1 server's dongle is missing.

If the dongle is removed from the Telephony Manager 3.1 server, it takes approximately 5 minutes, when it is reattached, for the Telephony Manager 3.1 client to recognize the dongle.

ATTENTION

When a user attempts to log on to Web Navigator after installing Telephony Manager 3.1 for the first time, an error message displays stating that the Telephony Manager 3.1 dongle is missing, when in fact it is not missing. If this occurs, the dongle timer is set to a two-minute interval for dongle checking (instead of the regular 30-minute interval). Therefore, the user must wait a maximum of only two minutes to attempt another Web Navigator logon.

The dongle is supported on both the Server and Standalone configurations:

- supports one USB dongle only or one parallel port dongle
 - A dongle connected to a USB port at the same time as one connected to a parallel port is not supported.
 - Two dongles connected at the same time is not supported.

DongleRead.exe

DongleRead.exe is included in the Telephony Manager 3.1 Installation CD. When launched, the DongleRead.exe utility reads the serial number of the dongle attached to the PC and displays it in the **DongleRead** window. See [Figure 40 "DongleRead" \(page 92\)](#). The Sentinel Security driver must be installed for the DongleRead.exe to function.

Figure 40
DongleRead



PCI port limitations

PCI-based parallel ports can have problems on certain operating systems. Compaq Proliant DL360R01 running Windows 2000 Server using a Lava PCI Bus Enhanced Parallel Port card is one such system. Telephony Manager 3.1 does not support this configuration.

Transfer from parallel port dongle to USB dongle

Migration from a parallel port dongle to USB dongle is supported, as is migration from a USB dongle to a parallel port dongle. To accommodate this, order the transfer code that replaces a parallel port dongle with a USB dongle.

When a customer orders a dongle transfer and goes from a parallel port to USB (or vice versa), the old dongle serial number is no longer valid. The keycode issued is for the new dongle serial number and does not work on the old dongle. The customer is expected to discard the old dongle. This dongle swap or transfer is only for end-user licensed dongles, not for distributor or enterprise licensed dongles. Distributors can just simply order more dongles of either type.

Before configuring Telephony Manager 3.1

Contents

This chapter contains information about the following topics:

- "Overview" (page 93)
- "Testing the connection" (page 94)
 - "Ethernet network (optional)" (page 94)
 - "Setting up communications information" (page 94)
 - "Setting up customer information" (page 97)
- Procedure 15 "Setting up Telephony Manager 3.1 applications" (page 99)
- "Setting up system data" (page 101)

Overview

Before configuring for Telephony Manager 3.1, test the connection between Telephony Manager 3.1 and your equipment, using the sample site and system configuration. Follow the procedure in this chapter.

After connecting successfully, refer to "Adding a site" in *Telephony Manager 3.1 System Administration (NN43050-601)* to configure your own sites and systems.

The complete list of Telephony Manager 3.1 configuration procedures includes:

- "Configuring Secure Sockets Layer (SSL)" (page 85)
- "Configuring a modem for Telephony Manager 3.1 applications" (page 149)
- "Initial logon" (page 177)
- "Testing the connection" (page 94)
- "Security Management" (page 157)
- "Adding Telephony Manager 3.1 Web users" (page 135)

- "Setting up the CND server and Terminal server" (page 179)
- "Configuring the Web browser client" (page 185)
- "Integrating Telephony Manager 3.1 with ENMS" (page 187)
- "Integrating Telephony Manager 3.1 with HP OpenView" (page 207)

Testing the connection

Use the following procedures to test the connection between Telephony Manager 3.1 and your equipment. For detailed instructions on adding sites and systems, see [Procedure 16 "Setting up system data" \(page 101\)](#).

Ethernet network (optional)

The network interface or interfaces must be configured and connected to the network prior to testing the connection (refer to Appendix A, "[Typical configurations" \(page 277\)](#)").

Setting up communications information

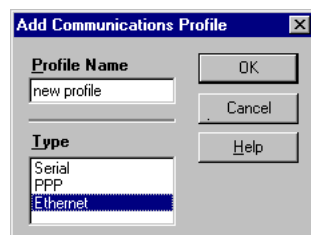
Procedure 13

Setting up communications information

Step	Action
1	Double-click Sample Site in the Telephony Manager 3.1 Navigator window.
2	Click Sample System , and then choose File > Properties .
3	The System Properties dialog box appears with the General tab selected.
4	Click Communications tab.
5	Click Add .

The Add Communications Profile dialog box appears. See [Figure 41 "Add Communications Profile dialog box" \(page 94\)](#).

Figure 41
Add Communications Profile dialog box

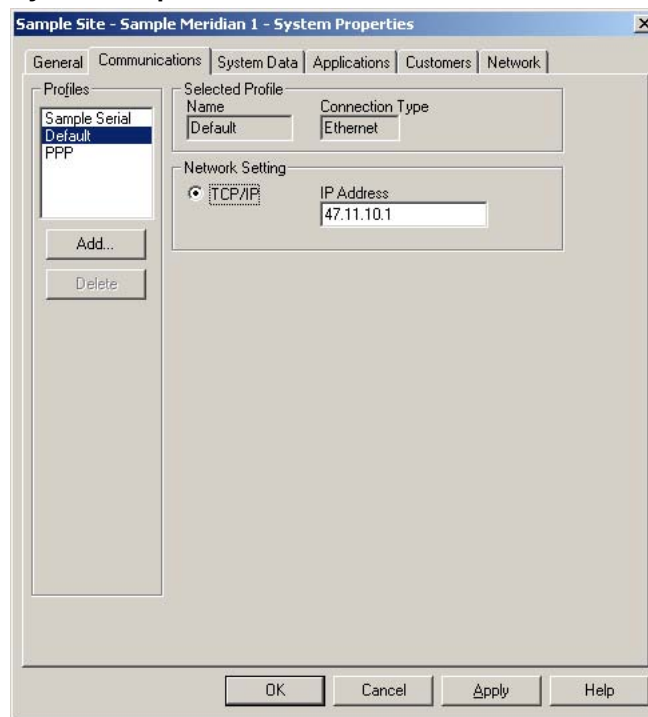


- 6 In the Type box, select a connection type for Telephony Manager 3.1.
- 7 Enter a Profile Name.
- 8 Click **OK**.
- 9 Enter the information in the System Properties—Communications dialog box for the connection type selected in step 6.

For an Ethernet connection type (see [Figure 42 "System Properties: Communications tab Ethernet Profile"](#) (page 95)):

- a. Enter the IP address that you configured on the system.
- b. Click **Apply**.

Figure 42
System Properties: Communications tab Ethernet Profile



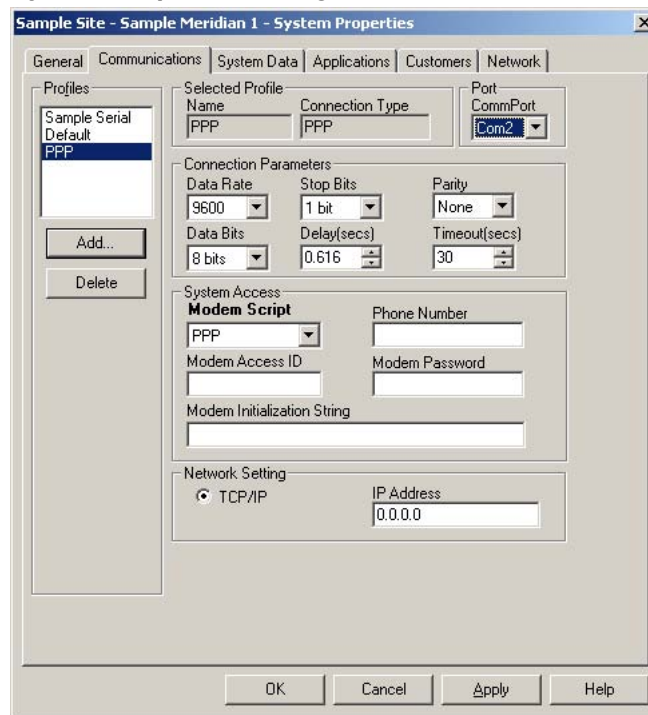
For a PPP connection type (see [Figure 43 "System Properties dialog box: Communications tab PPP Profile"](#) (page 96)):

- c. Enter all modem parameters and dial-up information.
- d. Select PPP in the Modem Script text box and enter the telephone number.

There can be conditions, depending on your particular installation, where you can be required to enter a modem access ID, a modem password, and a modem initialization string.

- e. Set the IP address to the local IP address, as configured on the system.
- f. Click **Apply**.

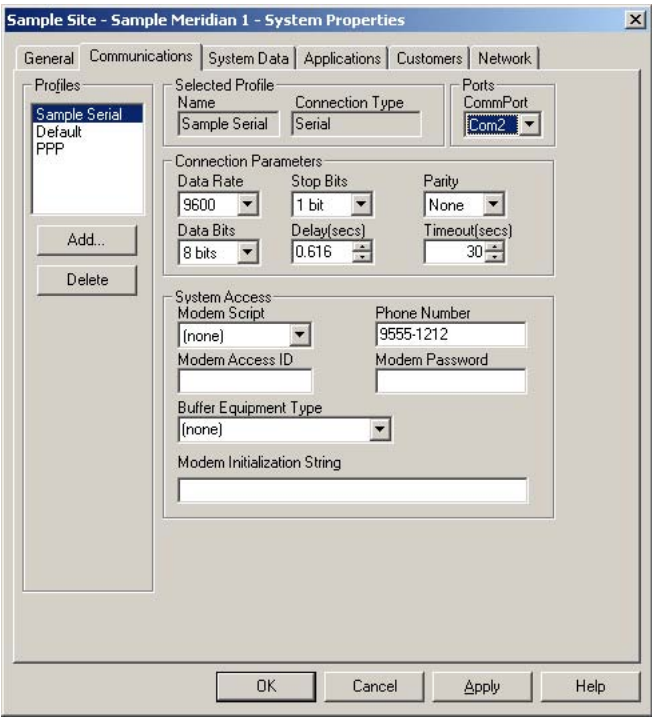
Figure 43
System Properties dialog box: Communications tab PPP Profile



For a Serial connection type (see [Figure 44 "System Properties dialog box: Communications tab Serial Profile"](#) (page 97)):

- g. Enter all modem parameters and dial-up information.
- h. Select the appropriate value in the Modem Script text box.
This is commonly **None** unless a specific value is defined for your system.
- i. Click **Apply**.

Figure 44
System Properties dialog box: Communications tab Serial Profile



—End—

Setting up customer information

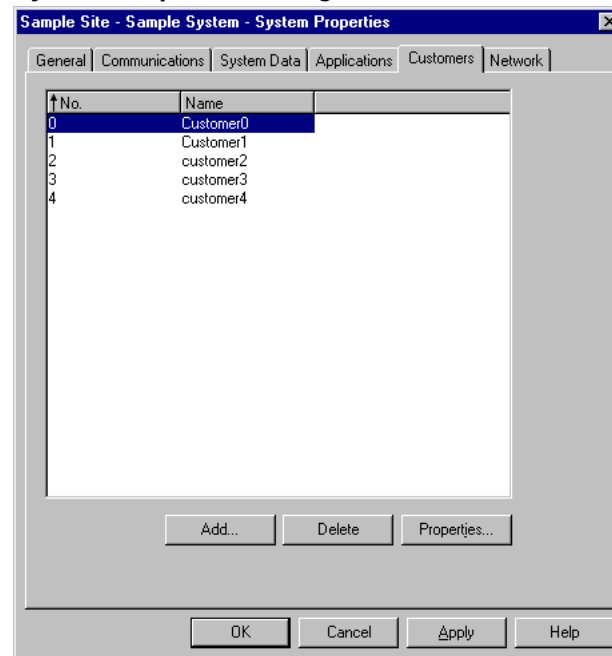
Procedure 14

Setting up customer information

Step	Action
------	--------

- | | |
|---|--|
| 1 | Click Customers tab. See Figure 45 "System Properties dialog box: Customers tab" (page 98). |
|---|--|

Figure 45
System Properties dialog box: Customers tab



A new customer may have to be added before Properties can be clicked. To add a new customer, click **Add**.

2 Click Properties.

The Customer Properties dialog box appears with the General tab selected. See [Figure 46 "Customer Properties: General tab" \(page 99\)](#).

Figure 46
Customer Properties: General tab

- 3 In the Scheduler System ID box, change the user ID and password to one that is valid for logging onto the system, and then click **OK**.
HLOC appears the home location code (ESN) defined in LD 90.

—End—

Setting up Telephony Manager 3.1 applications

Procedure 15

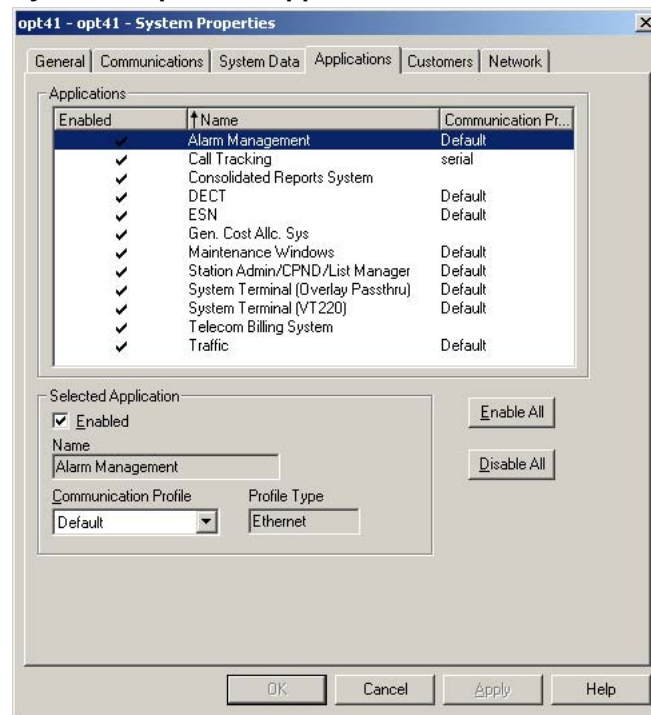
Setting up Telephony Manager 3.1 applications

Step	Action
------	--------

You must enable applications to make them available in the System window.

- 1 Click the Applications tab.
The System Properties—Applications tab appears (Figure 47 "System Properties: Applications tab" (page 100)).

Figure 47
System Properties: Applications tab



- 2 By default, each application is selected. Modify these selections by deselecting applications.
- 3 Choose one the following:
 - a. **Enable All:** Enables the default communication profile for all available applications under the **Application** tab (with the exception of Call Tracking which is always serial).

 If there is no serial profile added, then Call Tracking is not enabled. If the user has added any serial profile, then the first profile is set as the communication profile.

 The General Cost Allocation System and Telecom Billing System applications are enabled without a communication profile.
 - b. **Disable All:** Disables the communication profile for all available applications under the **Application** tab.
- 4 Click **OK**.

—End—

Setting up system data

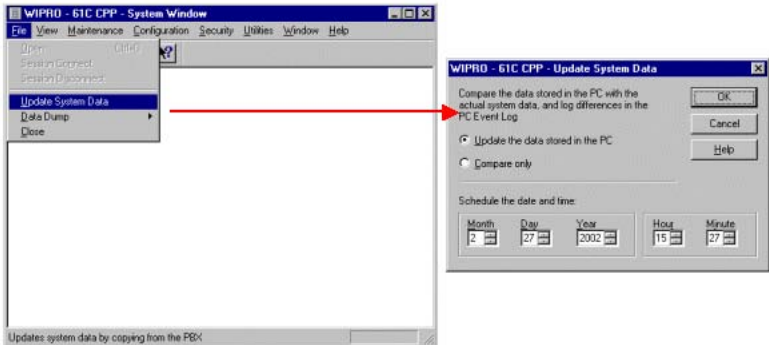
Procedure 16

Setting up system data

Step	Action
------	--------

- | | |
|---|--|
| 1 | Double-click the Sample System icon to open the System window. |
| 2 | Select File > Update System Data . |
| 3 | Select Update Data Stored in the PC . |

Figure 48
System Update



- | | |
|---|---|
| 4 | Click OK .

The system data (such as the PBX type and software packages) is copied into Telephony Manager 3.1 directly from the system.

When the data is copied from the system into Telephony Manager 3.1, the test procedure is complete. |
|---|---|

—End—

Windows Server 2003 configuration

Contents

This chapter contains information about the following topics:

- "Windows Server 2003 configuration and restrictions" (page 103)
 - "Web Server extensions " (page 104)
 - "Enabling Web Service extensions in IIS 6.0" (page 105)
 - "Add a New ISAPI Web Service extension to IIS 6.0" (page 106)
 - "Enabling parent paths" (page 107)
 - "IIS modes of operation" (page 109)
 - "Adjusting Internet Explorer security settings" (page 110)
 - "Remote Desktop and Terminal Server" (page 112)
 - "Telephony Manager 3.1 server-client setup" (page 113)
 - "Configuring client authentication on the server side" (page 113)
 - "Configuring security for Telephony Manager 3.1" (page 118)

Windows Server 2003 configuration and restrictions

Configuration Automation Tool

Some of the following configurations are automated using a script that is available for download from the Nortel Technical Support Web page for Telephony Manager 3.1.

The script, `ConfigureWin2003SA.vbs`, automates the workarounds that an administrator has to perform before using Telephony Manager 3.1 on a Windows Server 2003 as a stand-alone application. The script uses the `adsutil.vbs`, an IIS administration utility using Microsoft Visual Basic Scripting Edition (VBScript) with Active Directory Service Interfaces (ADSI) to manipulate the IIS configuration. The script is installed with Windows Script Host and is in the `%SystemRoot%\system32\inet_srv\adminsamples` folder.

`ConfigureWin2003SA.vbs` automates the following tasks:

- Creates the Telephony Manager Server and Jakarta Web Service extensions

- Enables the Active Server Pages and Server Side Includes Web Service Extensions
- Enables the parent paths
- Enables the www service to run in IIS 5.0 Isolation mode

ConfigureWin2003SA.vbs does not automate the following tasks:

- Does not add the http://localhost/admin site to the Trusted Sites (This has to be configured for every user.)
- Does not modify the COM Security Settings
- Does not change the Access Permissions for the shared Telephony Manager folder

When to run the ConfigureWin2003SA.vbs:

This script has to be manually run by the user after the installation of Telephony Manager 3.1 completes successfully.

How to run the ConfigureWin2003SA.vbs:

The user can launch this script by double-clicking the file or using the following command:

```
> cscript <path\ConfigureWin2003SA.vbs
```

The following sections describe the steps to perform the configurations manually. Of these, the configurations that are automated using the script are indicated.

Web Server extensions

Web server extensions are automated using the script.

By default, IIS serves only static content (ASP, ASP.NET). WebDAV publishing, FrontPage® Server Extensions, and Common Gateway Interfaces must be enabled after installing IIS. If not, IIS returns a generic **404 custom error page** to prevent disclosure of configuration information.

To permit IIS to serve dynamic content, the administrator must unlock this content in the Web service extensions node in IIS Manager. To do this, the administrator must either enable a pre-existing Web service extension or add a new Web service extension.

For Telephony Manager Web navigator to function, 3 Web Service extensions need to be enabled in IIS.

Enabling Web Service extensions in IIS 6.0

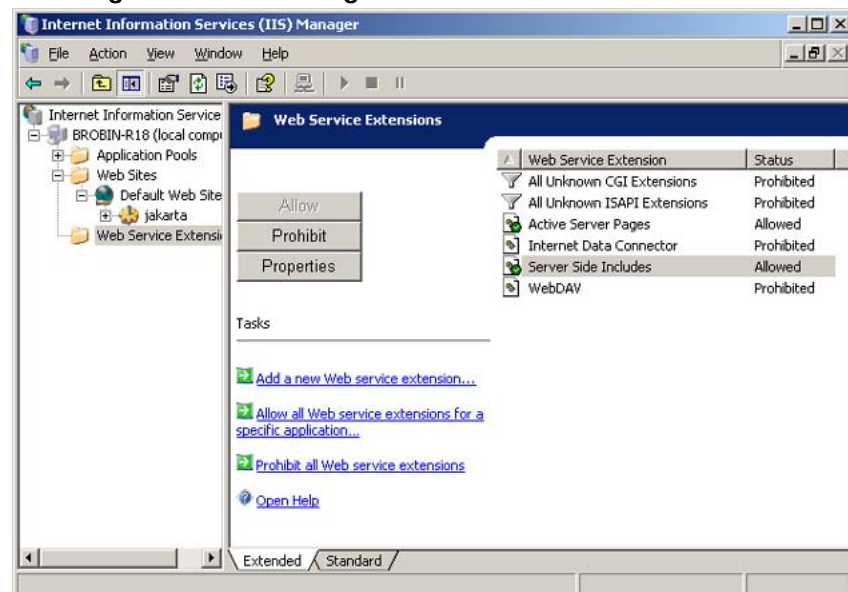
To enable IIS to serve content that requires the ASP extension and Server Side Includes, follow the steps in [Procedure 17 "Enabling Web Service extensions in IIS 6.0" \(page 105\)](#).

Procedure 17

Enabling Web Service extensions in IIS 6.0

Step	Action
1	Open IIS Manager, expand the master server node (that is, the Servername node), and select the Web service extensions node.
2	In the right pane of IIS Manager, right-click the extension that you want to enable. In the case for Telephony Manager 3.1, choose Active Server Pages (ASP) .
3	Click Allow .
4	Repeat the above steps for Server Side Includes (see Figure 49 "Enabling Active Server Pages" (page 105)).

Figure 49
Enabling Active Server Pages



—End—

Add a New ISAPI Web Service extension to IIS 6.0

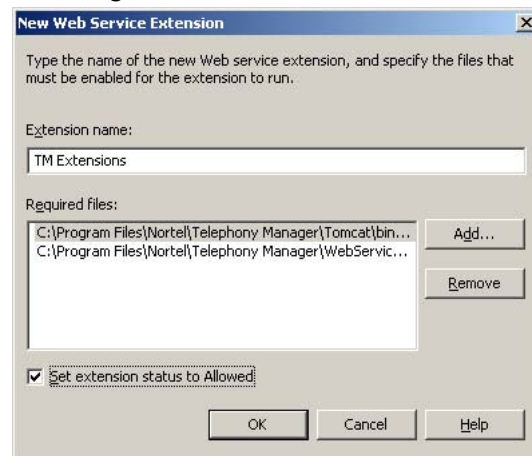
To enable IIS to serve content that requires a specific ISAPI or CGI extension that is not already listed in the Web service extensions list, follow the steps in [Procedure 18 "Adding a New ISAPI Web Service extension to IIS 6.0" \(page 106\)](#).

Procedure 18**Adding a New ISAPI Web Service extension to IIS 6.0**

Step	Action
1	Open IIS Manager, expand the master server node, and select the Web service extensions node.
2	In the right pane of the IIS Manager, under Tasks, click Add a new Web service extension.
3	In the Extension name box, type a friendly name for the extension that you want to add (see Figure 50 "Enabling new ISAPI extension" (page 107)).
4	In the Required files box, click Add, and then select the path and the name of the file that handles requests for the specific extension. For Telephony Manager 3.1, the path and file name is <tmroot>/WebServices/OMNavigator/SystemNavigator/Bin/ISAPISystemNavigator.dll
5	Repeat step 4 for Jakarta ISAPI file. After selecting the path and file name (<tmroot>/Tomcat/Bin/ISAPI_redirector2.dll), click OK.
6	Click to select the Set extension status to Allowed check box.
7	Click OK to save your changes.

—End—

Figure 50
Enabling new ISAPI extension



Enabling parent paths

Parent paths are automated using the script.

Enabling parent paths specifies whether an ASP page permits paths relative to the current directory (using the `..\` notation).

In IIS 6.0, parent paths are no longer enabled by default. This affects Telephony Manager 3.1 as it has Web pages that contain the `#include` server-side include directive and uses (`..`) notation to refer to a parent directory.

Procedure 19

Enabling parent paths

Step	Action
------	--------

To enable parent paths:

- 1 In IIS Manager, expand the local computer, right-click the starting-point directory of the application (Default Web Site) that needs to be configured, and click Properties.
- 2 Click the Home Directory tab, and then click Configuration (see [Figure 51 "Enabling parent paths" \(page 108\)](#)).
- 3 Click the Options tab (see [Figure 52 "Options tab" \(page 108\)](#)).
- 4 In the Application configuration section, select the Enable parent paths check box.
- 5 Click OK.

Figure 51
Enabling parent paths

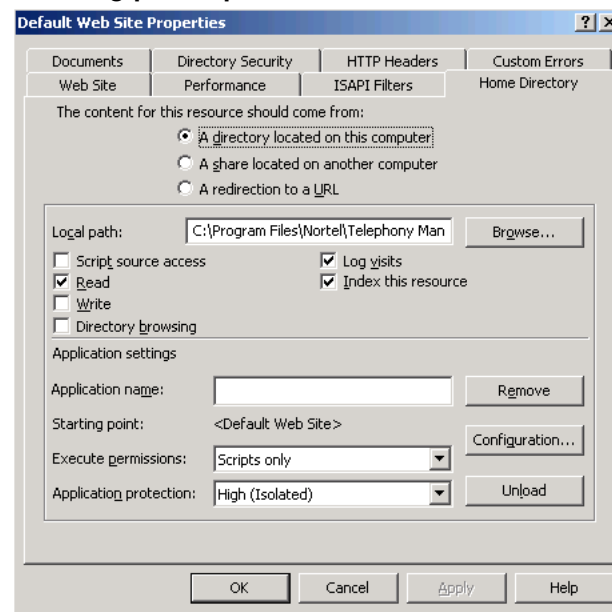
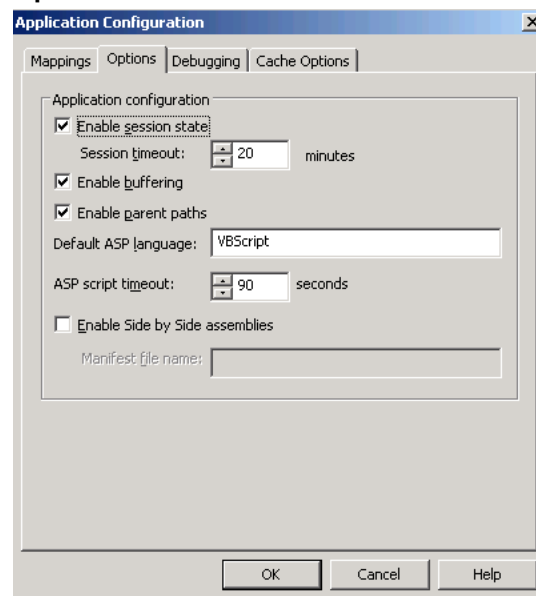


Figure 52
Options tab



—End—

IIS modes of operation

IIS modes of operation are automated using the script.

IIS 6.0 can run in one of two possible modes on Microsoft Windows Server 2003, IIS 5.0 isolation mode and worker process isolation mode. The default isolation mode of IIS 6.0 in Windows 2003 is worker process.

Telephony Manager 3.1 has characteristics that conflict with the worker process isolation mode, therefore IIS needs to be configured to run in IIS 5.0 isolation mode.

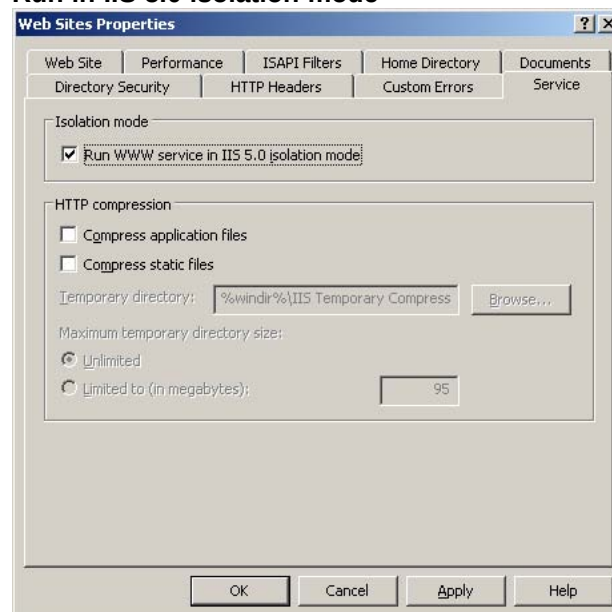
After completing the following procedure, you must restart the WWW service, which temporarily interrupts the service.

Procedure 20

Configuring IIS 5.0 isolation mode

Step	Action
1	In IIS Manager, expand the local computer, right-click Web Sites, and then click Properties.
2	Click the Service tab, select the Run WWW service in IIS 5.0 isolation mode check box, and then click OK (see Figure 53 "Run in IIS 5.0 isolation mode" (page 109)).
3	To restart the WWW service, click Yes.

Figure 53
Run in IIS 5.0 isolation mode



—End—

Adjusting Internet Explorer security settings

In Windows Server 2003, Internet Explorer is set to enhanced security configuration by default. The default settings of the security zones in Windows Server 2003 are also changed.

Telephony Manager 3.1 Web applications have functions that require privileges granted in the Medium-low default security template.

The following procedure, [Procedure 21 "Adjusting Internet Explorer security settings" \(page 110\)](#), describes one of the methods used to grant the required access rights to the Telephony Manager 3.1 Web site.

Procedure 21

Adjusting Internet Explorer security settings

Step	Action
1	In Internet Explorer, click on Tools and select Internet Options.
2	Click on the Security tab (see Figure 54 "Adding Trusted site" (page 111)).
3	Click on the Trusted sites icon.
4	Click Default Level to display slider.
5	Move the slider to select Medium security level for this zone (see Figure 54 "Adding Trusted site" (page 111)).
6	Click on Sites and add the Telephony Manager 3.1 Web site address to the list of trusted sites (see Figure 55 "Add the Telephony Manager 3.1 Web site" (page 111)).
7	Clear the Require server verification check box and click OK (see Figure 55 "Add the Telephony Manager 3.1 Web site" (page 111)).
8	Click OK to save your changes.

Figure 54
Adding Trusted site

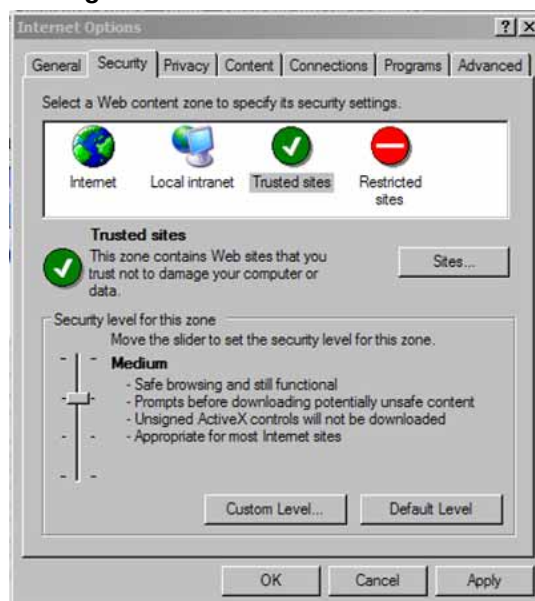
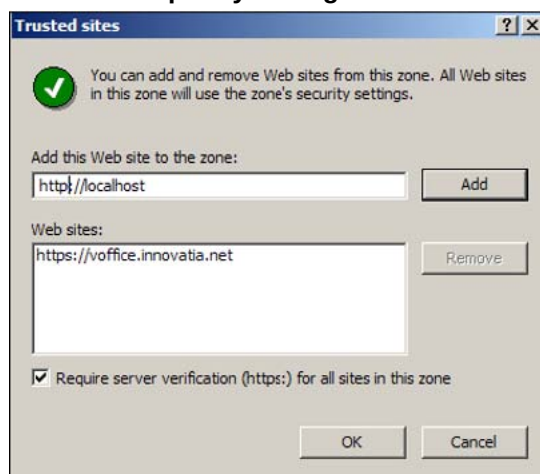


Figure 55
Add the Telephony Manager 3.1 Web site



—End—

Remote Desktop and Terminal Server

Remote Desktop for Administration and Terminal Server are components of Windows Server 2003. Terminal Server allows multiple remote clients to simultaneously access Windows-based applications that run on the server and Remote Desktop provides administrators with remote access to manage the server.

ATTENTION

If Terminal Server is enabled on the Telephony Manager Server, it can cause the following problems:

- When you use Remote Desktop for Administration, multiple instances of Telephony Manager may run. This leads to data corruption and Telephony Manager can exhibit unexpected behavior.
- If you have Terminal Services enabled on Telephony Manager Sever, the default Windows directory is **C:\Documents and Settings\Username\Windows**. If Terminal Services is not enabled on Telephony Manager Sever, the default Windows directory is **C:\Windows**. This change affects the applications installed on the server. In Telephony Manager, the TBS application fails to open the Call Database.

Nortel recommends you disable Terminal Services on the Telephony Manager Sever using the procedure "[Disable Terminal Services on the Telephony Manager Server](#)" (page 112).

Disable Terminal Services on the Telephony Manager Server

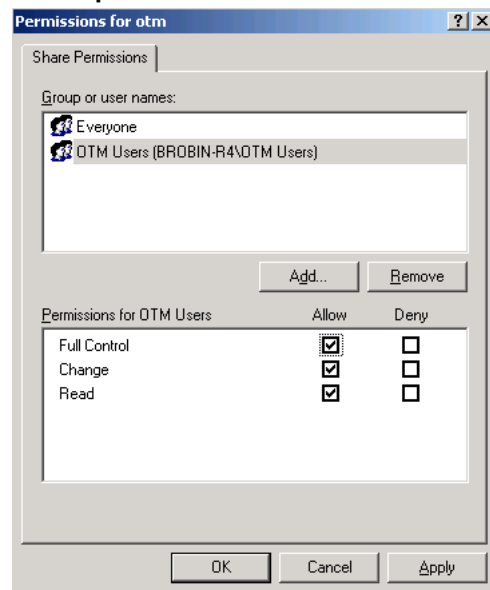
Step	Action
1	Go to Settings, Control Panel, Add/remove Programs .
2	Select Add/remove Windows components .
3	From the list populated, find the Terminal Services option. If it is checked, clear the checkbox.
4	Exit Add/remove Windows components .
5	Go to Settings, Control Panel, Administrative Tools, Services . - Right-click on Terminal Services and select Properties. - Change the startup type to Disabled. - Click Apply.
6	Exit Settings, Control Panel, Administrative Tools, Services .
7	Reboot the Telephony Manager Sever.

—End—

Telephony Manager 3.1 server-client setup

For a Telephony Manager 3.1 server-client setup, the Telephony Manager 3.1 root directory on the server must be given shared access. In Windows Server 2003, a shared directory is granted Read only permission by default. Ensure that **Full Control** permission is granted when assigning share permissions for the Telephony Manager 3.1 root directory see (see [Figure 56 "Share permissions" \(page 113\)](#)).

Figure 56
Share permissions



Configuring client authentication on the server side

The permissions in the Windows 2003 Service Pack 1 COM restrict remote calls that are not authenticated. Complete [Procedure 22 "Configuring client authentication on the server side" \(page 114\)](#) procedure to allow Telephony Manager 3.1 clients to authenticate to the Telephony Manager 3.1 server - for client authentication, to grant remote access, launch and activation permissions to Anonymous Logon.

For more information, refer to the following URL:

<http://support.microsoft.com/?kbid=892500>

Procedure 22**Configuring client authentication on the server side****Step Action**

- 1 Click Start, click Administrative Tools, Component Services.
- 2 Expand the Component Services\Computers container.
- 3 Right-click My Computer, click Properties (see [Figure 57 "Component Services" \(page 114\)](#)).
- 4 On the COM Security tab, click Edit Limits in the Access Permissions (see [Figure 58 "Com Security tab" \(page 115\)](#)).
- 5 Add Anonymous to the list of user names and click Allow for Remote Access permissions (see [Figure 59 "Access Permissions" \(page 115\)](#)).
- 6 Click OK to accept the change.
- 7 On the COM Security tab, click Edit Limits in the Launch and Activation Permissions area. (see [Figure 58 "Com Security tab" \(page 115\)](#)).
- 8 Add Anonymous to the list of user names and click Allow for Remote Launch and Activation permissions (see [Figure 60 "Launch Permission" \(page 116\)](#)).
- 9 Click OK to accept the change (see [Figure 60 "Launch Permission" \(page 116\)](#)).

Figure 57
Component Services

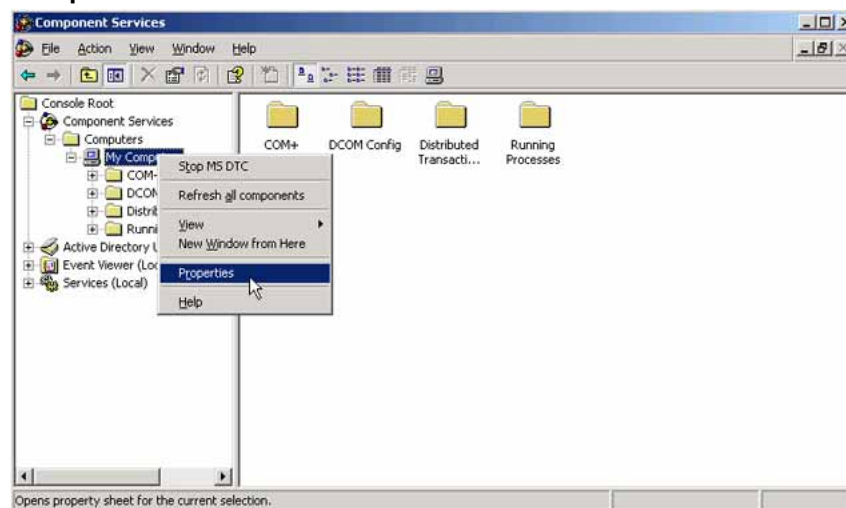


Figure 58
Com Security tab

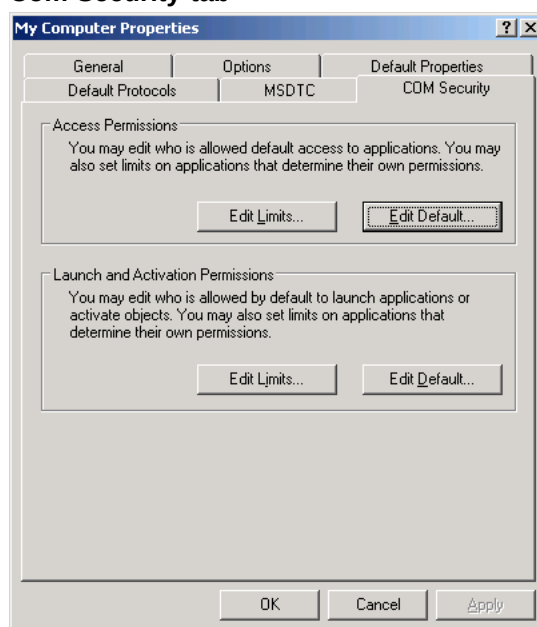


Figure 59
Access Permissions

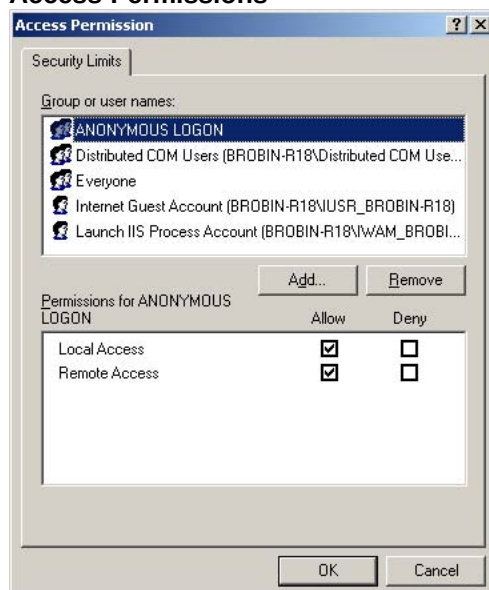
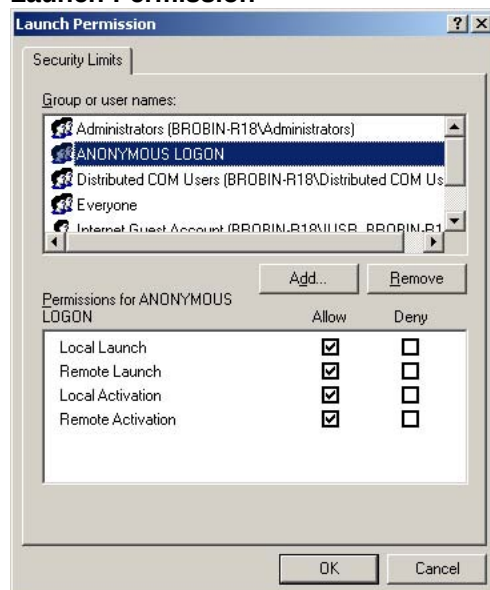


Figure 60
Launch Permission



—End—

Data Execution Prevention Settings

Data Execution Prevention (DEP) settings can cause applications within Telephony Manager to not execute, therefore you must ensure that (DEP) settings are appropriately set. DEP is controlled through parameters in the BOOT.ini file which can be set in the System dialog box in Control Panel.

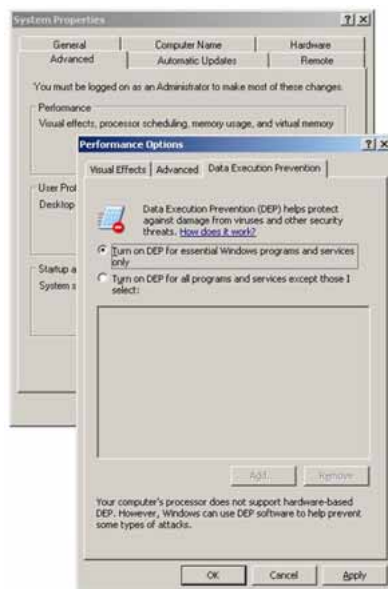
By default the parameter is **OptIn** which enables DEP only for system binaries and applications that opt in. An **OptOut** parameter enables DEP for all processes. If DEP is not to be applied to a particular process, that process should be manually added to the exception list. For details, refer to www.support.microsoft.com.

The following figures detail the two ways by which the changes can be effected.

Figure 61
DEP OptIn parameter selected



Figure 62
DEP OptOut parameter selected



<http://support.microsoft.com/kb/875352>

Configuring security for Telephony Manager 3.1

To configure security in Windows 2003, first install the Security Configuration Wizard. In Control Panel, choose Add/Remove Programs, then click on the Add/Remove Windows Components box to the left of the window. From the components list, check Security Configuration Wizard.

ATTENTION

IIS and FTP services must be installed before completing this procedure ([Procedure 23 "Configuring security for Telephony Manager 3.1" \(page 118\)](#)).

Procedure 23

Configuring security for Telephony Manager 3.1

Step	Action
------	--------

- | | |
|---|---|
| 1 | Run the Security Configuration Wizard from Start > Programs > Administrative Tools (see Figure 63 "Security Configuration Wizard" (page 118)). Click Next . |
|---|---|

Figure 63
Security Configuration Wizard



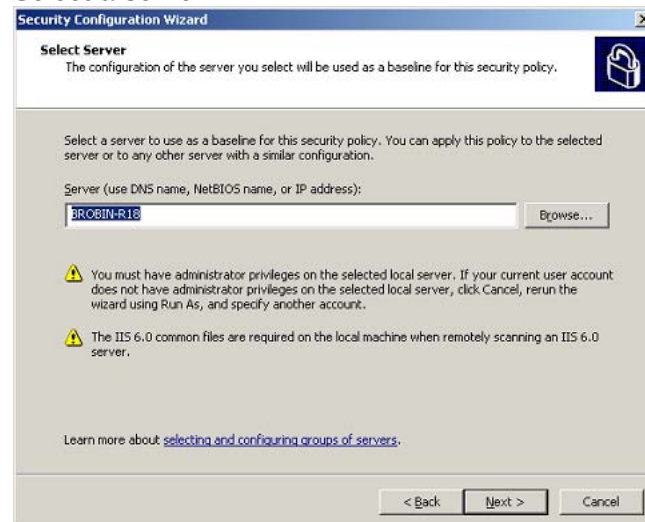
- | | |
|---|--|
| 2 | The Configuration Action window appears (see Figure 64 "Create a new security policy" (page 119)). Select Create a new security policy . |
|---|--|

Figure 64
Create a new security policy



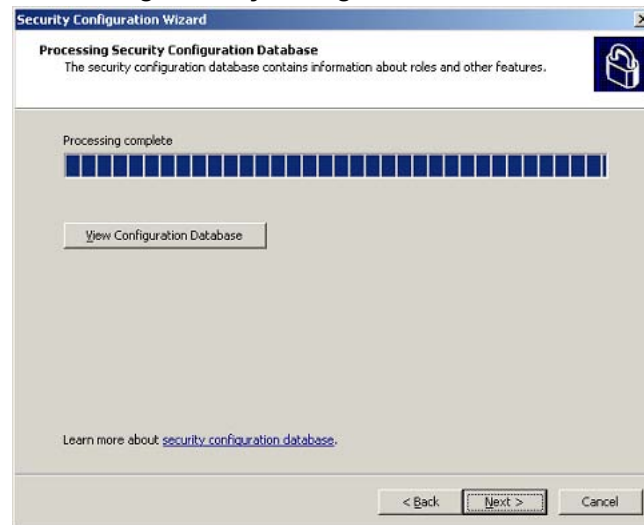
- 3 Click **Next**. The Select Server window appears (see [Figure 65 "Select a server"](#) (page 119)). Select or enter a server name. Click **Next**.

Figure 65
Select a server



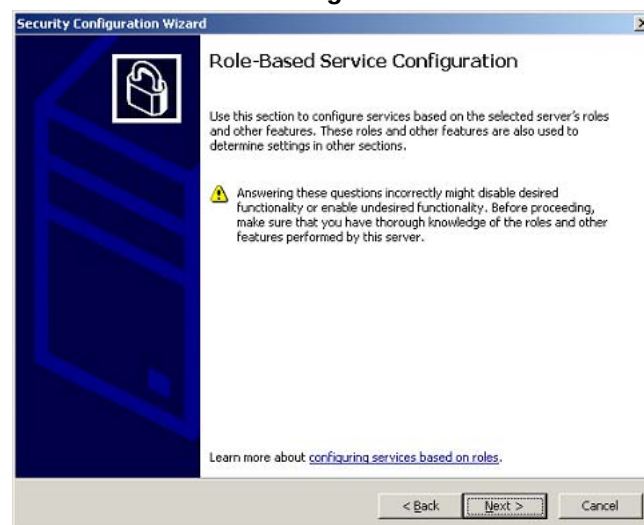
The Processing Security Configuration Database screen appears (see [Figure 66 "Processing security configuration database"](#) (page 120)).

Figure 66
Processing security configuration database



- 4 Click **Next**. The Role-Based Service Configuration window appears (see Figure 67 "Role based service configuration" (page 120)).

Figure 67
Role based service configuration



- 5 Click **Next**. The Select Server Roles window appears. Ensure your selected server roles match those in Figure 68 "Role-based service configuration - installed roles" (page 121) and Figure 69 "Role-based service configuration - installed roles, scrolled down" (page 121), and Figure 70 "Role-based service configuration - selected roles"

(page 122) and Figure 71 "Role-based service configuration - selected roles, scrolled down" (page 122), and click **Next**.

Figure 68
Role-based service configuration - installed roles



Figure 69
Role-based service configuration - installed roles, scrolled down

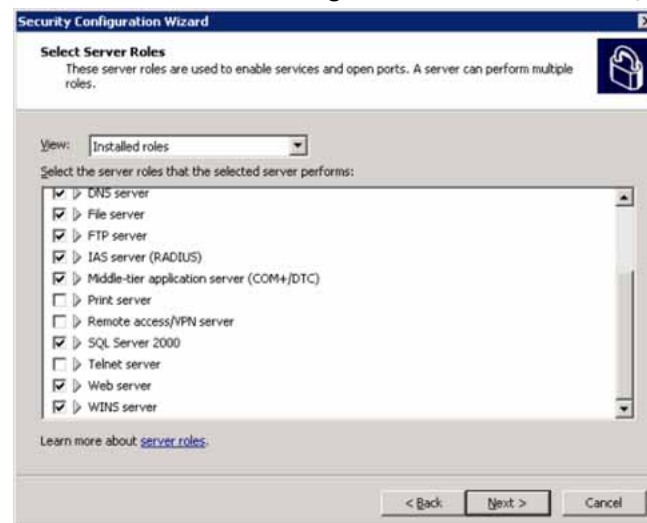


Figure 70
Role-based service configuration - selected roles

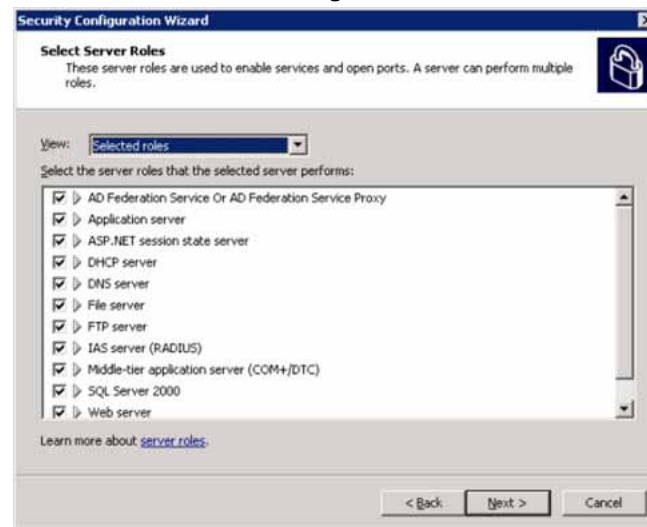
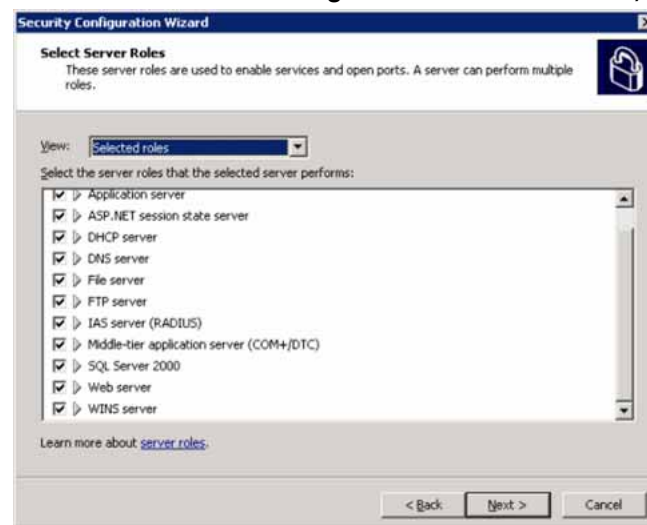
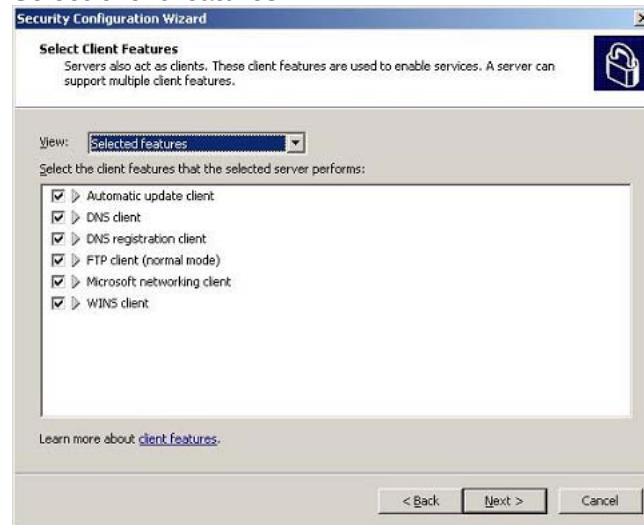


Figure 71
Role-based service configuration - selected roles, scrolled down



- 6 The Select Client Features screen appears (see [Figure 72 "Select client features"](#) (page 123)). Place a check mark in each box and click **Next**.

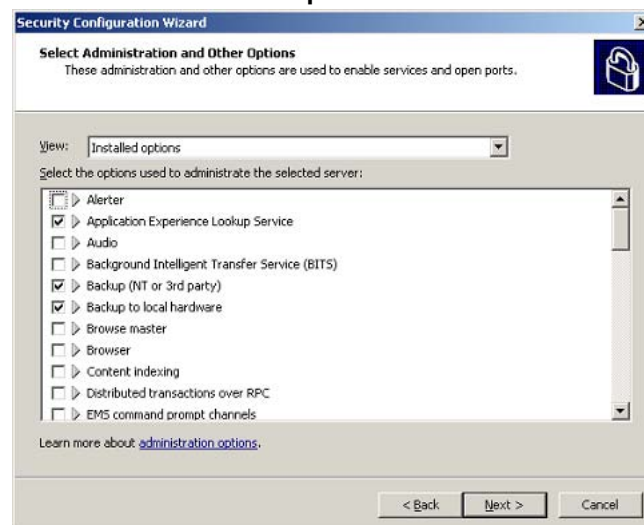
Figure 72
Select client features



- 7 The Select Administration Options window appears (see [Figure 73 "Select administration options" \(page 123\)](#)). Accept the defaults for all options, ensuring the following options have check marks:

- IIS 5.0 compatibility mode
- Task Scheduler

Figure 73
Select administration options



ATTENTION

Ensure the checks for the following Administration Options are removed, as these options are not supported:

- Remote desktop administration
- Remote windows administration
- Terminal Server clustering
- Windows Firewall

The correct selected options are shown in [Figure 74 "Select administration options"](#) (page 124) and [Figure 75 "Select administration options"](#) (page 125). Click **Next**.

Figure 74
Select administration options

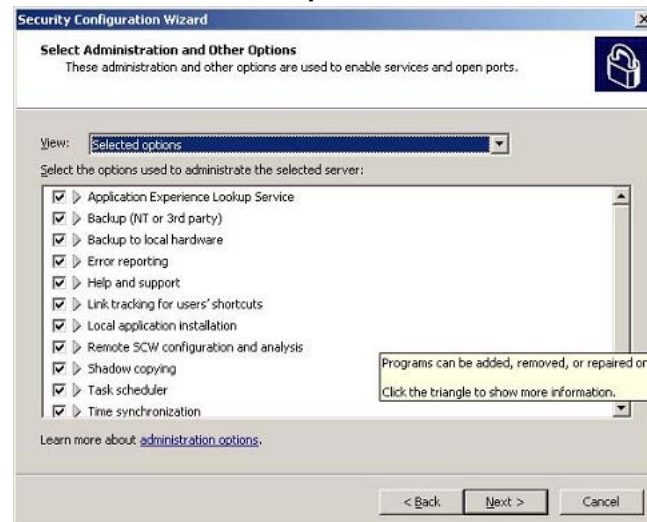
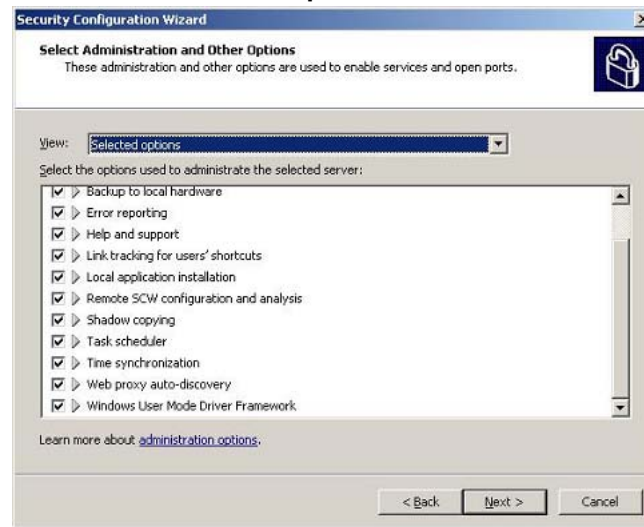


Figure 75
Select administration options



- 8 The Select additional services window appears (see [Figure 76 "Select additional services" \(page 126\)](#)). Accept the defaults for all options, ensuring the following options have check marks:

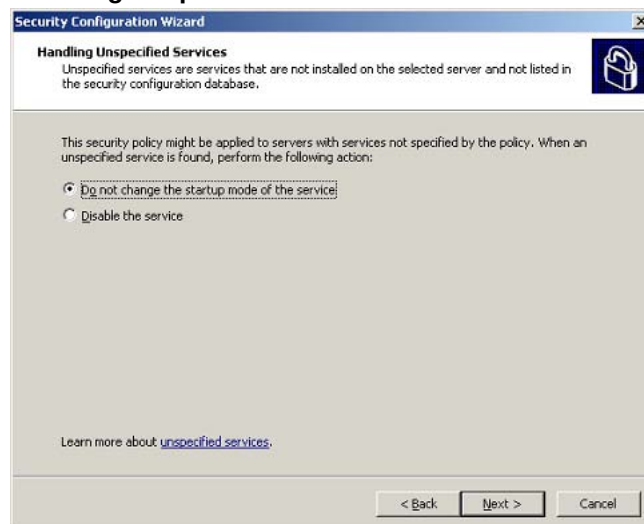
- Apache Tomcat
- Common Network Directory
- TMResourceManager
- TMSingletonServer
- TMTaskScheduler
- TMWatchdog
- PostgreSQL Database Server

Figure 76
Select additional services



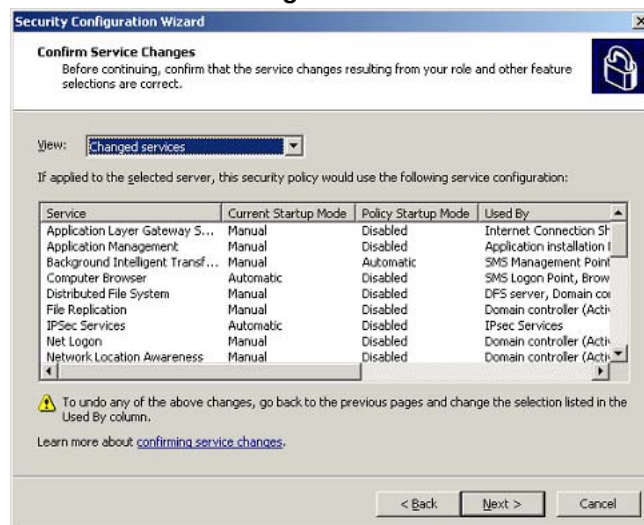
- 9 Click **Next**. The Handling Unspecified Services window appears (see [Figure 77 "Handling unspecified services" \(page 126\)](#)). Select **Do not change the startup mode of this service**.

Figure 77
Handling unspecified services



- 10 Click **Next**. The Confirm service changes window appears (see [Figure 78 "Confirm service changes" \(page 127\)](#)).

Figure 78
Confirm service changes



- 11 Click **Next**. The Network security window appears (see [Figure 79 "Network security" \(page 127\)](#)). **DO NOT place** a check mark in the **Skip this section** check box.

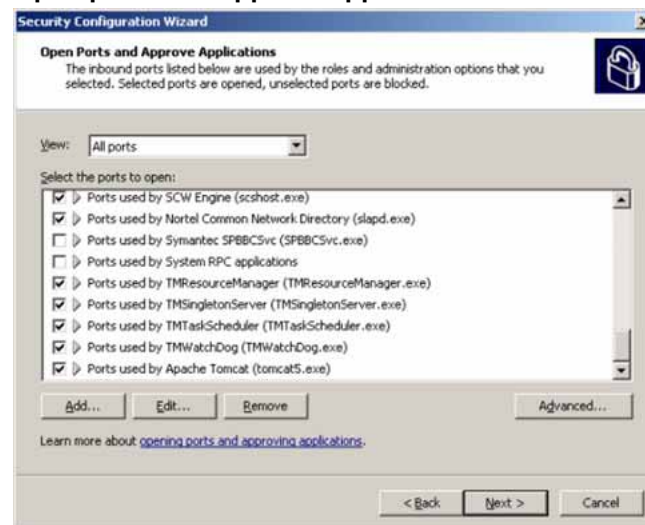
Figure 79
Network security



- 12 Click **Next**. The Open Ports and Approve Applications window appears (see [Figure 80 "Open ports and approve applications" \(page 128\)](#)). Accept the defaults, ensuring inclusion of the following:
- Nortel Common Network Directory

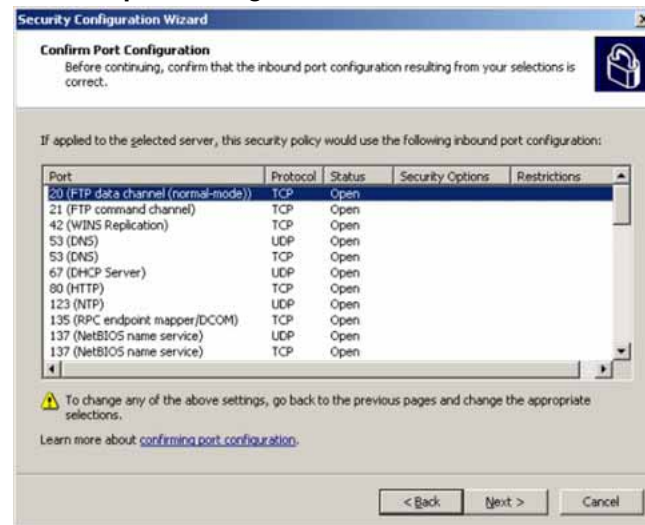
- TMResource Manager
- TMSingletonServer
- TMTaskScheduler
- TMWatchdog
- PostgreSQL
- Apache Tomcat

Figure 80
Open ports and approve applications



- 13** Click **Next**. The Confirm Port Configuration screen appears (see Figure 81 "Confirm port configuration screen" (page 129)).

Figure 81
Confirm port configuration screen



- 14 Click **Next**. The Registry Settings window appears (see [Figure 82](#) "Registry settings" (page 129)). Place a check mark in the **Skip this section** check box.

Figure 82
Registry settings





CAUTION

Do not attempt to edit the Windows Registry. Doing so may result in system failure.

- 15 Click **Next**. The Audit Policy window appears (see [Figure 83 "Audit policy" \(page 130\)](#)). Place a check mark in the **Skip this section** check box.

Figure 83
Audit policy



- 16 Click **Next**. The Internet Information Services window appears (see [Figure 84 "IIS" \(page 131\)](#)). **DO NOT place** a check mark in the **Skip this section** check box.

Figure 84
IIS



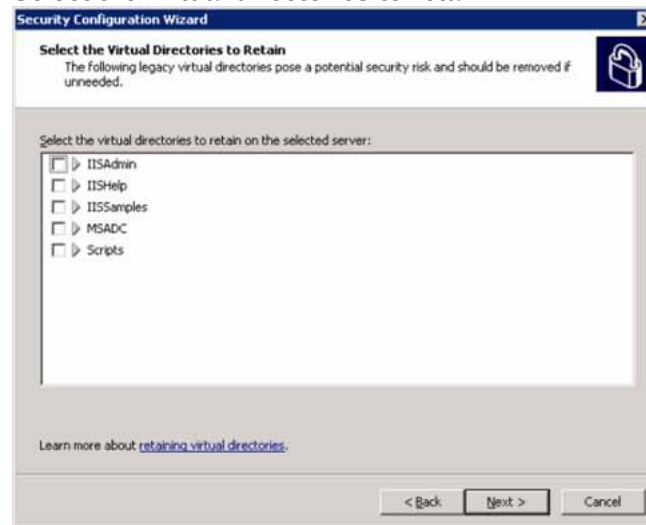
- 17 Click **Next**. The Select Web service extensions for dynamic content window appears. Place check marks in the check boxes to match those shown in Figure 85 "Select Web service extensions for dynamic content" (page 131).

Figure 85
Select Web service extensions for dynamic content



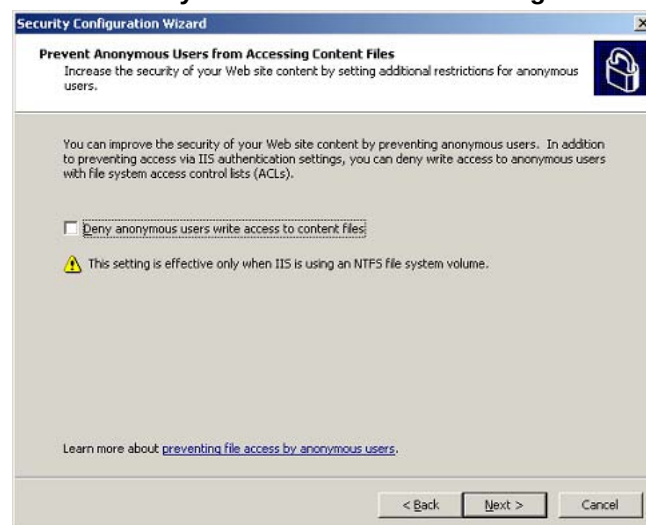
- 18 Click **Next**. The Select the Virtual Directories to Retain screen appears (see Figure 86 "Select the virtual directories to retain" (page 132)).

Figure 86
Select the virtual directories to retain



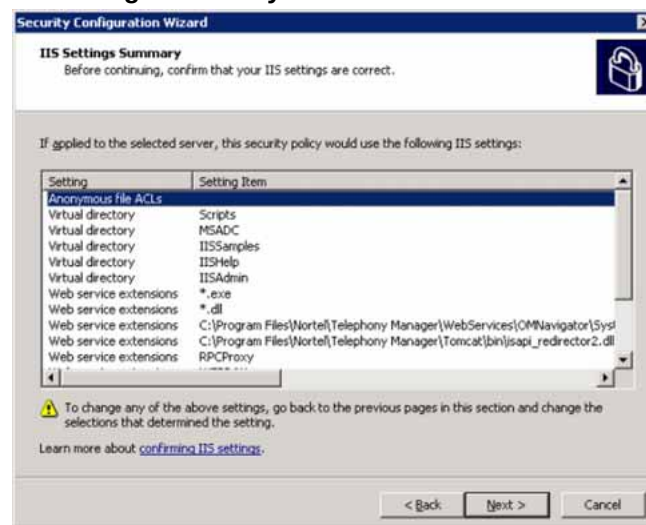
- 19 Click **Next**. The Prevent anonymous users from accessing content files screen appears. **DO NOT place** a check mark in the box called "Deny anonymous users write access to content files" (see [Figure 87 "Prevent anonymous users from accessing content files"](#) (page 132)).

Figure 87
Prevent anonymous users from accessing content files



- 20 Click **Next**. The IIS Settings Summary screen appears (see [Figure 88 "IIS settings summary"](#) (page 133)). Click **Next**.

Figure 88
IIS settings summary



- 21** After clicking **Next** on the IIS Setting Summary windows, save the Security Policy, apply the Security Policy, and reboot the system.

—End—

Adding Telephony Manager 3.1 Web users

Contents

This chapter contains information about the following topics:

"Overview" (page 135)

"Capabilities" (page 135)

"User logon and security" (page 136)

"Access permissions" (page 137)

"User authentication" (page 138)

"User groups" (page 140)

"Installing and configuring desktop services" (page 147)

Overview

This chapter contains information about:

- Web capabilities
- User logon and security
- Access permissions
- User authentication
- User groups
- Desktop services

Capabilities

For details on Telephony Manager 3.1 Web capabilities, see *Telephony Manager 3.1 System Administration (NN43050-601)*.

User logon and security

Users log on to the Telephony Manager 3.1 Web using their Windows userID and password. Logon security for Telephony Manager 3.1 Web services ensures protection against unauthorized entry and enforces access permissions for logged-on users.

CND authentication is the only supported authentication method for Desktop Services (End Users). All 3 authentication methods (local, domain, and CND) are supported in both Windows and Web administrator logon.

There are three categories of users:

- Administrators — Telephony Manager 3.1 administrators
- HelpDesk — Telephony Manager 3.1 Help desk users
- EndUser — Telephony Manager 3.1 end users

In addition, there is a Default user category. Default users can successfully log on to the Web, but they do not have an access profile defined in their Directory record.

Telephony Manager 3.1 administrators and Help desk users have user accounts in a Windows domain. End-users must have accounts either in a Windows domain or through an CND server. Telephony Manager 3.1 administrators must be set up in a Windows Administrator group on the server itself, not on a remote computer.

Telephony Manager 3.1 administrators and Help desk users can access and change their own telephones through either the Web or the Desktop Services end user pages. Access to the end-user pages requires the appropriate CND Directory setup (user logon and user group) for these administrators and Help desk users.

Telephony Manager 3.1 Web application access permissions are controlled by the administrator on a per-Windows user group basis. For example, the administrator can limit the Telephony Manager 3.1 user's access to only some of the Telephony Manager 3.1 Web-based functionality. The Telephony Manager 3.1 Web controls access to applications by shielding Web links to which the user does not have access. The directories and files comprising those applications are similarly protected.

Configure Windows® 2000 user groups and individual users using the Windows user interface on the Telephony Manager 3.1 server and then determine the access permissions for each user group by using the Telephony Manager 3.1 Web page. For information about setting user access, refer to ["User groups" \(page 140\)](#).

Precaution

As a security precaution, with any upgrade or reinstallation of Telephony Manager 3.1 software, access profiles for all user groups except Administrator are reset. Any member of the Administrator user group can log on and set up access profiles for members of the HelpDesk, end-user, and default plug-ins.

Plug-ins

When an administrator or HelpDesk user first points a browser to the Telephony Manager 3.1 Navigator Web site, a check is performed to see if the user has the required Telephony Manager 3.1 Java plug-in. If the plug-in is not installed, the administrator or Help desk user is given the option of downloading and installing the plug-in. This operation is similar to the standard download operations in that the user must download the plug-in to the user's hard disk, and then it installs itself onto the computer.

The plug-in check is performed the first time the application is launched.

Default URL

The default Telephony Manager 3.1 URL is the end user logon page. To navigate to the administrator logon page, place `/admin` after the Telephony Manager 3.1 IP address or host name.

Example: `http://TM 3.1 IP address or host name/admin`

Access permissions

When Telephony Manager 3.1 starts for the first time, the Administrator profile is the only active profile. Access permissions for the other Windows XP or Windows 2000 Groups that have been set up on the Telephony Manager 3.1 server must be assigned.

Administrator Group access permissions

Persons belonging to the Administrators user group on the Telephony Manager 3.1 server can log on to the Telephony Manager 3.1 Web site and get unrestricted access. The Administrators group has unrestricted access by default. Access permissions for the Administrators user group cannot be altered.

French or German OS Administrator groups

Important advice for localized OS — The name of the administrators user group in the French and German operating systems is not Administrators. These names are localized by Microsoft in the regional operating system software. In a default French installation the local administrators user group is Administrateurs. In the German version, this user group is

Administratoren. When installed on a French or German OS, the Telephony Manager 3.1 predefined administrators user group is named Administrateurs or Administratoren to match the OS.

User group access rights

The network administrator logs into the Telephony Manager 3.1 Administration Web site and assigns access rights to the other user groups. By default, a member of any group other than Administrators does not have any access to Telephony Manager 3.1 Web applications unless appropriate permissions are specifically granted to that group.

From the User Groups page, access to Web applications to a group, not to individual users, are either granted or denied. To change the security access for individual users, their group membership can be changed. For new groups, the Administrator must assign access rights for Web applications before any users from that group can log on. For information about setting user access, refer to "[User groups](#)" (page 140).

With the exception of Administrators, a person is not placed in multiple groups. The first group detected by Telephony Manager 3.1 is used to determine access permissions. There is no restriction on the Administrators group. Users can belong to other groups, but if they belong to the Administrators group, the Administrators profile overrides all other profiles.

While assigning access permissions, be certain that the top-level application for every sub-application assigned is selected. For example, if selecting System Alarms, Equipment must also be selected. Failure to do so can result in members of the user group denied access to the Web site.

User authentication

One of the following methods can be selected to authenticate Telephony Manager 3.1 users:

- Local server account
- Windows domain account
- CND authentication

The Administrator account is always authenticated through the local server account because it is a default account on all supported Windows platforms.

The default authentication method is the Local Telephony Manager 3.1 server account. This method provides the best logon performance because there is no requirement to search the CND Directory for the user's assigned User Group.

Procedure 24

Configuring authentication

Step Action

To configure authentication:

- 1 Under Web Administration in the Telephony Manager 3.1 Web tree, select **User Authentication**.

The User Authentication page appears. See [Figure 89 "User Authentication page"](#) (page 139).

Figure 89
User Authentication page

- 2 Use the check boxes to select one or more of the available authentication methods. If CND authentication is selected, use the drop-down list to choose either Common Name, EmployeeID, or E-mail.
- 3 Use the drop-down lists to assign the order in which the authentication methods are performed.

If multiple authentication methods is selected, Telephony Manager 3.1 respects the configured order; however, note that the best performance is achieved by using the Local Telephony Manager 3.1 server account method.
- 4 To use the SSL during the authentication process, the Telephony Manager 3.1 server must have the required certificate installed as described in ["Configuring Secure Sockets Layer \(SSL\)"](#) (page 85).

Click the **Use SSL for Web logon authentication** check box after installing the certificate.

If the Telephony Manager 3.1 server has the required certificate installed, selecting the check box causes Telephony Manager 3.1 to use SSL-encrypted transport during authentication. In this case, Web logon is performed using https:// rather than http://, and the traffic is encrypted. The Telephony Manager 3.1 server automatically switches to non-SSL transport when the user is successfully authenticated.

- 5 The selected method(s) are used to authenticate users on all Telephony Manager 3.1 platforms: Telephony Manager 3.1 server, Telephony Manager 3.1 client, and Telephony Manager 3.1 Web client.

—End—

For information about configuring users for desktop access, see ["Enable Web desktop access in the CND Directory"](#) (page 148).

Authentication methods can also be configured using the Windows navigator. See ["User authentication"](#) (page 138).

User groups

Navigator access is controlled by user group. A user's user group assignment determines which features are available on the Telephone features page. The User Groups page is also used to indicate which users are permitted to make changes to the General and Keys pages.

User groups must be added and deleted in the Telephony Manager 3.1 Windows Navigator.

Telephony Manager 3.1 is shipped with the following user groups and corresponding access rights:

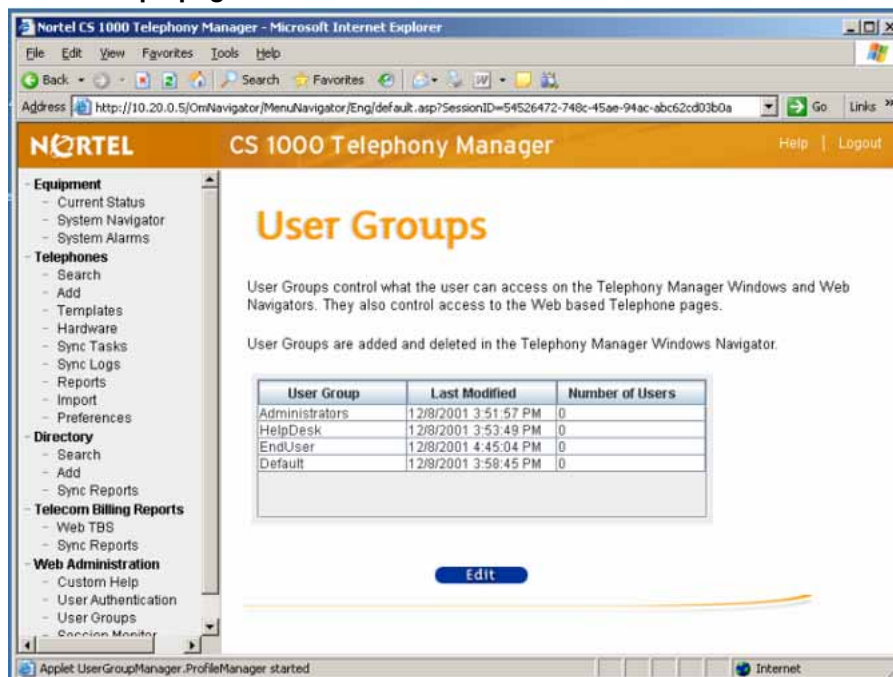
- Administrators
 - Full read/write access rights. Access rights cannot be changed for this user group.
- HelpDesk
 - Full access to all Web tree items except those under Web Administration.
 - Full access to Web Desktop Services, including read/write and synchronization capabilities.

- Full access to Windows Navigator applications with the exception of ITG Services.
- EndUser
 - No access to Web or Windows Navigator applications.
 - Web Desktop Services is read-only. Only 21 features are available; the rest are hidden.
- Default
 - No access.

To view the available user groups, click the **User Groups** link located under Web Administration in the Telephony Manager 3.1 Web tree.

The **User Groups** page appears. See [Figure 90 "User Groups page" \(page 141\)](#).

Figure 90
User Groups page



Navigator access

Access to the sites, systems, and applications available in both the Windows and Webs is controlled on a user-group basis through the User Group Properties Java application.

When the user group name is entered into the User Group field in an Telephony Manager 3.1 user's directory record, the entry must match the user group name exactly. This is primarily a concern when Telephony Manager 3.1 is operating in a language other than English. In this case, the access profile name HelpDesk can have been translated into the local language.

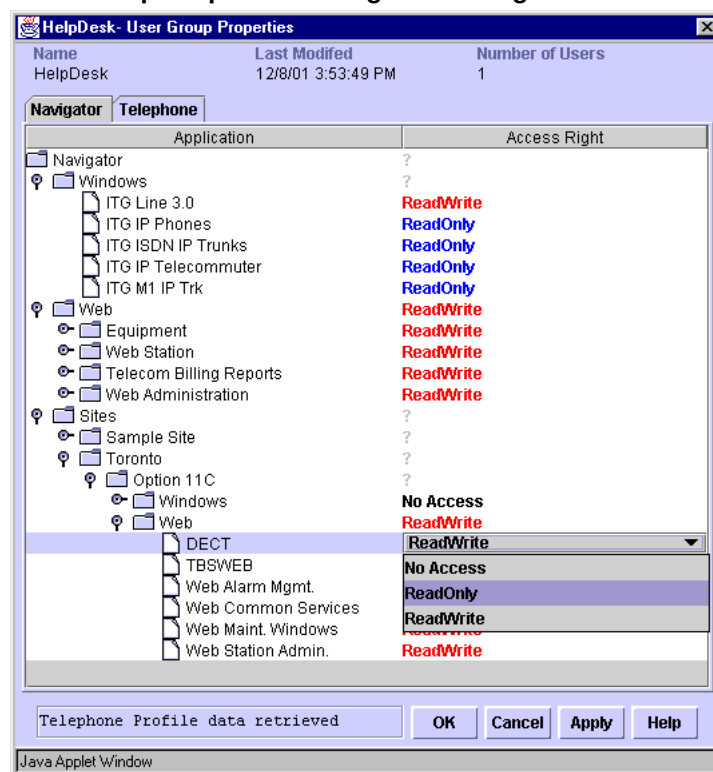
To modify the access rights of a user group:

Step	Action
1	Click to select a User Group.
2	Click Edit .
—End—	

The User Group Properties Java application launches, and the User Group Properties dialog box for the selected user group appears. See [Figure 91 "User Group Properties dialog box: Navigator tab" \(page 143\)](#).

Alternatively, double-click the user group to display the **User Group Properties** dialog box for the selected user group.

Figure 91
User Group Properties dialog box: Navigator tab



The Access Right column lists the level of access allowed for each site, system, and application. This is the same tree structure and performs the same function as the Windows-based New User Group Properties dialog box.

The question mark indicates that the sub-items belonging to the item displaying the question mark have mixed access settings.

To modify access rights:

- | Step | Action |
|------|--|
| 1 | Use the drop-down list to select ReadWrite , ReadOnly , or No Access for each item in the tree. |
| 2 | Click Apply . |

—End—

Telephone access

The Telephone tab in the User Group Properties dialog box is used to control access to the telephone pages on the Web for each user group. See [Figure 92 "Telephone access properties dialog box: Keys tab" \(page 145\)](#).

The options that are configured in the upper section of this dialog box are applicable to all of the tabs in telephone pages. These options include:

- Allowing or denying this group the ability to synchronize changes with the system. If synchronization is denied, the changes must be manually synchronized with the system using Station Administration.
- Determining whether the troubleshooting link appears at the top of the telephone page for members of this group.
- Allowing or denying this group the ability to restore changes made to a telephone.

Procedure 25

Configuring telephone access options

Step	Action
------	--------

- | | |
|---|--|
| 1 | Select Allow user to synchronize changes check box. |
| 2 | Select Show Trouble Shooting link check box to enable this option.

For EndUsers, clicking the link appears the Telephone Troubleshooting Help page which includes a reset button.

For Web users, clicking the link appears the maintenance page for the telephone with all of the available commands. |
| 3 | Select Allow users to restore pending changes check box to permit the users in this group to restore the changes made to a telephone. |
| 4 | Click Apply . |
-

—End—

Keys tab

In the Keys tab, see [Figure 92 "Telephone access properties dialog box: Keys tab" \(page 145\)](#), the check box and lists of key-based features can be used to determine whether the Telephone—Keys page appears and, if so, which keys the users in this group can change.

Figure 92
Telephone access properties dialog box: Keys tab



Procedure 26
Configuring the Telephone: Keys page

Step Action

- 1 Go to the Telephone—Keys page.
- 2 Use the Move and Move All buttons to move the key-based features that this user group can change into the left column.
 By putting keys into the left column, users in this group can interchange these key types and change the key parameters.
 If the user selects a key that is not in the left-hand column while viewing the Telephone—Keys page, the Change button does not appear.
- 3 Click **Apply** to apply your changes.

—End—

Features tab

In the Features tab (see [Figure 93 "Telephone access properties dialog box: Features tab"](#) (page 146)), use the check box and list of features to determine whether the Telephone—Features page appears and, if so, which features the users in this group can view and change. The list of features contains all the non-key features listed alphabetically by prompt in LD 10 and LD 11. Each feature is assigned a restriction of Hidden, ReadOnly, or ReadWrite. If Hidden, the feature does not appear in the end user Feature drop-down list.

Read/Write capability requires the Telephony Manager 3.1 Premium package.

Figure 93

Telephone access properties dialog box: Features tab

Administrators- User Group Properties

Name: Administrators Last Modified: 12/2/2005 4:05:20 PM Number of Users: 0

Navigator: Telephone

General Properties: Read-Write Show Trouble Shooting link: ☒

Directory Options: Read Write Allow user to restore pending changes: ☒

Keys: Read Write Allow user to synchronize changes: ☒

Features: Read Write

Administration: Read Write

Keys: Features

Set each feature to be hidden, read only or read/write Show: All

Restrictions for telephone features page

Mnemonic	Description	Restrictions
AAA	AAA	ReadWrite
AACD	AACD	ReadWrite
ABDA	ABDA	ReadWrite
ADAY	ADAY	ReadWrite
ADCP	ADCP	ReadWrite
ADV	ADV	ReadWrite
AEFD	AEFD	ReadWrite
AEHT	AEHT	ReadWrite

Telephone Profile data retrieved successfully OK Cancel Apply Help

Java Applet Window

To configure the Telephone - Features page, see [Procedure 27 "Configuring the Telephone: Features page"](#) (page 147)

Procedure 27**Configuring the Telephone: Features page**

Step	Action
1	Go to the Telephone—Features page. Use the drop-down lists in the Restrictions column to configure each feature as ReadWrite, ReadOnly, or Hidden. The Show drop-down list contains All, Hidden, ReadOnly, and ReadWrite. This is used to limit the size of the list.
2	Click Apply .

—End—

Installing and configuring desktop services

The following procedure outlines the steps required to install and configure Desktop Services.

Procedure 28**Installing and Configuring Desktop Services**

Step	Action
1	Install Telephony Manager 3.1. "Adding Telephony Manager 3.1 Web users" (page 135) .
2	Create accounts for Help Desk users and End Users as required.
3	log on to the Web as Administrator, and go to the User Groups page. To navigate to the Administrator logon page, place <code>/admin</code> after the Telephony Manager 3.1 IP address or host name in the Web browser. Example: <code>http://TM 3.1 IP address or host name/admin</code>
4	Configure the Help Desk, Default, and End User Access Profiles as desired. By default, Help Desk users are given read/write access to all features. Default and End Users have read-only access to 21 features. To enable Help Desk users to make changes to other user's telephone configuration data, make sure that they have access to the Find Telephones page.

- 5 Enter the Help Desk user's logon Name and Access Profile in the user's CND Directory entry. "[Enable Web desktop access in the CND Directory](#)" (page 148).
- 6 Enter the End User's logon Name and Access Profile in the user's CND Directory entry. See "[Enable Web desktop access in the CND Directory](#)" (page 148) next.
- 7 Select the desired Web Reporting Role in the user's CND Directory entry.

—End—

Enable Web desktop access in the CND Directory

End users access the Telephony Manager 3.1 Desktop Services Web site to view information about, and make changes to, their telephones.

Although end users can be given a Telephony Manager 3.1 user account similar to Navigator users, the only supported authentication method for end users is CND authentication.

For end users, the following attributes must be configured in the CND users record through the Directory section of the Web Navigator.

- logon name. When configuring CND authentication, the logon name can be one of the following:
 - commonName
 - e-mail
 - employee number
- User group
- Web Reporting Access Rights

For end user reference information, and for information about populating entries using CND import and CND sync, see *Common Network Directory 2.1 Administration Guide (NN43050-101)*.

For information about configuring users in CND, see *Common Network Directory 2.1 Administration Guide (NN43050-101)*.

Configuring a modem for Telephony Manager 3.1 applications

Contents

This chapter contains information about the following topics:

["Using installation tools" \(page 149\)](#)

["Configuring high-speed smart modems" \(page 150\)](#)

["Troubleshooting modem connections" \(page 151\)](#)

Using installation tools

To ensure that a modem is configured correctly for use with Microsoft operating systems, use the modem control panel to configure it. The modem control panel automatically searches for and detects a connected modem, and then stores the configuration information in the registry for other Windows applications to access.

The same is also true for Telephony Manager 3.1 applications, where the modem configuration information is obtained by searching the Windows registry with the COM port specified in the communication profile. Telephony Manager 3.1 communications software then sets up the Run-Time-Container (RTC) with the modem-initialization string and communication-profile settings for the application to make its connection to the system.

Limitations

When configuring modems, the following limitations with this process must be taken into account:

- The Windows Modem control panel allows multiple modems to be configured on the same COM port, however to ensure proper modem operation, configure only one modem or communication device on a given COM port.
- A factory modem-initialization (INIT) string is stored in the Windows registry. Telephony Manager 3.1 applications use this INIT string to set

up the modem connection. The Telephony Manager 3.1 communications software is written to use verbal (V1) result code. If the factory INIT string is set to use numeric (V0) result code, the "Can't set modem parameters" error message occurs and the dial-up attempt is aborted. To change the factory INIT string to use verbal (V1) result code, follow the steps in [Procedure 29 "Changing the factory INIT string" \(page 150\)](#).

Procedure 29**Changing the factory INIT string**

Step Action

- | | |
|---|---|
| 1 | From the Start menu, select Settings > Control Panel > Phones and Modems > Properties > Advanced . |
| 2 | Type in the appropriate INIT string. |
-

—End—

Configuring high-speed smart modems

As modem technology progresses, the new generation of high-speed modems provides additional functionality to achieve the highest possible connection rate. These high-speed smart modems use various tones during the handshaking period to negotiate the speed and protocol.

SDI port

The modem configured on the SDI port needs extra attention. In most cases, the modem attached to the SDI port is configured to run in dumb mode at the same speed for which the system SDI port is configured (at 9600 bps or less). This locks the modem into a specific mode of operation, preventing it from running in command mode (echo input) or from connecting at a different baud rate than is configured for the system SDI port.

Prevent lockup

When a high-speed smart modem is used on the Telephony Manager 3.1 PC to dial up the system modem, the PC modem always attempts to connect at its highest possible speed. The system's modem, however, can only connect at the configured speed. Therefore, during the modem online handshaking period, the PC modem sends out different tones to negotiate the speed and protocol, and the switch modem connects at its configured speed and ignores additional attempts.

When the switch modem is connected, any additional handshaking tones sent by PC modem are translated into data (garbage under this condition) and forwarded to the system SDI port. These garbage characters can eventually lock up the system port. The two modems can still be connected, but access to the system overlay input is no longer possible.

To avoid this type of problem, the key is to maintain modem compatibility. To avoid potential problems and increase the connection success rate:

- Configure the PC modem to match the switch modem's settings.
- The speed between the system SDI port and the system's modem is locked to the system SDI port's baud rate if a high-speed modem is installed on the SDI port.
- To minimize the garbage characters after carrier-detect or carrier-lost situations, set your modem S9 register to a higher value (for example, 30 = 3 seconds) and S10 register to a lower value (for example, 7 = 7/10 of a second).

When increasing the value of the S9 register, timing adjustments on some of the modem/buffer equipment scripts.

Troubleshooting modem connections

The following procedures are solutions to the most common troubles.

Modem does not dial

Procedure 30

Verifying that the modem is properly configured

Step	Action
1	From the Start menu, select Settings > Control Panel .
2	Open the Modems file and click Properties .
—End—	

Procedure 31

Testing the COM port

Step	Action
<i>Test the COM port to which the modem is connected by launching HyperTerminal:</i>	
1	From the Start menu, select Programs > Accessories > HyperTerminal .

This action tests the COM port to which the modem is connected by launching the HyperTerminal.

HyperTerminal prompts for a connection name and presents the telephone number dialog box.

- 2 In the **Connect Using** drop-down list box, select **Direct to COM X**, where X is the COM port to which the modem is connected.
- 3 When in the terminal, type the command **AT <Enter>**.
The modem responds with OK.
If the modem does not respond, the wrong COM port may be being used.

—End—

To verify that the correct COM port is being used:

Procedure 32
Verifying the COM port

Step	Action
------	--------

- | | |
|---|---|
| 1 | In the File/Properties menu, select Direct to COM Y , where Y is a different COM port. |
| 2 | When the correct COM port has been located, go back to Telephony Manager 3.1 Navigator and bring up the properties for the system to which you are trying to connect. |
| 3 | Click Communication tab, and then choose PPP or Serial from the communication profile list. |
| 4 | Verify that the COM port selected for this profile is the COM port on which the modem was located using HyperTerminal. |
| 5 | Verify that the baud rate matches the settings for the system port that is dialed. |
-

—End—

Step	Action
------	--------

If the modem still does not dial:

- | | |
|---|---|
| 1 | Follow the steps in the procedure Procedure 31 "Testing the COM port" (page 151) to establish a HyperTerminal connection. |
|---|---|
-

- 2 After issuing the **AT** command and receiving the OK prompt, issue the command **ATDT 1234567**, where **1234567** is the telephone number for the modem connected to the system.
- 3 Listen to determine whether the modem dials and connects:
 - a. If unable to hear the modem dialing and connecting at this point, verify that the telephone line and modem cables are connected correctly.
 - b. If the modem dials and connects, verify that dial-up networking is installed along with a dial-up-adaptor.

—End—

Scripting fails

In this scenario, the modem dials and connects but the Connection Details button reveals that scripting failed while waiting for a prompt.

In the Communications profile, verify that the baud rate configured for the TTY on the switch matches the baud rate configured for the modem in the PPP or Serial Communications profiles for the system to which you wish to connect. Make sure that the data bits, stop bits, and parity match as well.

Procedure 33

Viewing the Communications profiles

Step	Action
------	--------

To view the Communications profiles for a system:

- 1 Right-click on the desired system in the **Navigator** window.
- 2 Select **Properties**, and then click **Communications** tab in the Properties dialog box.

—End—

Modem dials but does not connect

Procedure 34

Verifying the modem connection

Step	Action
------	--------

- 1 Verify that the dialed telephone number is not busy.

- 2 Verify that all necessary digits in the telephone number have been included.
- 3 Check the **PPP** or **Serial Communications** profiles for the system to which you wish to connect.

To view the Communications profiles for a system:

- a. Right-click on the desired system in the **Navigator** window.
- b. Select **Properties**, and then click **Communications** tab in the Properties dialog box.

—End—

Session fails

In this scenario, the modem dials and connects and the scripting is completed successfully, but the Connection Details button reveals that the session failed.



WARNING

Disabling the shells in LD 117 will cause telephony applications on external devices to stop communicating with the PBX.

Procedure 35

Resolving a failed session

Step	Action
1	Verify that the IP address that you assigned to the local PPP interface on the system is the same as the IP address you entered in the address field in the PPP Communications profile for the system to which you wish to connect. To view the Communications profiles for a system: a. Right-click on the desired system in the Navigator window. b. Select Properties, and then click Communications tab in the Properties dialog box.
2	If possible, verify that an Ethernet connection can be made to the same system: a. After establishing a PPP connection, but before canceling the connection dialog, open a DOS command prompt: From the Start menu select Programs > MS-DOS Prompt.

- b. Run the ping command by typing **ping 47.1.1.10** where **47.1.1.10** is the system's local IP address. See "Adding a system" in *Telephony Manager 3.1 System Administration (NN43050-601)* for information about configuring Ethernet and PPP on the system.
- c. Verify that the data lights on the modem flash as the ping data is sent to the system.

If a response is not received from the system, verify that the IP address is the same as the one assigned to the local PPP interface on the system. To verify the IP address, go to the System Properties—Communication, PPP Connection Type dialog box, and confirm that the IP address that appears in the address field is correct.

—End—

COM port error

In this scenario, the modem dials and connects but the error message "Error writing to COM port" or "Error reading from COM port" is received.

Procedure 36

Resolving COM port error

Step	Action
1	Verify that the modem installed in Control Panel matches your modem type.
2	Remove the installed modem driver and install a generic modem driver in its place: a. From the Start menu, select Settings > Control Panel. b. Double-click Modems. c. Click Remove to remove the modem from the installed list. d. Click Add to add a new modem driver. e. Select the check box Don't detect my modem; I will select it from a list, and then click Next. f. Select the standard modem driver matching your modem's baud rate (for example, Standard 28 800 bps Modem), and then click Next. g. Select the COM port to which your modem is connected, and then click Next. h. Click Finish to complete the modem installation.

- i. Restart the system, and try to establish a PPP or serial connection.

—End—

Security Management

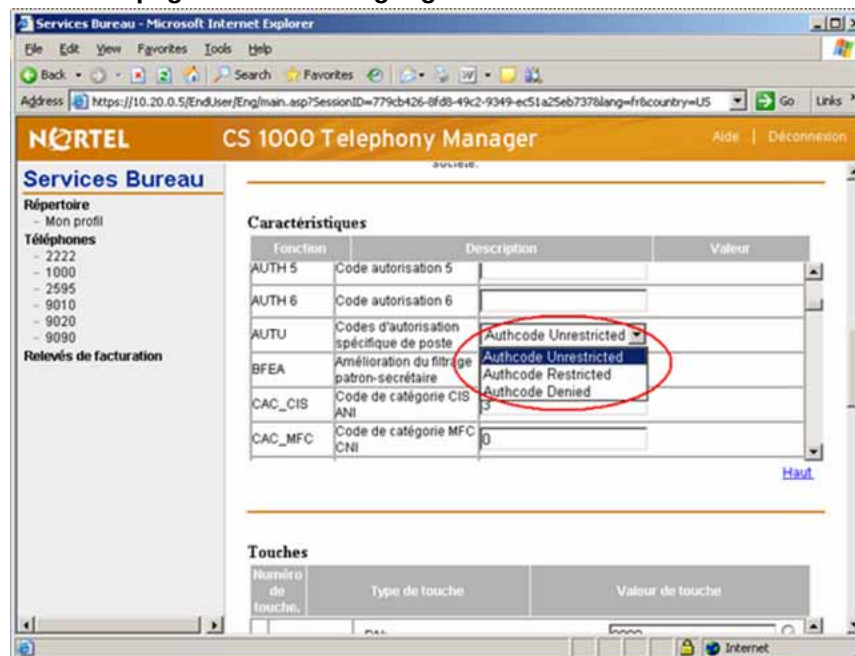
When Telephony Manager 3.1 starts for the first time, the Administrator, HelpDesk, EndUser, and Default user groups are the only active user groups. You must assign access properties for any other groups that you have set up on the Telephony Manager 3.1 server.

Localization

Important advice for regionalized operating systems — The name of the administrators user group in the French and German OS is not Administrators. These names are localized by Microsoft in the regional OS software. In a default French Windows installation, the local administrators user group is Administrateurs. In the German version, this user group is Administratoren. When installed on a French or German OS, the Telephony Manager 3.1 predefined administrators user group is named Administrateurs or Administratoren to match the OS.

When an End User logs into the German or French version of the Telephone Details page of an IP phone set, the list of feature values is displayed only in English. The values are not translated into German or French. See [Figure 94 "End User page in French language" \(page 158\)](#)

Figure 94
End User page in French language



Assigning access properties

Telephony Manager 3.1 provides easy access to users for personal, system, site, or network-wide management of systems. The administrator determines the level of access for the users in a particular user group. The administrator also determines which sites and systems the members of the user group can manage. It is the responsibility of the network administrator to ensure that only authorized users can access the Telephony Manager 3.1 server and its associated system.

The administrator configures Windows user groups and individual users using the Windows user interface. The administrator then determines the access permissions for each user group by using the Telephony Manager 3.1 Web Navigator page. For more information about setting user access, refer to "User groups" (page 164).

Security for upgrades and re-installations

As a security precaution, with any upgrade or reinstallation of Telephony Manager 3.1 software, access properties for all user groups are reset to the default values.

Administrators

Users of the Telephony Manager 3.1 Administration Site belong to a distinct user group and are assigned the security profile for that user group. Users are not able to alter access permissions for the Administrators user group.

Members of the Administrators user group can:

- log on to the Telephony Manager 3.1 Administration Web site
- Access all Telephony Manager 3.1 Web applications.
- Assign access rights to the other user groups.
- Assign access rights to applications. HelpDesk users have access to all applications except those listed under Web Administration. No other user groups have any access to Telephony Manager 3.1 Web applications unless that group has been specifically granted appropriate permissions.
- Assign access rights for Web applications before any users from that group can log on.

While assigning access permissions, be certain to select the top level application for every sub-application assigned. For example, if **System Alarms** is selected, **Equipment** must also be selected. Failure to do so can result in members of the user group denied access to the Web site.

Telephony Manager 3.1 Web application access permissions are controlled by the Administrator on a per-user group basis. For example, the administrator may limit the Telephony Manager 3.1 users access to only some of the Telephony Manager 3.1 Web-based functionality. The Telephony Manager 3.1 Web Navigator controls access to applications by shielding Web links that the user does not have access to. The directories and files comprising those applications are similarly protected.

Users

Users log on to the Telephony Manager 3.1 Web Navigator using their Microsoft Windows userID and password. logon security for Telephony Manager 3.1 Web services ensures protection against unauthorized entry and enforces access permissions for logged-on users.

Access to Web applications applies to a group, not to individual users. To change the security access for individual users, their group membership should be changed. For information about setting user access, refer to ["User groups" \(page 164\)](#).

With the exception of Administrators, do not place a person in multiple groups. The first group detected by Telephony Manager 3.1 is used to determine access permissions. There is no restriction on the Administrators group. Users may belong to other groups, but if they belong to the Administrators group, the Administrators profile overrides all other profiles.

There is a Default user category. Default users can successfully log on to the Web Navigator, but they do not have a user group defined in their Directory record.

Telephony Manager 3.1 administrators and Help desk users have user accounts in a Windows domain. End users may have accounts either in a Windows domain or through a CND server.

Telephony Manager 3.1 administrators and Help desk users can access and change their own telephones through either the Web Navigator or the Desktop Services end user pages. Access to the end-user pages requires the appropriate CND Directory setup (user logon and user group) for these administrators and Help desk users.

Authentication

Authentication requests are passed to Telephony Manager 3.1 Watchdog, which applies the configured authentication method and creates a session for the user. For authentication on Local Server account or Windows Domain account, the standard Windows Security Provider is used. For authentication using CND Authentication for end users, the logon name and the password are passed to the CND server.

In Telephony Manager 3.1, Windows and Web users are authenticated using the settings configured either on the User Authentication Web page or in the User Authentication dialog box. The information that appears on the Web page and in the dialog box is identical. The Web link to the User Authentication page is found under Web administration in the Telephony Manager 3.1 Web Navigator tree. The User Authentication dialog box is accessed from the Security menu in the Telephony Manager 3.1 Windows Navigator.

Authentication methods

The following user authentication methods are available:

- Local Telephony Manager 3.1 server account
- Windows Domain account
- CND authentication

Any one of the three methods or a combination of these methods can be selected to authenticate users on all Telephony Manager 3.1 platforms: Telephony Manager 3.1 server, Telephony Manager 3.1 Windows client, and Telephony Manager 3.1 Web client.

The Administrator account is always authenticated as a Windows local account. This is due to the fact that the Administrator account is the default account on these Windows platforms.

The default authentication method is Local Telephony Manager 3.1 server account. Because this method does not require a search of the CND Directory to find the user's assigned user group, the Local Telephony Manager 3.1 server account method provides the best logon performance.

If multiple authentication methods is chosen, Telephony Manager 3.1 respects the order configured; however, it should be noted that the best performance is achieved by using the Local Telephony Manager 3.1 server account method.

For information about configuring authentication methods using the User Authentication Web page, see "User authentication" in *Telephony Manager 3.1 System Administration (NN43050-601)*.

For information about configuring authentication methods using the User Authentication Windows dialog box, see "User authentication" in *Telephony Manager 3.1 System Administration (NN43050-601)*.

Password policy

Password security during transport across the network is accomplished in the following manner:

Default passwords on the Call Server, Signalling Server and the Voice Gateway Media Card are forced changed by the software.

Telephony Manager 3.1 uses the PWD1, PWD2 and PDT passwords for certain functions that interact with the Call Server, Signalling Server and Voice Gateway Media Card.

If any of the passwords expire due to the force change feature, Telephony Manager 3.1 functionality fails similar to having incorrect passwords.

The passwords must be updated manually on the Call Server, Signalling Server and Voice Gateway Media Card through CLI commands. Telephony Manager 3.1 system properties must also be updated with the new passwords before proceeding with any Telephony Manager 3.1 functionality.

- Telephony Manager 3.1 Windows client passwords are encrypted using Crypto APIs prior to transmission. The same private key is used by both the client and the server.

- For Telephony Manager 3.1 Web clients, by default, clear text passwords are used; however, if the Telephony Manager 3.1 server has the proper certificate installed, the use of SSL encrypted transport during authentication can be forced. To use the SSL during the authentication process, the Telephony Manager 3.1 server must have the required certificate installed as described in "[Configuring Secure Sockets Layer \(SSL\)](#)" (page 85). Click the **Use SSL for Web logon authentication** check box after installing the certificate.

Before using SSL on the Telephony Manager 3.1 server, the Telephony Manager 3.1 server must have the required certificate installed as described in "[Configuring Secure Sockets Layer \(SSL\)](#)" (page 85). If **Use SSL for Web logon authentication** is selected, Web logon is performed using https://... instead of http://... and traffic is encrypted. The Telephony Manager 3.1 server automatically switches to non-SSL transport when the user is successfully authenticated.

- If CND authentication is used, the following sequence is used:
 - The Telephony Manager 3.1 server tests to determine whether the Directory server offers SSL-based authentication.
 - If SSL is supported by the Directory server, passwords are encrypted before transmission using a Public-Private key pair negotiated through the CND mechanism.
 - If SSL is not supported, passwords are transmitted as clear text.
- All passwords, including passwords to access the system, are stored in the Telephony Manager 3.1 database in an encrypted format. Crypto API, the standard Windows Security Provider encryption service, is used for this purpose.

Blank passwords

Telephony Manager 3.1 does not support blank passwords.

User management

There are two major categories of users within Telephony Manager 3.1 — Navigator users and end users. Access for these users is controlled by configuring Navigator users in the Telephony Manager 3.1 Users window, and end users in the Employee Editor.

Navigator users

Telephony Manager 3.1 Windows Navigator and Web Navigator users are managed through Telephony Manager 3.1 User administration. Users are created and assigned to a particular user group. This user group assignment controls access to Telephony Manager 3.1 Windows and Web applications.

There are two different types of Navigator users:

- Local — Local Navigator users have accounts that exist on the Telephony Manager 3.1 server. When a user is added, an Telephony Manager 3.1 user account and a corresponding local Windows user account are created on the Telephony Manager 3.1 server. The new user is assigned to the selected Windows user group.

Delete an Telephony Manager 3.1 user account to remove the user account from the account list, as well as from all relevant database tables.

- Remote — Remote Navigator users have accounts that reside on a domain controller or in a CND Directory. Telephony Manager 3.1 User administration is used to assign the Remote Navigator user's logon name to an Telephony Manager 3.1 user group.

For information about configuring Navigator users, see "[Configuring Telephony Manager 3.1 Navigator users](#)" (page 167).

End users

End users access the Telephony Manager 3.1 Desktop Services Web site to view information about, and make changes to, their telephones.

Although end users can be given a Telephony Manager 3.1 user account similar to Navigator users, the only supported authentication method for end users is CND authentication.

For end users, the following attributes are entered into the users record in the CND Directory:

- logon name. When configuring CND authentication, the logon name may be one of the following:
 - commonName
 - e-mail
 - employee number
- User group
- Web Reporting Access Rights

For information about using the CND Directory to configure end users for access to Telephony Manager 3.1, see the *Common Network Directory 2.1 Administration Guide (NN43050-101)*.

Logon process

This chapter describes the activities performed by Telephony Manager 3.1 to authenticate and log on Telephony Manager 3.1 users.

Procedure 37
logon process

Step Action

- 1** The user accesses the Windows logon dialog box or the Web logon page.
- 2** User enter their logon name and password.
- 3** Telephony Manager 3.1 performs authentication respecting the configured order.
- 4** If authentication is successful, user group resolution is performed as follows:
Navigator logon — Windows or Web
 - If the user is authenticated using a local Telephony Manager 3.1 server account, user group resolution is performed using the local account database.
 - If the user is authenticated using a Windows domain account, user group resolution is performed using the Telephony Manager 3.1 user database. If the user group mapping is not found in the Telephony Manager 3.1 user database, the CND Directory is used.
 - If the user is authenticated using a CND Directory, user group resolution is performed using the Telephony Manager 3.1 user database. If the user group mapping is not found in the Telephony Manager 3.1 user database, the CND Directory is used.
If the user cannot be mapped to a user group, Telephony Manager 3.1 appears the following message: "You have not been assigned to an Telephony Manager 3.1 user group. Please contact the Telephony Manager 3.1 Administrator."
 - End users — Web only: User group resolution is performed using the CND Directory. If users are not found, they are assigned to the default user group.

—End—

User groups

Telephony Manager 3.1 user groups provide the mechanism to control access to the following Telephony Manager 3.1 resources:

- Telephony Manager 3.1 Windows Navigator — Navigator and site/system level applications

- Telephony Manager 3.1 Web Navigator — Navigator and site/system level applications
- Access to telephone manager Administration — Web Desktop Services for end users

In addition, Telephony Manager 3.1 provides the following user management functions:

- The ability to create/delete users and user groups (Windows user interface only)
- The ability to configure Web Desktop Services for end users (Web user interface only)

Creating a user group

The Windows user group application was known as User Templates in early versions of Telephony Manager 3.1. New user groups are created using an existing user group as the base.

User groups provided with Telephony Manager 3.1

The following user groups and access definitions are shipped with Telephony Manager 3.1:

- Administrators — This user group has read/write access to all sites, systems, and applications. The Administrators user group cannot be changed, renamed, or deleted.

The other user groups provided with Telephony Manager 3.1 can be changed, but they cannot be renamed or deleted.

- HelpDesk — This user group has the following access privileges:
 - Access to all Web Navigator tree items except those located under the Web Administration branch
 - Full access to Web Desktop Services, including read/write and synchronization capabilities
 - Full access to the Windows Navigator applications with the exception of IP line/IP Trunk Services
- EndUser — This user group has the following access privileges:
 - No access to the Telephony Manager 3.1 Windows or Web applications
 - Web Desktop Services is read-only; however, all except 21 of the most commonly used features are set to **Hidden**
- Default — This user group has no access to any Telephony Manager 3.1 features or applications.

User management recommendations

The Administrator user account for the Windows OS does not appear in the Telephony Manager 3.1 Users window. This is to prevent users from changing the Administrator account password from within Telephony Manager 3.1.

Even though it is not listed in the Users window, the OS Administrator account can always be used to log on to Telephony Manager 3.1.

Nortel strongly recommends that a new user group be created in Telephony Manager 3.1 based on the Administrators user group. Telephony Manager 3.1 users should be assigned to this new user group instead of adding them to the Administrators user group. This is a security measure to ensure that a user with administrative access to Telephony Manager 3.1 does not also have access to the OS on the Telephony Manager 3.1 server as a member of the Administrators group.

Installation

Fresh installation

In a fresh installation, three new user groups are created in Windows. Telephony Manager 3.1 utilizes HelpDesk, EndUser, and Default user groups along with the existing Administrators group.

For Telephony Manager 3.1 Windows clients, the Telephony Manager 3.1 server's host name must be provided during installation. The host name is saved in the registry.

Upgrade

In an upgrade, existing Telephony Manager 3.1 Windows Templates are created as user groups. By default, these groups do not have access to Telephony Manager 3.1 Web Navigator applications.

A local server account is created for each existing Telephony Manager 3.1 Windows user. The new account is assigned to the appropriate user group.

Existing Telephony Manager 3.1 Telephone Access Profiles, which were based on user groups, are migrated from the Web Navigator database to the new user group database. This assumes that the corresponding groups related to them already exist.

These user groups are also migrated to the telephone manager database; however, new user groups do not have access to telephone manager administration. Access to telephone manager Administration must be configured by using the User Groups Web page. "[User groups](#)" (page 140).

Configuring Telephony Manager 3.1 Navigator users

Telephony Manager 3.1 permits the creation of user groups to speed the process of adding users accessing the Telephony Manager 3.1 Windows Navigator and certain Telephony Manager 3.1 Web-based applications. In the User Group Properties dialog box, most aspects of a certain kind of user are defined by the administrator, such as level of access to sites and systems, and automatic connection to particular systems. As many user groups as required can be created. Individual users are assigned to a user group when users are added to the Telephony Manager 3.1 database.

There are two types of users — local users and remote users. Local users have accounts on the Telephony Manager 3.1 server. When adding a new local user, an Telephony Manager 3.1 user account and a local Windows user account are created and the account is assigned to the specified user group. Deletion of a user removes the user account from the account list in Windows, as well as from all relevant database tables. Remote users have accounts that exist on a domain controller or in the CND. For these users, Telephony Manager 3.1 is used to assign the logon name for the account to a Telephony Manager 3.1 user group. The logon names defined in Telephony Manager 3.1 must be unique for all users.

Access to Telephony Manager 3.1 Windows and Web applications is provided through the Windows server. A Windows domain account or the CND can also be used to authenticate Telephony Manager 3.1 users for Web Services. See "Web Navigator" in *Telephony Manager 3.1 System Administration (NN43050-601)*.

Deleting a user group

A user group can be deleted only after all associated members of that group are either deleted or reassigned to another user group.

The account used when logging in to your current session cannot be deleted.

Restricting user access permission levels

A user can be restricted from having access to sites, systems, and applications. However, when a user is defined as restricted from any access to all sites, systems, and applications in the Navigator, the user can, in fact, see all the sites and systems in the Navigator tree and has read-only access to their properties. If restricted users try to open a system, they see a System Window with no applications visible.

Sites and systems displayed in user groups

When adding or modifying a user group, only systems that have applications enabled are presented. If no applications are enabled for the systems within a given site, the site and system(s) do not appear in the User Group Properties dialog box.

For information about configuring end users for access to the Telephony Manager 3.1 Web site, see ["User groups" \(page 140\)](#).

User authentication

Any of the following three methods or combination of these methods can be used to authenticate Telephony Manager 3.1 users:

- Local Server account
- Windows NT Domain account
- CND authentication

The Administrator account is always authenticated through the local server account because it is a default account on all supported Windows platforms.

The default authentication method is the Local Telephony Manager 3.1 server account. This method provides the best logon performance because there is no requirement to search the CND Directory for the user's assigned user group.

User authentication can also be configured using the Telephony Manager 3.1 Web Services. For information, see ["User authentication" \(page 138\)](#).

Procedure 38**Configure authentication**

Step Action

- 1 From the Telephony Manager 3.1 Windows Navigator, select **Security > User Authentication**.

The User Authentication dialog box appears [Figure 95 "User Authentication dialog box" \(page 169\)](#).

Figure 95
User Authentication dialog box

The dialog box is titled "User Authentication". It contains the following text and controls:

- Text: "Users are authenticated upon login to Windows and Web application."
- Text: "Once logged in, the user's assigned User Group controls access to specific applications."
- Text: "Select the order of authentication methods to be performed at login:"
- A table with two columns: "Order" and "Authentication Method".

Order	Authentication Method
1	Local Server account
2	Windows Domain account
3	Common Network Directory (CND)
- Under "Windows Domain account", there is a "Domain:" text box.
- Under "Common Network Directory (CND)", there is an "Identifier:" dropdown menu with "Common Name" selected.
- Text: "Web Endusers are always authenticated using CND authentication method only."
- Check box: "Use SSL for Web login authentication" (unchecked).
- Buttons: "OK" and "Cancel".

- 2 Use the check boxes to select one or more of the available authentication methods.
 - a. If selecting Windows NT Domain account, enter one or more domains in the Domain text box. Separate the domain names with a comma.

ATTENTION

The domain names must be separated by a comma. Do not use any spaces.

- b. If you select CND authentication, use the drop-down list to choose **Common Name**, **EmployeeID**, or **E-mail**.
- 3 Use the drop-down lists to assign the order in which the authentication methods are performed.

If choosing multiple authentication methods, Telephony Manager 3.1 respects the order configured; however, it should be noted that the best performance is achieved by using the Local Telephony Manager 3.1 server account method.
- 4 To use the SSL during the authentication process, the Telephony Manager 3.1 server must have the required certificate installed as described in "[Configuring Secure Sockets Layer \(SSL\)](#)" (page 85).

Select the **Use SSL for Web logon authentication** check box after installing the certificate.

If the Telephony Manager 3.1 server has the required certificate installed, selecting the check box causes Telephony Manager 3.1 to use SSL-encrypted transport during authentication. In this case, Web logon is performed using https:// rather than http://, and the traffic is encrypted. The Telephony Manager 3.1 server automatically switches to non-SSL transport when the user is successfully authenticated.

The selected method(s) are used to authenticate users on all Telephony Manager 3.1 platforms: Telephony Manager 3.1 server, Telephony Manager 3.1 client, and Telephony Manager 3.1 Web client.

—End—

Creating a user group

Telephony Manager 3.1 allows the creation of User Groups to speed the process of adding users by accessing the Telephony Manager 3.1 Windows Navigator and certain Telephony Manager 3.1 Web-based applications. In the User Group Properties dialog box, define most aspects of certain kinds of users, such as their level of access to sites and systems and automatic connection to particular systems. As many User Groups as required can be created. Individual users are assigned to a User Group when adding users to the Telephony Manager 3.1 database.

There are two types of users: local users and remote users. Local users have accounts on the Telephony Manager 3.1 server. When adding a new local user, a Telephony Manager 3.1 user account and a local user account are created, and the account is assigned to the specified User Group. Deletion of a user removes the user account from the account list as well as from all relevant database tables. Remote users have accounts that exist on a domain controller or in the CND. For these users, Telephony Manager 3.1 is used to assign the user ID for the account to a Telephony Manager 3.1 user group. The logon names defined in Telephony Manager 3.1 must be unique for all users.

Access to Telephony Manager 3.1 Web Services is provided through the server. Refer to "[User authentication](#)" (page 138).

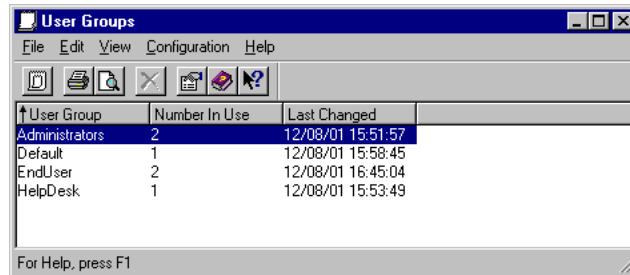
Procedure 39

Creating a user group

Step	Action
------	--------

- | | |
|---|---|
| 1 | In the Navigator window, choose Security > User Groups to display the User Groups window Figure 96 "User Groups window" (page 171). |
|---|---|

Figure 96
User Groups window

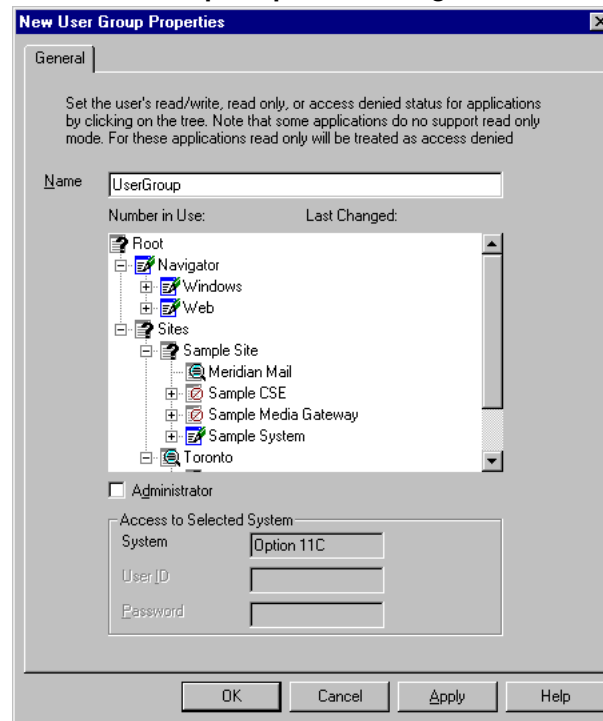


User Group	Number In Use	Last Changed
Administrators	2	12/08/01 15:51:57
Default	1	12/08/01 15:58:45
EndUser	2	12/08/01 16:45:04
HelpDesk	1	12/08/01 15:53:49

- | | |
|---|--|
| 2 | Choose Configuration > Add User Group . The new user group is created with the same access privileges as the highlighted user group. The New User Group Properties dialog box appears Figure 97 "New User Group Properties dialog box" (page 172). |
|---|--|

The Administrators, Default, EndUser, and HelpDesk User Groups are always available and cannot be deleted. All groups except for Administrators can be modified. The Administrators User Group has access to all Windows-based and Web-based Telephony Manager 3.1 applications.

Figure 97
New User Group Properties dialog box



3 Enter a name for this User Group.

For each site, system, and application in the tree, use the right mouse button to assign user privileges (**Read-write**, **Read-only**, or **No Access**). Each click of the right mouse button causes the access privileges and corresponding icon to change. Select the Administrator box, if appropriate. The site and system icons change to reflect the access level.

Access privileges defined for sites or systems at higher levels in the tree structure are applied to all subordinate items. [Table 11 "Access privilege icons" \(page 173\)](#).

The question mark icon indicates that the sub-items belonging to the item displaying the question mark icon have mixed access settings.

Table 11
Access privilege icons

Icon	Explanation
	Read and write access
	Read only access
	No access
	Indicates that the access privileges in the branch are mixed between one or more of the above levels

- 4 Enter values in the User ID and Password text boxes to allow this class of user to connect to this system without having to enter a User ID and Password each time for connection.

If the Administrator wants to use the Web Maintenance Pages, these fields must be completed in the Administrators User Group properties.

- 5 Click **OK** to save changes and close the User Group Properties dialog box.

—End—

Adding a user

The Administrator user account for the Windows 2000 OS does not appear in the Telephony Manager 3.1 Users window. This is to prevent users from changing the Administrator account password from within Telephony Manager 3.1.

Even though it is not listed in the Users window, the OS Administrator account can always be used to log on to Telephony Manager 3.1.

Procedure 40

Adding a user

Step	Action
------	--------

- 1 In the Telephony Manager 3.1 Users window, choose **Configuration > Add User**.

The New User Properties dialog box appears. See [Figure 98 "New User Properties dialog box"](#) (page 174).

Figure 98
New User Properties dialog box

- 2 Select a User Type from the drop-down list:
 - Local - Users who are authenticated using an account on the Telephony Manager 3.1 server.
 - Remote - Users who are authenticated using CND or domain.

When Remote is selected, the Change Password button, as well as the Status and Current Status controls, are disabled.

- 3 Enter a User ID.

ATTENTION

The user name cannot contain spaces, including between the first and last name, or special characters, such as forward slash (/), backward slash (\), brackets ([]), plus sign (+), equals sign (=), semi-colon (;), comma (,), asterisk (*), single quote (') or double quote (").

- 4 From the User Group drop-down list, select the group to use as the basis for this user definition.
- 5 Enter other data as required.
- 6 Click **Apply**. Telephony Manager 3.1 prompts the entry of a password.
- 7 Enter the password and click **OK** to change the Telephony Manager 3.1 logon password for this user only.
- 8 Click **OK**. The new user appears in the Telephony Manager 3.1 User window. Close the Telephony Manager 3.1 User window.

—End—

Authenticating users

One of the following methods can be selected to authenticate Telephony Manager 3.1 users:

- Local Server account
- Window Domain account
- CND authentication

The Administrator account is always authenticated through the local server account because it is a default account on all supported Windows platforms.

The default authentication method is the Local Telephony Manager 3.1 server account. This method provides the best logon performance because there is no requirement to search the CND Directory for the user's assigned User Group.

To configure authentication, complete [Procedure 38 "Configure authentication" \(page 168\)](#).

Initial logon

Windows users are authenticated using either a local account on the Telephony Manager 3.1 server, a Windows domain account, or CND. There is no default logon name and password for these systems.

Any user account (for example, Administrator) that is a member of the local Administrators group is always able to log on to Telephony Manager 3.1. In a new Telephony Manager 3.1 installation, use any local Administrators group account for the initial log on.

After logging in to Telephony Manager 3.1 for the first time, you can set up additional users and user groups by selecting the following paths:

- To add user groups, select **Security > User Groups** from the Telephony Manager 3.1 Navigator window, and then select **Configuration > Add User Group...** from the User Groups window. See "Creating User Groups" in *Telephony Manager 3.1 System Administration (NN43050-601)* for detailed instructions on adding Telephony Manager 3.1 user groups.
- To add users, select **Security > Users** from the Telephony Manager 3.1 Navigator window, and then select **Configuration > Add User...** from the Telephony Manager 3.1 Users window. See "Adding Users" in *Telephony Manager 3.1 System Administration (NN43050-601)* for detailed instructions on adding Telephony Manager 3.1 users.

Users that are not created from within Telephony Manager 3.1 do not appear in the Telephony Manager 3.1 Users window.

Setting up the CND server and Terminal server

CND server

The CND allows you to link and synchronize data in the Telephony Manager 3.1, CND, and supported Corporate LDAP directories. Telephony Manager 3.1 acts as a client to the CND.

- If CND is installed on the same server as Telephony Manager 3.1, then all properties were preconfigured and no changes are required.
- If CND is installed on a different PC from the Telephony Manager 3.1 server, the IP address of the CND server must be entered in the CND server setup dialog box.
- If the default Telephony Manager 3.1 account password is changed from CND Manager, the password value must be updated in the CND server setup dialog box.
- If Telephony Manager clients need to access CND data, CND setup on their Telephony Manager server must be configured with the Computer name (host name) or IP address of the CND server (not localhost), even though the CND server is installed on the same server as Telephony Manager 3.1 server. This is configured manually after installing the Telephony Manager 3.1 server.

For detailed instructions on setting up the CND server, as well as an example of importing attributes to the CND Directory, see *Common Network Directory 2.1 Administration Guide (NN43050-101)*.

Terminal server

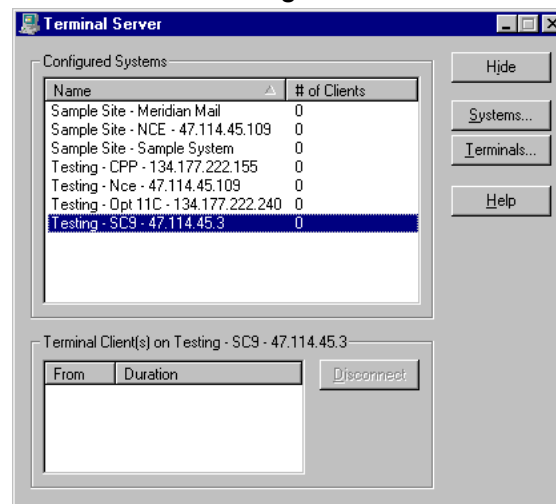
The Terminal server application is a Windows application that uses the Telephony Manager 3.1 database to obtain site, system, and IP address information. The Terminal server supports direct serial connections and system overlay connection over an IP network. If connecting over an IP network to a system, the port user types (SCH, MTC, BUG, TRF) can be configured.

Telephony Manager 3.1 does not support Remote Desktop with Terminal Server.

Terminal server setup

To launch the Terminal server application, from the Start menu, select **Programs > Nortel CS 1000 Telephony Manager > Terminal server**. The Terminal server dialog box appears. See [Figure 99 "Terminal server dialog box"](#) (page 180).

Figure 99
Terminal server dialog box



ATTENTION

Click **Hide** on **Terminal server** dialog box (see [Figure 99 "Terminal server dialog box"](#) (page 180)), **do not** close from the window **close** button (X) as this loses all configuration.

The Terminal server window appears two lists:

- configured systems
- configured ports

The configured systems list appears information about the virtual port that is configured:

- Name:
As defined in the Telephony Manager 3.1 Windows Navigator
- Number of clients:
The number of terminal clients using the port

When selecting an entry in the Configured Ports list, the clients on Port list appears the following information for each terminal client using the port:

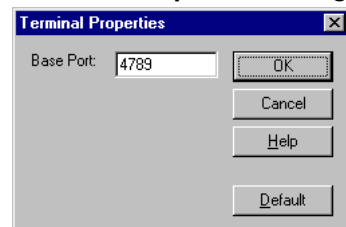
- **From:**
IP address of the terminal client
- **Duration:**
How long the connection is in use

The Disconnect button next to the clients on Port list allows termination of the connection to one or more terminal clients.

The Terminal server application also has the following buttons:

- **Hide** Hides the application window. During normal operation, the Terminal server application runs without user input, so hiding its window frees up some desktop space. The window can be viewed at any time by double-clicking the Terminal Service icon in the Task Bar tray.
- **Systems...** Configures the virtual ports. "[Virtual ports](#)" (page 181).
- **Terminals...** Configures the starting network socket port number for communications between the Telephony Manager 3.1 server and the Telephony Manager 3.1 Web System Terminal see [Figure 100 "Terminal Properties dialog box"](#) (page 181). The default is 4789. Typically, this does not need to be changed.
- **Help** Get context-sensitive Help on the application.

Figure 100
Terminal Properties dialog box



Virtual ports

In the Terminal server application, the Virtual Ports Properties window allows the user to enable or disable connection to a particular device. It displays the virtual port number for each configured device, and the corresponding serial or network settings.

In the Virtual Port Properties window, a tree appears the devices that can be connected through a virtual port. For serial ports, the window retrieves the available serial ports from the Registry. For network connections, the window retrieves the site and system information from the Telephony Manager 3.1 database. The virtual port for a system uses the same IP

address assigned to System Terminal. The tree mirrors the tree in the Telephony Manager 3.1 Navigator. It uses the communication profile in System Properties, determined as follows:

- For a Generic system, it uses the profile (serial or network) selected in the Application page in System Properties.
- For a non-Generic system, it uses the communication settings from the profile (serial or network) assigned to Virtual System Terminal in the Applications page in System Properties.
- For any system, if a network (Ethernet) profile is selected, Terminal server uses a Telnet connection.

To configure virtual port connection for a device, click Systems in the Terminal server window, or double-click a Configured System in the list (this selects the corresponding device in the Virtual Port Properties window allowing you to quickly change the settings for a particular device).

To enable virtual port connection for a device, do one of the following:

- Double-click the disabled port in the tree.
- Select the item and select the Enabled check box.
- Click **Enable All**. This enables all the items listed in the tree with the default configuration. The item becomes bold to show that it is enabled.

The field to the right of the Enabled check box automatically fills in the Site - System name for the selected device. This is the name displayed in the Terminal server's main window.

To disable a virtual port, do one of the following:

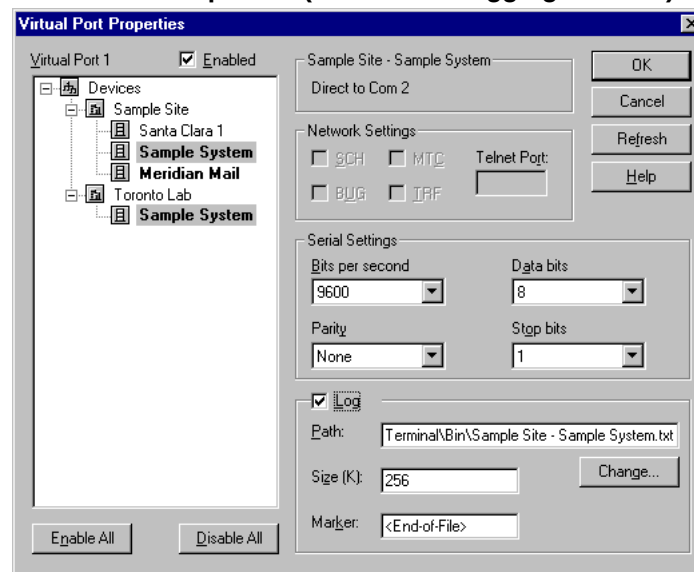
- Double-click an enabled item in the tree.
- Select the item and clear the Enabled check box.
- Click **Disable All**. This disables all the devices listed in the tree. The item is no longer bold, and does not appear from the Terminal server main window when you click **OK**.

Serial connections

The Terminal server application supports all the serial ports on the Telephony Manager 3.1 server PC plus the systems configured in the Telephony Manager 3.1 Navigator. Telephony Manager can support 10 COM ports, assuming that the user already has 2 ports configured on his PC and another 8 ports are added.

For a serial connection, Direct to Com x appears, where x is the com port number. The fields for serial settings are enabled. The default is the serial settings from the Telephony Manager 3.1 database. The settings in the dialog box can be changed, as shown [Figure 101 "Virtual Port Properties \(Serial with Logging enabled\)"](#) (page 183).

Figure 101
Virtual Port Properties (Serial with Logging enabled)



Network connections

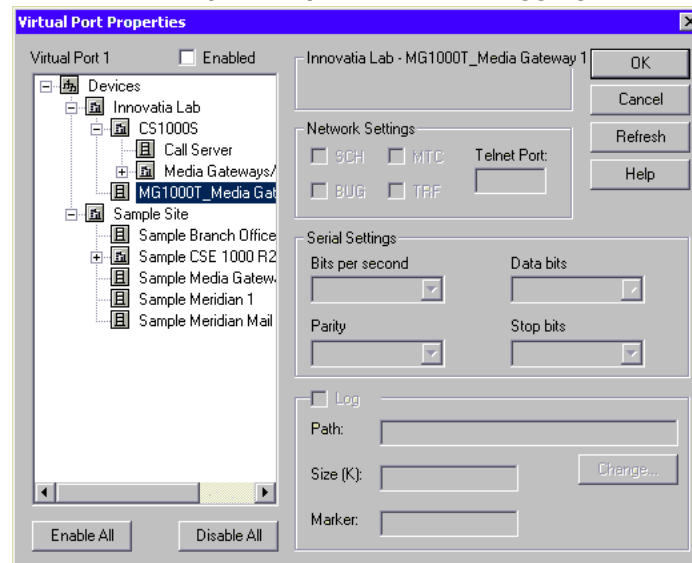
For a network connection, the IP address appears. It also indicates whether the system is a Meridian 1, CS 1000, or Generic.

- Make sure the IP address is correct. If the IP address is different from the Telephony Manager 3.1 database's setting, click Refresh to update all of the network ports with the latest settings from the Telephony Manager 3.1 database.
- If selecting an M1 or CS 1000 System, the fields for M1 port settings are enabled (default = SCH). The Telnet port field is disabled.
- If selecting a Generic System, the fields for both serial and M1 port settings are disabled. The Telnet port field is enabled.
- Select the Log check box to turn on data capture. The log file name defaults to the Site - System name plus a .txt extension. The path and the file name can be changed by typing in the edit box or clicking Change.
- The maximum size of the log file is customized (in the Size field) on a per-system basis, and defaults to 256 K. When the file size reaches the

limit, the Terminal server starts from the beginning of the file, overwriting the oldest logs.

- Due to the circular nature of the log, the Terminal server writes an end-of-file marker (customizes in the Marker field) at the end of the log entries.
- The log records the time and date of when a client connects and disconnects to the virtual port, and writes all text received from and sent to the host. This allows a network administrator to keep an activity log of the virtual port connection.
- If this ASCII log is to be viewed from a Web browser, the file is stored in a Web-accessible path. For more information on Virtual Port Properties (Network with Logging disabled), see [Figure 102 "Virtual Port Properties \(Network with Logging disabled\)"](#) (page 184).

Figure 102
Virtual Port Properties (Network with Logging disabled)



Configuring the Web browser client

This chapter contains information about configuring the Telephony Manager 3.1 Web browser client.

Make sure that the PC client requirements are met, as described in ["Telephony Manager 3.1 hardware requirements" \(page 33\)](#).

Configure Windows® XP SP2 to work with Telephony Manager 3.1

ATTENTION

Ensure firewalls and NAT routers are configured appropriately for Telephony Manager to facilitate free communication between the Telephony Manager server and clients, and between the Telephony Manager server, clients, and communication servers.

Procedure 41

Configure Windows XP SP2 to work with Telephony Manager 3.1

Step	Action
1	Open Control Panel > Windows Firewall . Choose one of the following options: - Select General tab, and then set Windows Firewall to Off, or - Select Exceptions tab, and then select only those applications that you want network access enabled.
2	To enable Web applications from the Internet Explorer menu bar, select Tools > Manage Add-Ons > and then select Add-ons that have been used by Internet Explorer in Show dropdown and enable each of the required items.
3	From the Internet Explorer menu bar, select Tools > Pop-Up Blocker > and then enable Pop-Up Blocker.

- 4 From the Internet Explorer menu bar, select **Tools > Internet Options > Security > Trusted Sites**, click **Sites** and then add server IP address to trusted site.

—End—

Accessing the Telephony Manager 3.1 Web server from a Web browser

Procedure 42

Accessing the Telephony Manager 3.1 Web server from a Web browser

Step	Action
------	--------

- | | |
|---|---|
| 1 | Enter the Telephony Manager 3.1 server IP address or computer name in the location bar of the Web browser on the PC client. To access the Telephony Manager Administrator page enter http://<tmserver hostname>/admin/ |
| 2 | Press Enter . |
-

—End—

Integrating Telephony Manager 3.1 with ENMS

Contents

This chapter contains information about the following topics:

"Overview" (page 188)

"Integration requirements" (page 188)

"Telephony Manager 3.1: ENMS integration" (page 189)

"Telephony Manager OIT files" (page 190)

"Checklist for installing the Optivity Integration Toolkit" (page 190)

"About oitInstall" (page 191)

"Using ENMS InfoCenter" (page 192)

"Viewing Telephony Manager 3.1 server object properties" (page 196)

"Modifying Telephony Manager 3.1 server object properties" (page 197)

"Starting Telephony Manager 3.1 Web applications" (page 197)

"Using FaultSummary" (page 200)

"Configuring Telephony Manager 3.1" (page 203)

"Removing a Telephony Manager 3.1 server" (page 203)

"Troubleshooting" (page 204)

Overview

Telephony Manager 3.1 integrates with ONMS versions 10.1 and 10.2 and ENMS version 10.4. ENMS is an enterprise-level network management solution providing fault, performance, configuration, and security management for Nortel inter-networking devices. Through ENMS, you can monitor your Telephony Manager 3.1 servers.

Telephony Manager 3.1 Alarm Manager receives SNMP traps from managed CS 1000 and Meridian 1 entities. Through Alarm Notification, Telephony Manager 3.1 sends filtered traps to ENMS.

By using ENMS InfoCenter, you can manually add Telephony Manager 3.1 servers into the Telephony Managers Resources folder. Property information that you add about the Telephony Manager 3.1 servers is added to the ENMS database. For access to ENMS documentation, in your Web browser go to www.nortel.com and follow the appropriate links.

InfoCenter graphically identifies when a device is in an alarm state. By using Optivity InfoCenter, you can set the color for alarm levels. When a device is in an alarm state, you can right-click it to open an ENMS fault management application. For instance, you can start Fault Summary that graphically lists faults for the selected device. You can also set the fault management categories for alarm monitoring.

Integration requirements

This section lists the conditions upon which Telephony Manager 3.1 integrates with ENMS optimally:

- For optimum performance, install Telephony Manager 3.1 on a separate computer from ENMS.
- For more information refer to the OIT support Web site at www.nortel.com. See [Procedure 43 "Downloading the OIT files" \(page 189\)](#) for details.
- Telephony Manager 3.1 integrates with ENMS through OIT on any NMS platform. See ["Checklist for installing the Optivity Integration Toolkit" \(page 190\)](#). Coresidence with ENMS, however, is supported only on Windows 2000 Server.
- All software requirements for Telephony Manager 3.1 must be met. Install IIS before applying the service pack.
- Always install ENMS prior to installing Telephony Manager 3.1.

There are certain restrictions in Telephony Manager 3.1 application features when installed coresident with ENMS.

- ENMS and Telephony Manager 3.1 use different Web servers: Apache and IIS respectively.

In the Telephony Manager 3.1 installation, when installing IIS, make sure that the default HTTP port 80 is not used by both the Apache and the IIS Web servers.

- Change the ENMS Apache Web server HTTP port from the default value of 80 prior to running IIS installation. If a port clash occurs, the default port on the Apache server must be changed.

Telephony Manager 3.1: ENMS integration

Telephony Manager 3.1 does not automatically install any OIT files. You must manually install the OIT files. The OIT files can be downloaded from the OIT support Web page.

Procedure 43

Downloading the OIT files

Step	Action
1	In your Web browser, go to http://www.nortel.com/ .
2	Click the Product link.
3	In the drop-down list, select ENMS OIT , and click Save .
4	In the drop-down list for software types, select ENMS OIT for Telephony Manager .
5	Click the link under the Description heading that matches your operating system platform.
6	Click the link to the Readme file to view the installation instructions in your Web browser. This file is also included in the zipped archive.
7	Click the link to the zipped archive to download the latest Telephony Manager 3.1 OIT files.

—End—

Integration with ENMS version 10.4

ENMS version 10.4 comes pre-installed with the device OIT files required for releases of Telephony Manager to OTM 2.0. The device OIT file for OTM 2.0 and the application OIT file must be downloaded and installed manually. The application OIT file is common to all releases of Telephony Manager. These OIT files can be obtained from the OIT support Web page. See [Procedure 43 "Downloading the OIT files" \(page 189\)](#) for details.

Telephony Manager OIT files

Telephony Manager 3.1 requires the following OIT files for integration with ENMS:

- NMS_otm_v10-B.oit
 - Telephony Manager server device support entries
 - Telephony Manager Open Alarm II definitions
- NMS_otmApp_v10-B.oit
 - Telephony Manager Web Application integration entries
 - Telephony Manager also contains the following mib file:
- rfc1223.mib
 - Standard RFC 12313 MIB definitions

Run oitInstall for each .oit file, one at a time. The .mib file must be present in the same directory when oitInstall is executed. See [step 5](#) under "[Checklist for installing the Optivity Integration Toolkit](#)" (page 190).

Checklist for installing the Optivity Integration Toolkit

This section provides general information about OIT. Refer to the NTPs, release notes, and read me files that are provided with your ENMS software package for specific information about OIT.

OIT files for Telephony Manager 3.1 can be installed on any platform that runs ENMS as long as it supports the Java Runtime Environment required by Telephony Manager 3.1 Web applications. In this case, follow the steps in this section.

In the case of coresidence, you must understand the prerequisites and install Telephony Manager 3.1. The installation of Telephony Manager 3.1 automatically performs the OIT integration steps. Steps 1 through 6, as shown in [Procedure 44 "Checking the current configuration"](#) (page 190), is used to check the OIT.

Checklist for a Telephony Manager 3.1 installation on an existing ENMS server

Procedure 44

Checking the current configuration

Step	Action
------	--------

- | | |
|---|----------------------------------|
| 1 | log on to ENMS as Administrator. |
|---|----------------------------------|

- 2 Check for the environment variable LNMSHOME.
View environment variables using the System option in Control Panel on the Environment Variables tab. This variable holds the path of the Optivity installation (typically, c:\Optivity\NMS). All the executables are located in c:\Optivity\NMS\bin.
- 3 Check for the environment variable OITHOME.
This environment variable points to the Optivity Integration Toolkit home directory (typically, C:\Optivity\oit). If unable to find OITHOME, create it.
- 4 Copy Telephony Manager 3.1 OIT files to the appropriate subdirectories in OITHOME.
All of the subdirectories under \Optivity\Oit\ on the Telephony Manager 3.1 CD-ROM are copied to OITHOME.
- 5 Run LNMSHOME\bin\oitinstall -u <full path of TM 3.1 OIT file> for every .oit file in the Telephony Manager Directory, where -u indicates to upgrade ENMS. If the -u format is not specified, only a syntax check is performed on the OIT file.
This command updates the ENMS database with the new definitions.
- 6 Proceed with Telephony Manager 3.1 installation, checking for prerequisites (IIS, for instance) as always.

—End—

About oitlInstall

ENMS includes a program, oitlInstall, that extracts the information that ENMS needs for new device application support.

This information includes:

- database schema definitions
- MIB information
- trap information
- device management application launch points from within ENMS applications
- device discovery information

OIT definitions for Telephony Manager 3.1 reside in \$OITHOME\OTM\otm.oit. It also contains the file rfc1213.mib.

The \$OITHOME environment variable is typically C:\Optivity\oit on Windows systems, and /usr/oit on UNIX.

What you do

OIT definitions are updated into ENMS by manually placing the OIT files into the appropriate directories and starting oitInstall from the command line.

For Telephony Manager 3.1, Telephony Manager 3.1 server must be added manually.

What OIT does

The oitInstall program does the following:

- Automatically stops and restarts all ENMS daemons (UNIX) or services (Windows).
- Automatically backs up the ENMS databases, by default /usr/oit/oitdb for UNIX, and C:\Optivity\oit\oitdb for Windows. The oitInstall program automatically restores the database if the device support upgrade installation fails.
- Updates ENMS with two new files: new device and device management support, and deletes the database backup if the integration is successful.

Using ENMS InfoCenter

When Telephony Manager 3.1 is integrated with ENMS and the OIT definition files, Telephony Manager 3.1 server objects must be added manually to the resources folders in InfoCenter. The Telephony Manager 3.1 integration does not currently support Autodiscovery of these objects.

You must be logged in as administrator or root to perform this activity.

Configuring ENMS InfoCenter for Telephony Manager 3.1

Procedure 45

Configuring ENMS InfoCenter for Telephony Manager 3.1

Step	Action
------	--------

- | | |
|---|---|
| 1 | Create a Voice Management folder in InfoCenter to contain all of the Voice Elements integrated into ENMS (Telephony Manager 3.1 in this case). |
| 2 | Modify the default Properties of the Voice Management folder to display the Optivity Telephony Manager objects added to this folder: <ul style="list-style-type: none">a. Right-click the Voice Management folder and choose Properties. See Figure 103 "InfoCenter Resources" (page 193).b. Open the Management server folder. |
-

- c. Select Telephony Manager. See Figure 104 "InfoCenter Voice Management Properties dialog box" (page 194).
- d. Click **Apply**.

—End—

The wizards provided in ENMS 9.0.1 and later add new Telephony Manager 3.1 servers to ENMS. These wizards automatically establish the Device-Agent-Interface relationship in ENMS databases.

Figure 103
InfoCenter Resources

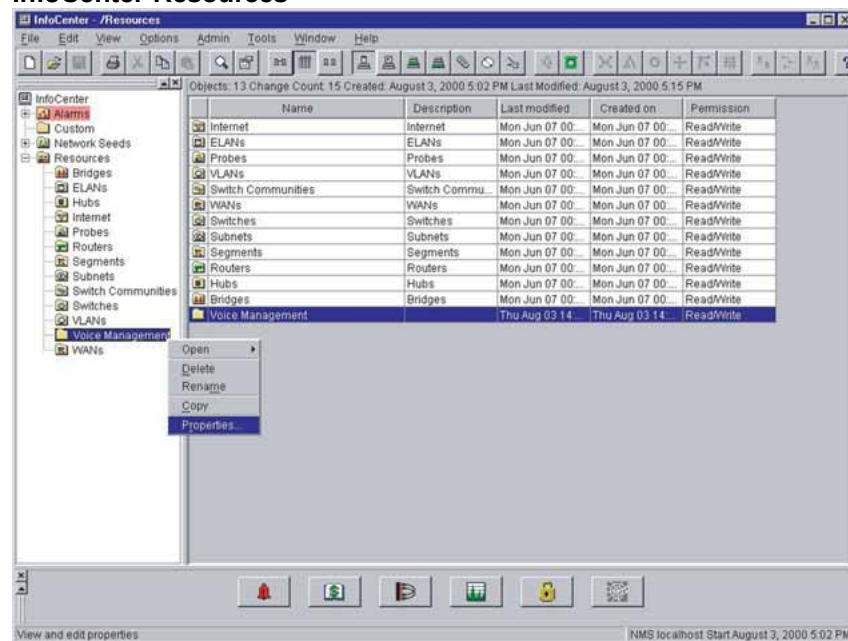
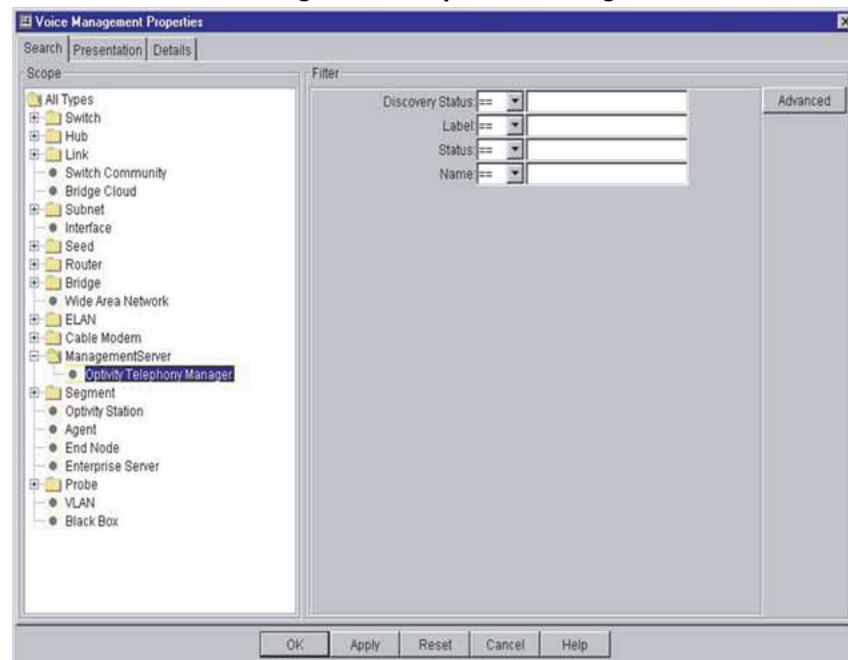


Figure 104
InfoCenter Voice Management Properties dialog box



Adding Telephony Manager 3.1 server object to ENMS InfoCenter

Add a Telephony Manager 3.1 server resource for every Telephony Manager 3.1 server that you integrate and monitor with ENMS.

If Access Control is enabled, you must have a valid local user account (user name and password) and an ENMS user account to log on to InfoCenter.

Procedure 46

Logging in to InfoCenter

Step	Action
1	From the Windows Start menu, choose Programs > Optivity > InfoCenter . The ENMS InfoCenter logon window appears.
2	Type the UserID, password, and the name of the ENMS server, and then click OK . ENMS InfoCenter appears.
3	In the Folders pane, click the InfoCenter icon.
4	Double-click the Resources folder to open it.
5	A Telephony Managers folder appears.

A Telephony Managers folder is created in ENMS InfoCenter to contain all the Voice Elements integrated into ENMS.

- 6 Double-click the **Telephony Managers** folder to open it.
- 7 Modify the default view properties of the folder or you cannot view the Telephony Manager 3.1 servers that are added to this folder.

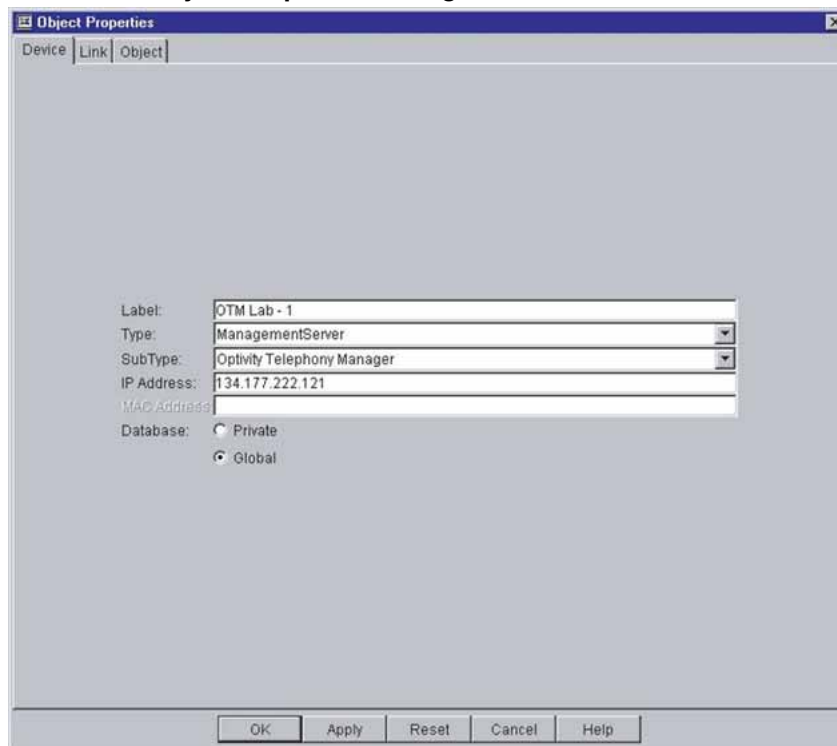
Right-click the **Telephony Managers** folder and choose **Properties**. Open the Management server folder. Select **Telephony Manager**, and click **Apply**.
- 8 From the InfoCenter menu bar, choose **File > New > Object**.

The Object Properties dialog box appears with the Device tab selected. See [Figure 105 "InfoCenter Object Properties dialog box" \(page 196\)](#).
 - a. In the Label box, type a label for the new object.
 - b. In the Type box, select the Management servers object type.
 - c. In the Subtype box, select a Telephony Manager subtype for the object.
 - d. In the IP address box, type the IP address of the object.
 - e. Click **Private** or **Global**.

Private lets the local user see the device. Global lets all users see the new object.
 - f. Click **OK**.A default switch icon appears for the Telephony Manager 3.1 server.

—End—

Figure 105
InfoCenter Object Properties dialog box



Viewing Telephony Manager 3.1 server object properties

Procedure 47

Viewing Telephony Manager 3.1 server Object Properties

Step	Action
1	In InfoCenter, open a folder in the Folders pane.
2	Select the Telephony Manager 3.1 server that you added.
3	From the InfoCenter menu bar, select File > Properties . The Object Properties dialog box appears, displaying the properties for the selected network object. Click OK .

—End—

Modifying Telephony Manager 3.1 server object properties

Procedure 48

Modifying Telephony Manager 3.1 server Object Properties

Step	Action
1	In InfoCenter, open a folder in the Folders pane.
2	Select the Telephony Manager 3.1 server that you added.
3	From the InfoCenter menu bar, select File > Properties . The Object Properties dialog box appears, displaying the properties for the selected network object.
4	Edit the object properties that you want. Click OK .

—End—

Starting Telephony Manager 3.1 Web applications

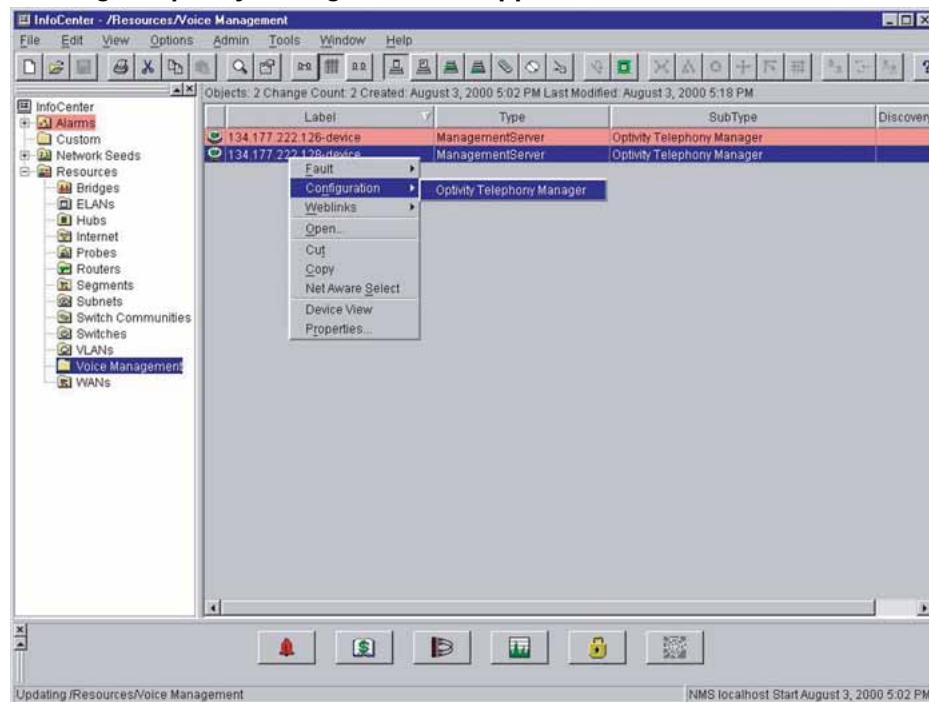
Telephony Manager 3.1 Web Application links are integrated with ENMS when a Telephony Manager 3.1 server is added.

The Telephony Manager 3.1 system accessed can be connected remotely through the network.

You can start Telephony Manager 3.1 Web applications by choosing Configuration and selecting Telephony Manager from the shortcut menu on the Telephony Manager 3.1 icon in Enterprise NMS InfoCenter. See [Figure 106 "Starting Telephony Manager 3.1 Web applications" \(page 198\)](#).

This action launches the default Web browser for your system and connects to the Telephony Manager 3.1 Web server. See ["Java Runtime Environment for Telephony Manager 3.1 and Enterprise NMS" \(page 198\)](#) for details on JRE.

Figure 106
Starting Telephony Manager 3.1 Web applications



Java Runtime Environment for Telephony Manager 3.1 and Enterprise NMS

Telephony Manager 3.1 Web applications require Java Plug-In 1.5.0_02 on the client browser. Enterprise NMS uses JDK 1.1.x, which is older than the version used by Telephony Manager 3.1.

JRE clash for Telephony Manager 3.1 and Enterprise NMS Web clients

In both co-resident and non-co-resident situations, Telephony Manager 3.1 and Enterprise NMS applications cannot be launched simultaneously. The successful launch of Telephony Manager 3.1 and Enterprise NMS Web applications accessing JRE depends on the version of JRE currently loaded in the system.

If a version of JRE that is different than 1.5 is loaded in the system and you access Telephony Manager 3.1 Web applications, you are prompted to install and load Java Plug-In 1.5.0_02 the first time that you try to connect to the Telephony Manager 3.1 server. With the Java Plug-In 1.5.0_02 loaded, Telephony Manager 3.1 Web applications load successfully.

If a version of JRE that is higher than 1.2.2 is loaded on the system, then Enterprise NMS Web applications that require JRE cannot be launched. This can occur even when the lower version is installed, but not loaded, on the system. To successfully launch Enterprise NMS Web applications, you must remove the higher version of JRE, and run the JRE 1.2.2 setup program.

JRE release specific to Apache Tomcat

Apache Tomcat is associated with the latest Java Runtime Environment (JRE) installed on the server. If that release is removed from the server, Tomcat fails. The user must update Tomcat to replace the JRE path with a different path.

To update the Apache Tomcat path, as shown in [Figure 107 "Apache Tomcat Properties dialog"](#) (page 200), follow [Procedure 49 "Updating Apache Tomcat path"](#) (page 199).

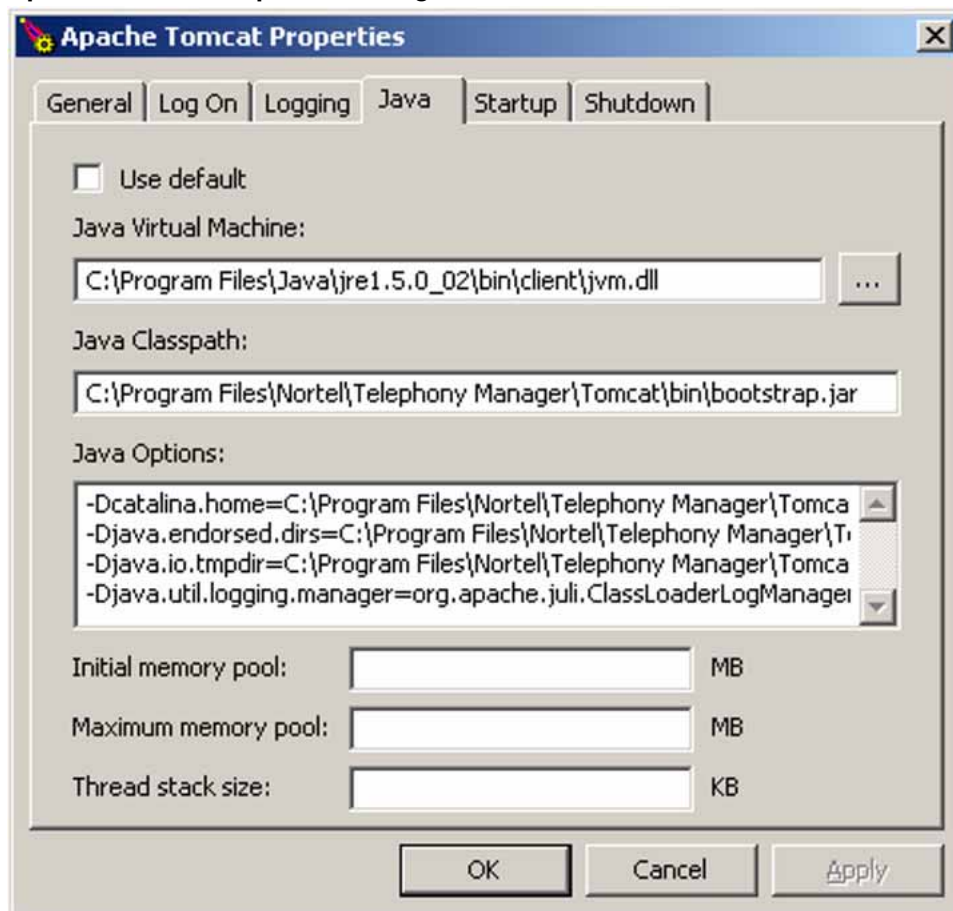
Procedure 49

Updating Apache Tomcat path

Step	Action
1	Go to Start > All Programs > Apache Tomcat 5.5 > Configure Tomcat .
2	Select Java tab on the Apache Tomcat properties page.
3	Update Apache Tomcat path.
4	Click OK or Apply to save changes.
5	Restart Apache Tomcat service.

—End—

Figure 107
Apache Tomcat Properties dialog



Web server

ENMS uses Apache Web server for its Web applications, whereas Telephony Manager 3.1 uses Internet Information server (IIS).

Using FaultSummary

Telephony Manager 3.1 filters and then forwards system traps to ENMS. Because Telephony Manager 3.1 forms the main representative agent for systems, all alarms received by ENMS result in the change of status state of Telephony Manager 3.1 depicted in Optivity InfoCenter.

When ENMS and Telephony Manager 3.1 co-reside on the same server, the Telephony Manager 3.1 Trap system disables its Trap server and instead interfaces with the Optivity Trap server to receive traps.

Upon receiving a system alarm (or other traps that it is configured to handle), Telephony Manager 3.1 reformats it and forwards it to ENMS. ENMS recognizes the trap (from OIT definitions) and is able to reflect the changed status.

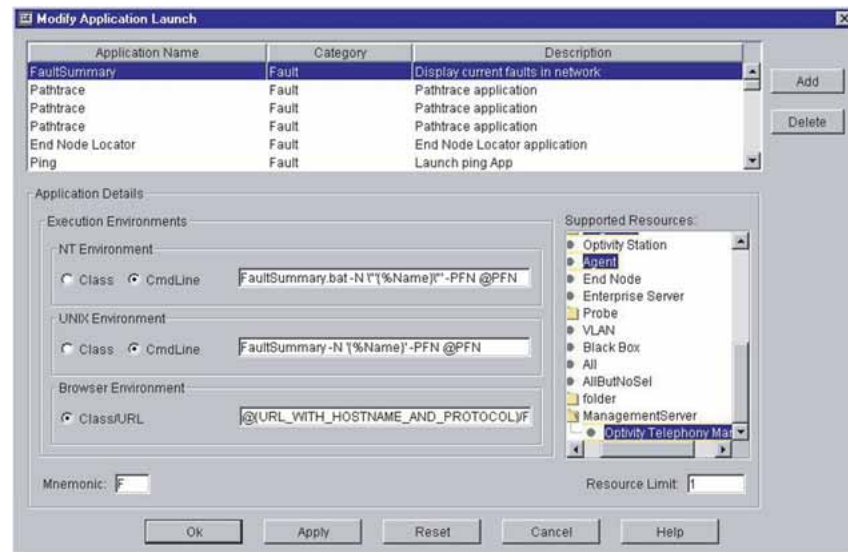
Procedure 50 Setting up FaultSummary

Step	Action
------	--------

- | | |
|---|--|
| 1 | Select Application Launch from InfoCenter's top menu. |
| 2 | Select the Fault Summary application. See Figure 108 "Modify Application Launch dialog box" (page 201). |
| 3 | While holding down the Ctrl and Shift keys, select the Managementserver > Telephony Manager resource to enable FaultSummary for Telephony Manager 3.1. |
| 4 | Click Apply . |

—End—

Figure 108
Modify Application Launch dialog box

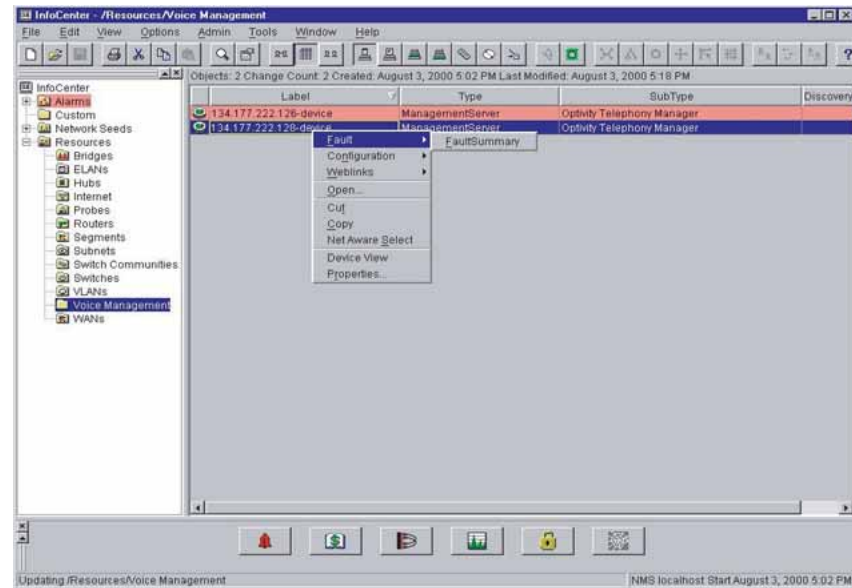


Procedure 51
Launching FaultSummary

Step Action

- 1 Select the Telephony Manager 3.1 icon and use the right-click menu to launch FaultSummary. See [Figure 109 "Launch FaultSummary"](#) (page 202).

Figure 109
Launch FaultSummary



—End—

Configuring Telephony Manager 3.1



CAUTION Service Interruption

Telephony Manager 3.1 is included in the device file to monitor the alarms received from the Telephony Manager 3.1 server. When Telephony Manager 3.1 coresides with ENMS, the trap server is shared and both ENMS and Telephony Manager 3.1 receive and process all traps. In this case, the number of traps is multiplied and the trap server receives a large volume of traps, which can cause the trap server to crash. To prevent this, you must modify the notification script on the coresident Telephony Manager 3.1 system so that traps are not forwarded to the Telephony Manager 3.1 server.

The Telephony Manager 3.1 server must be set up to forward traps to Enterprise NMS. Forwarded traps must be in the Telephony Manager 3.1 Open Alarm II format to be recognized.

The Telephony Manager 3.1 Alarm notification application forwards traps of interest to Enterprise NMS.

Sample scripts are provided with the Alarm Notification application, which you can modify in the following ways to forward traps:

- Change the target IP to the address of the Enterprise NMS server.
- Select the severity of the traps that you want to forward: Critical, Major, Minor.
- Modify the sample scripts to forward traps to Enterprise NMS.

Take care to translate the incoming trap to Telephony Manager 3.1 Open Alarm II, and set the proper device identification and error code fields.

These traps, when received by Enterprise NMS, result in a change of status of Telephony Manager 3.1 and can be viewed through the Fault Summary.

Removing a Telephony Manager 3.1 server

Procedure 52

Removing a Telephony Manager 3.1 server

Step	Action
1	In InfoCenter, open a folder in the Folders pane.
2	Select the Telephony Manager 3.1 server that you want to delete.

- 3 From the InfoCenter menu bar, choose **File > Delete**. This action deletes the object from ENMS.

—End—

Troubleshooting

If you do not see the OITHOME environment variable, you must manually set it before installing Telephony Manager 3.1 or manually running oitlInstall to update the Enterprise NMS database.

If you do not see Managementserver type and Telephony Manager sub-type on the Device — Add panel:

- Check to see if the OITHOME variable was set.
- Check to see if the Telephony Manager 3.1 OIT files are present and in the correct folder.
- Check the oitlInstall log file to verify that the Telephony Manager 3.1 entries were updated.
- You need to run oitlInstall again.

If you cannot see the Telephony Manager 3.1 server that you have added:

- Check the View Properties of the folder to verify that it can display Telephony Manager 3.1 servers.

If you cannot launch or connect to Telephony Manager 3.1 Web applications:

- Verify that the IP Address of the Telephony Manager 3.1 server entered in InfoCenter is correct.
- Verify that the Telephony Manager 3.1 Web server is running.
- Verify that you have the proper Java Plug-In installed.

If you are not receiving traps from an Telephony Manager 3.1 server:

- Verify that the Telephony Manager 3.1 Alarm Notification application is running and receiving traps.
- Verify that the Telephony Manager 3.1 Alarm Notification scripts are configured to send traps to Enterprise NMS.
- Check the oitlInstall log files to verify that the Telephony Manager 3.1 entries were updated.
- Check the status of Enterprise NMS daemons from Control Panel > Services, or by typing `optstatus -fe` at the command prompt.

If you cannot launch Fault Summary for Telephony Manager 3.1:

- Check the Application Launch entries. FaultSummary is enabled for Managementserver > Telephony Manager.

Integrating Telephony Manager 3.1 with HP OpenView

Contents

This chapter contains information about the following topics:

"Overview" (page 207)

"Limitations" (page 208)

"Hardware and software requirements" (page 208)

"System integration" (page 209)

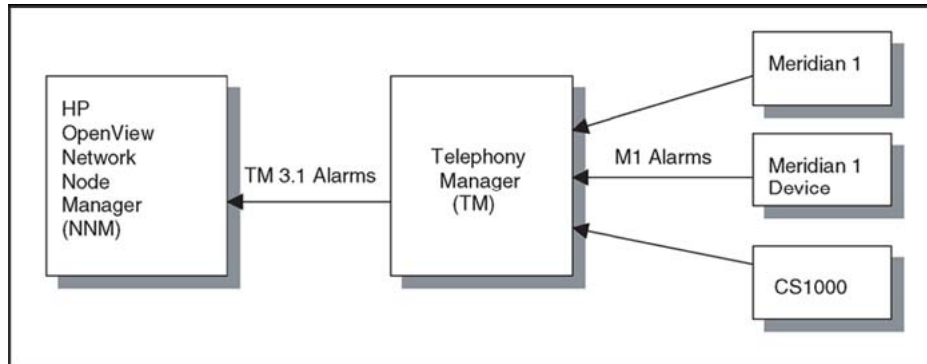
"Installation and configuration" (page 211)

Overview

This chapter provides information about the integration of the HP* OpenView* (HP OV) Network Node Manager (NNM) management platform with Nortel's Telephony Manager 3.1. It discusses the type of integration supported. The included procedures provide detailed step-by-step instructions on how to configure HP OV NNM to access Telephony Manager 3.1-related functionality and information.

Nortel's technical support for this feature is limited to support of the two software files that are distributed with Telephony Manager 3.1, *OtmOpenAlarm.mib* and *OtmStMon.exe*. These files are compatible with the version of HP OpenView that was current at the time your Telephony Manager software was released.

Figure 110
Telephony Manager 3.1 alarm integration with HP OpenView Network Node Manager



As seen in [Figure 110 "Telephony Manager 3.1 alarm integration with HP OpenView Network Node Manager"](#) (page 208), Communication Server 1000 and Meridian 1 systems, Meridian Mail, and other devices send their alarms to the Telephony Manager 3.1 server, which can then collect the alarms and forward them to the NNM. The NNM appears the Telephony Manager 3.1 alarms in its Alarm Browser and updates the color of the Telephony Manager 3.1 object in the Network Map to reflect the current status of the Telephony Manager 3.1 server, or the status of the devices the Telephony Manager 3.1 server manages. In addition, you can also configure the NNM to allow the network administrator easy access to the Telephony Manager 3.1 server.

See *Telephony Manager 3.1 System Administration (NN43050-601)* for information about configuring the Telephony Manager 3.1 server to forward alarms to an external management station.

Limitations

- coresidency is not supported for NNM and Telephony Manager 3.1 on the same PC. However, for Web clients, if the appropriate version of JRE is loaded in the system and the default Web browser is Internet Explorer, both Telephony Manager 3.1 and HP OpenView Web applications can be launched simultaneously.
- The Telephony Manager 3.1 server does not support auto-discovery from NNM.

Hardware and software requirements

PC hardware requirements (HP OV PC)

Refer to HP OV NNM documentation for details.

PC software requirements (HP OV PC)

- HP OV NNM Release 6.4.1(7.0.1)
- TM 3.1 Alarm Integration Package:
 - Telephony Manager 3.1 Alarm MIB (OtmOpenAlarm.mib)
 - Telephony Manager 3.1 Status Monitor (OtmStMon.exe)

Telephony Manager 3.1 software requirements (Telephony Manager 3.1 PC)

- Alarm Notification application
- Web-based alarm browser

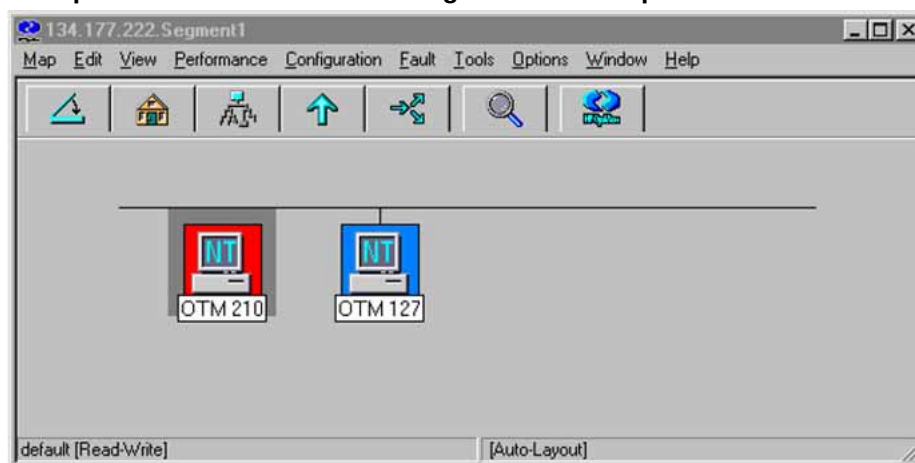
System integration

HP OV NNM Network Map

On the NNM Network Map. See [Figure 111 "HP OpenView Network Node Manager Network Map"](#) (page 209), a Telephony Manager 3.1 server can be represented as an object. You can configure incoming events to trigger a color change to the object icon to indicate the current status of the Telephony Manager 3.1 server or of the devices monitored by the Telephony Manager 3.1 server.

Figure 111

HP OpenView Network Node Manager Network Map

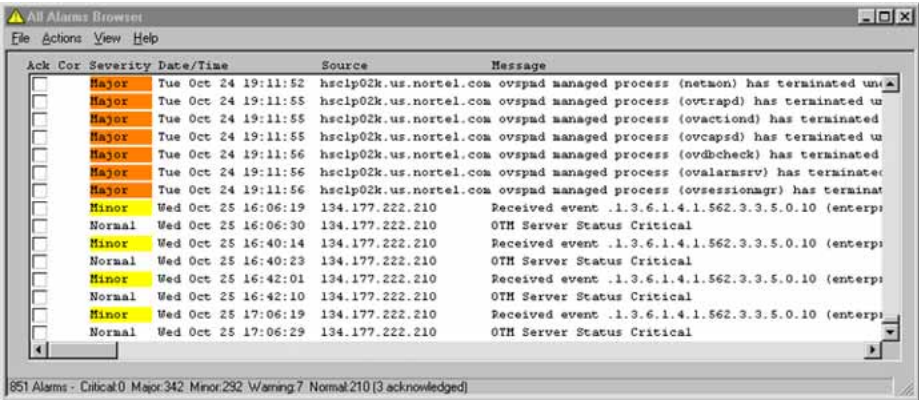


The Telephony Manager 3.1 Status Monitor (OtmStMon) is the program that is used to update the color of the icon for a Telephony Manager 3.1 object. When the color is changed upon the receipt of an incoming event, a message is also logged and appears in the NNM Alarm Browser to indicate the status update.

HP OV NNM Alarm Browser

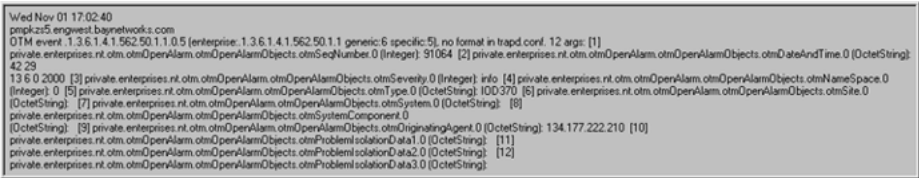
You can display contents of incoming Telephony Manager 3.1 events in the NNM Alarms Browser. See [Figure 112 "HP OV NNM Alarms Browser" \(page 210\)](#).

Figure 112
HP OV NNM Alarms Browser



You can also highlight a specific alarm message on the NNM Alarms Browser, and right-click to display the message content in a separate window. See [Figure 113 "Alarm message content" \(page 210\)](#). You can then analyze the different variables and their values.

Figure 113
Alarm message content

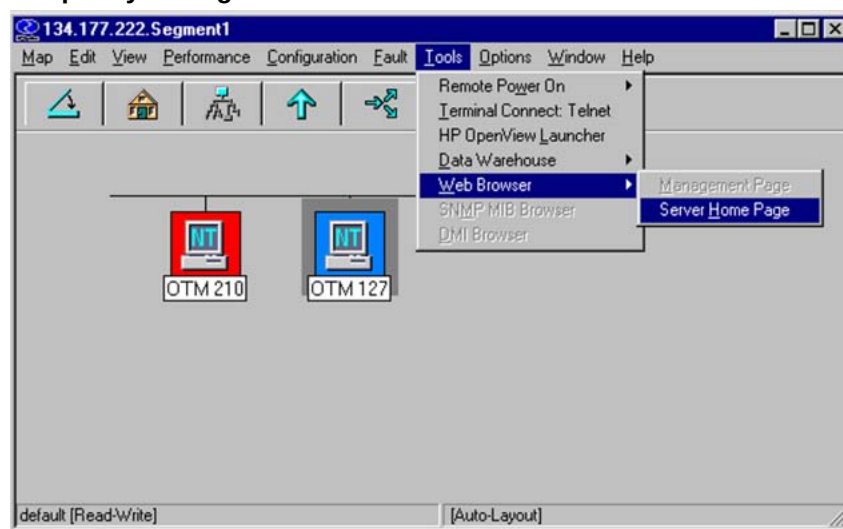


Telephony Manager 3.1 Web Access

Procedure 53
Accessing the Telephony Manager 3.1 server from NNM

Step	Action
1	Highlight the Telephony Manager 3.1 object on the Network.
2	Select Tools > Web Browser > server Home Page Figure 114 "Telephony Manager 3.1 Web Access" (page 211) .

Figure 114
Telephony Manager 3.1 Web Access



Your default Web browser is brought up with the Web-based Telephony Manager 3.1 interface. You can log on to the Telephony Manager 3.1 Web and access the various Telephony Manager 3.1 applications including the Telephony Manager 3.1 Alarm Browser.

—End—

Installation and configuration

Telephony Manager 3.1 Alarm Integration Package (HP OV PC)

1. Copy the OtmStMon.exe to the Openview/bin (\$OV_BIN) directory.
2. Copy the OtmOpenAlarm.mib to the directory \$OV_SNMP_MIB/Vendor/Nortel. Create this directory if it does not already exist.

HP OV NNM (HP OV PC)

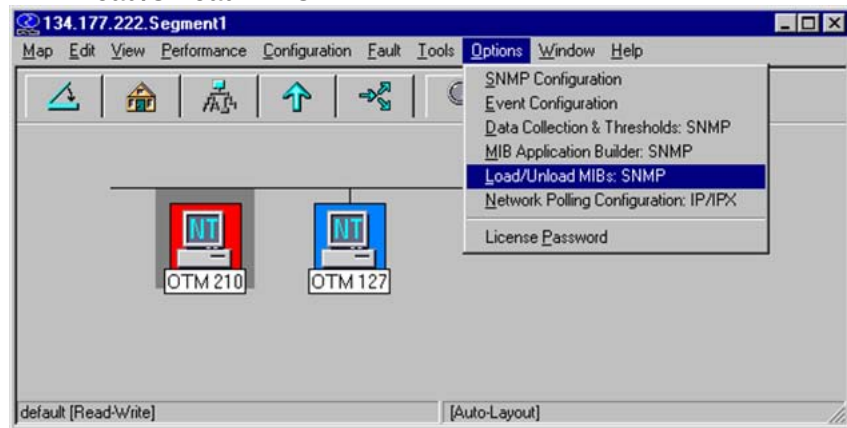
The following configuration procedures are performed while NNM is running:

Procedure 54

Installing Telephony Manager 3.1 Alarm MIB

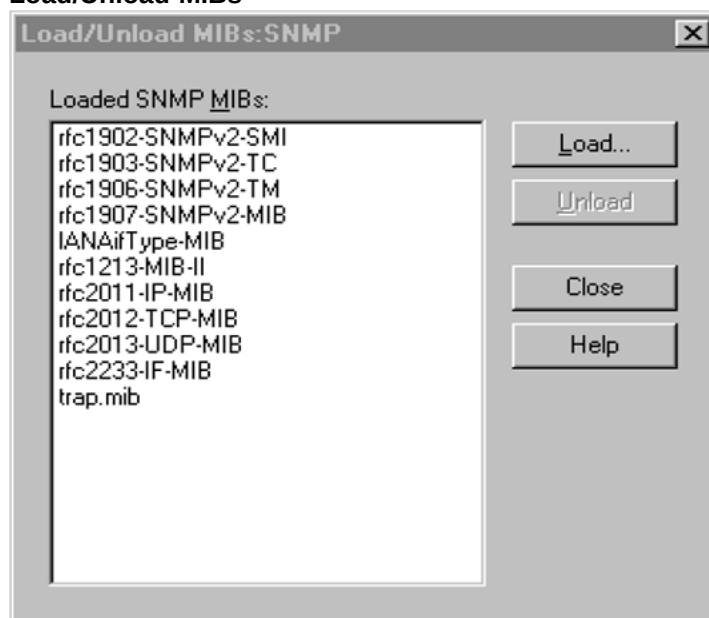
Step	Action
1	Select Options > Load/Unload MIBs: SNMP . See Figure 115 "NNM Load/Unload MIBs" (page 212) .

Figure 115
NNM Load/Unload MIBs



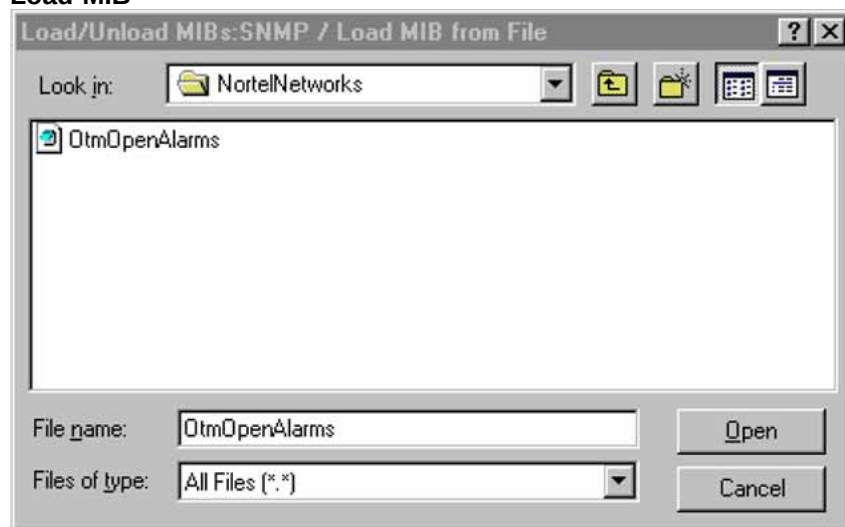
- 2 Click **Load** in the Load/Unload MIBs dialog box. See [Figure 116 "Load/Unload MIBs"](#) (page 212).

Figure 116
Load/Unload MIBs



- 3 Open the OtmOpenAlarm.mib file. See [Figure 117 "Load MIB"](#) (page 213).

Figure 117
Load MIB



The Telephony Manager 3.1 alarm MIB definitions are now loaded into the NNM's MIB database.

—End—

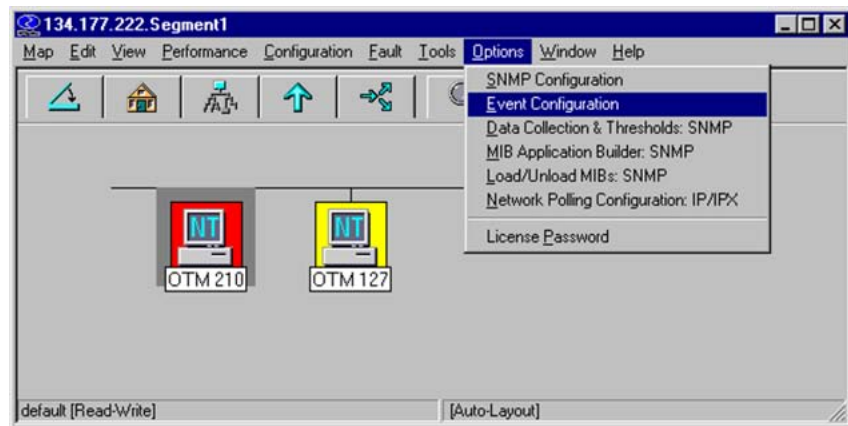
After the Telephony Manager 3.1 Alarm MIB is loaded, actions must be defined through the NNM Event Configuration for each Telephony Manager 3.1 event. (See [Procedure 55 "Configuring an event" \(page 213\)](#)).

Procedure 55 **Configuring an event**

Step	Action
------	--------

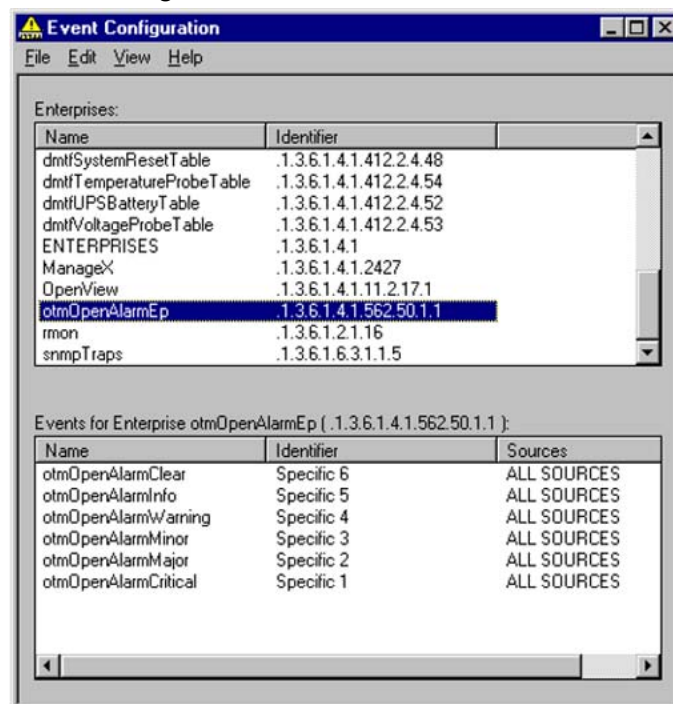
- | | |
|---|--|
| 1 | Select Options > Event Configuration . See Figure 118 "NNM Main Menu - Event Configuration" (page 214) . |
|---|--|

Figure 118
NNM Main Menu - Event Configuration



- 2 Locate and select **otmOpenAlarmEp** from the list of Enterprises. See [Figure 119 "Event Configuration"](#) (page 214).

Figure 119
Event Configuration



There are six events defined for the otmOpenAlarmEp Enterprise. For each event, you configure the desired actions to be taken if the event occurs.

Use the Telephony Manager 3.1 Major Alarm event (otmOpenAlarmMajor, Specific 2) as an example:

- 3 Double-click the corresponding entry on the list.

The Modify Events dialog box appears. See [Figure 120 "Modify Events - Description"](#) (page 215).

Figure 120
Modify Events - Description

Modify Events

Description Sources Event Message Actions Forwarding

Event Name: otmOpenAlarmMajor Enterprise: otmOpenAlarmEp

Generic Trap: Enterprise Specific Specific Trap Number: 2

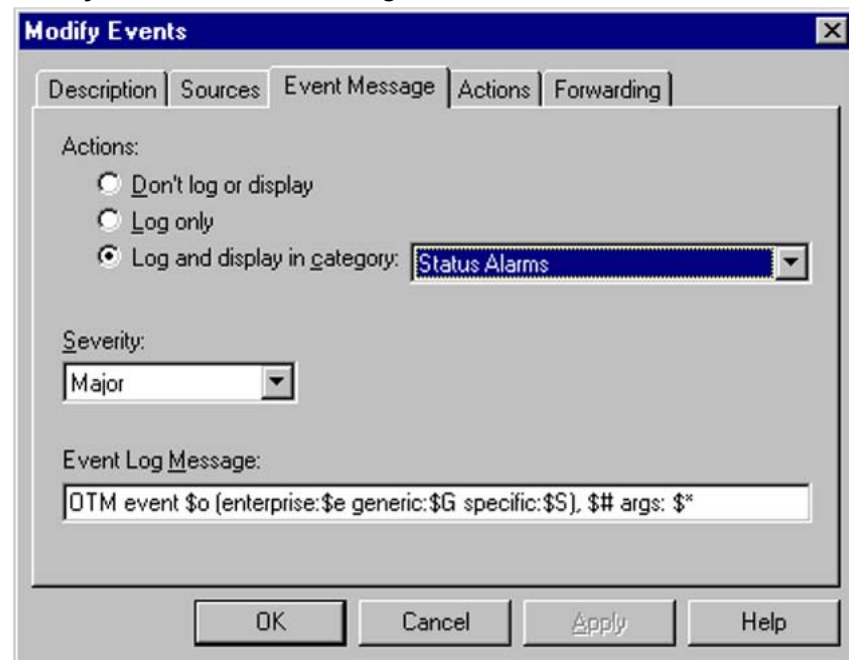
Description:

Long Descr.: The OTM Open Alarm Trap with a severity of major(2).
This trap is intended to be internationalizable, hence, it contains no natural language text.

OK Cancel Apply Help

- 4 Select the Event Message tab. See [Figure 121 "Modify Events - Event Message"](#) (page 216).

Figure 121
Modify Events - Event Message



- 5 Configure the following:
 - a. Actions: Select Log and display in category: Status Alarms.
 This enables the display of the incoming event message in the NNM Alarm Browser.
 - b. Severity: Select Major for this event.
 - c. Event Log Message: Enter the following default text:
 Telephony Manager 3.1 event \$o (enterprise:\$e generic:\$G specific:\$S), \$# args: \$*
 The displayed message shows the contents of the event message. See [Table 12 "Legend for variables in the Event Log Message" \(page 217\)](#) for other variables.
 You are allowed to display any message that you choose in the Alarm Browser.

—End—

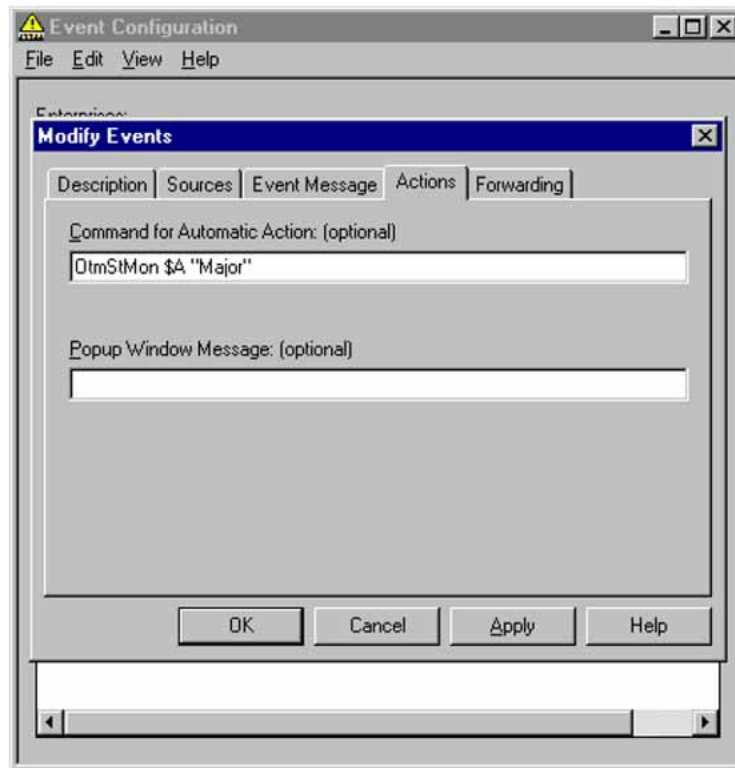
The following table provides the legend for \$ variables in the Event Log Message.

Table 12
Legend for variables in the Event Log Message

Variable	Action
\$o	Print the name (object identifier) of the received event as a string of numbers.
\$e	Print the trap enterprise as an Object ID string of numbers. This number is implied by the event object identifier for non-SNMPv1 events.
\$G	Print the trap's generic-trap number. This number is implied by the event object identifier for non-SNMPv1 events.
\$S	Print the trap's specific-trap number. This number is implied by the event object identifier for non-SNMPv1 events.
\$#	Print the number of attributes in the event.
\$*	Print all the attributes as seq name (type): value strings, where seq is the attribute sequence number.

If you also want the color of the object on the map to change to reflect the occurrence of the incoming event, you can also invoke the Telephony Manager 3.1 Status Monitor (OtmStMon.exe) by specifying a call to it under the Actions item. See [Figure 122 "Modify Events - Actions" \(page 218\)](#).

Figure 122
Modify Events - Actions



Telephony Manager 3.1 Status Monitor

The Telephony Manager 3.1 Status Monitor enables you to change the color of the Telephony Manager 3.1 object on the Network Map to reflect the current status of the server. In addition, a message is also logged onto the HP OV NNM Alarm Browser to indicate the status change.

OtmStMon is written in C and makes use of the HP OV ovevent application. OtmStMon takes in two parameters: an object's selection name and a textual representation of the new status (for example, Critical or Normal). If ovevent cannot locate an object on the current Network Map with the specified selection name, an error message appears. Therefore, if a Telephony Manager 3.1 object is not defined in the Network Map, OtmStMon are not invoked for an event.

The invocation format for OtmStMon is as follows:

OtmStMon <selection_name> <object_status>

where

<selection_name> is HP OV NNM's unique selection name for an object item on the Network Map.

<object_status> is one of the following textual strings: Unknown, Normal, Warning, Minor, Major, Critical, Restricted, Testing, Disabled, Managed, Unmanaged.

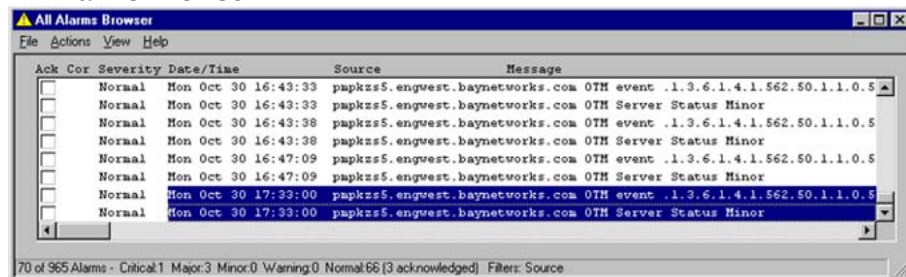
If the Telephony Manager 3.1 Status Monitor is not called, then the color of the object that appears on the Network Map does not change for the incoming event.

If no object is defined for the Telephony Manager 3.1 server on the Network Map, a call to Telephony Manager 3.1 Status Monitor results in an error. Therefore, do not specify calls to OtmStMon if there is no Telephony Manager 3.1 server defined on the Map.

A call to the Telephony Manager 3.1 Status Monitor results in a message, in addition to the original incoming event message, appearing in the NNM All Alarms Browser. See [Figure 123 "All Alarms Browser" \(page 219\)](#). This message is logged whenever the Telephony Manager 3.1 Status Monitor changes the color of an object.

Not every incoming Telephony Manager 3.1 event necessitates the changing of the object's color. For example, a minor or info event may not need to alert the customer. In these cases, the customer may want to configure these events in such a way to simply log the incoming event message and not call OtmStMon.

Figure 123
All Alarms Browser

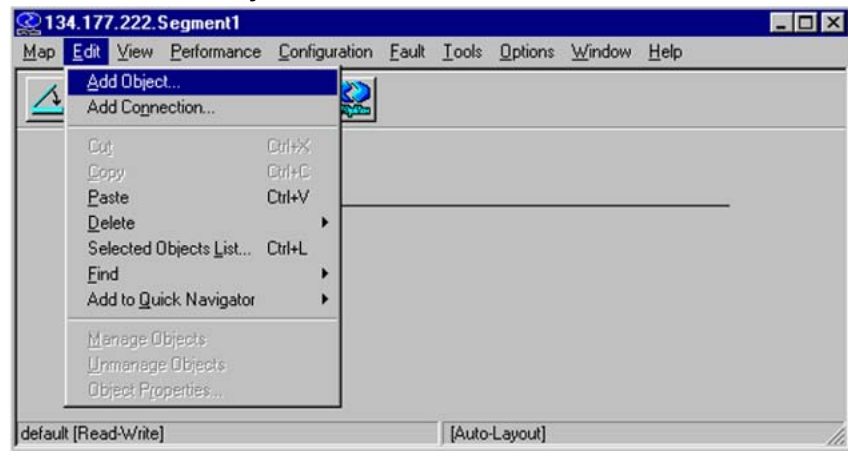


Procedure 56

Setting up a Telephony Manager 3.1 server object on the Network Map

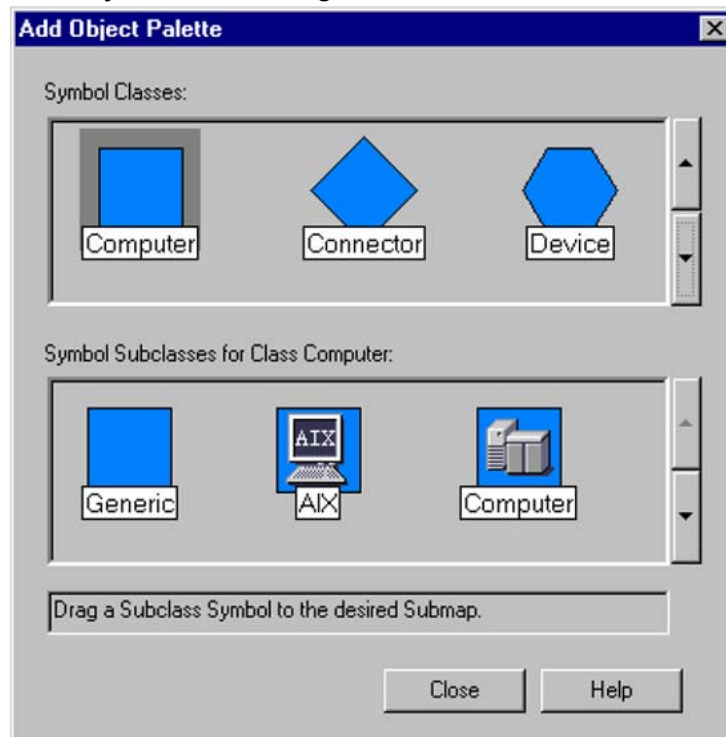
Step	Action
1	Locate the appropriate place in the Network Map for the Telephony Manager 3.1 server.
2	Select Edit > Add Object . See Figure 124 "NNM Edit - Add Object" (page 220) .

Figure 124
NNM Edit - Add Object



- 3 Select **Computer** from the Symbol Classes in the **Add Object Palette** dialog box. See [Figure 125 "Add Object Palette dialog box"](#) (page 220).

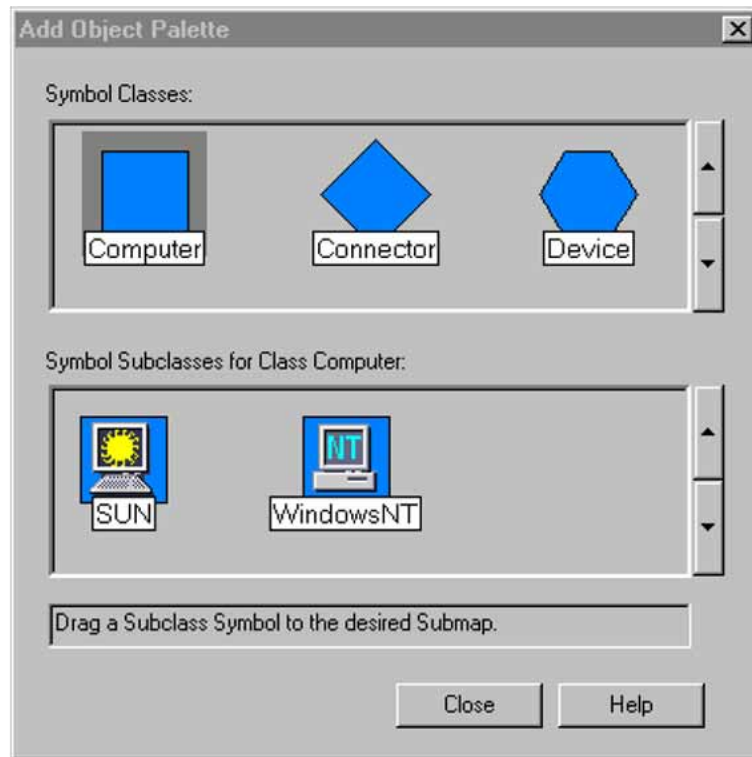
Figure 125
Add Object Palette dialog box



- 4 Select and drag the standard WindowsNT icon from the Symbol Subclasses. See [Figure 126 "Add Object Palette dialog box II" \(page 221\)](#) onto the appropriate location on the Network Map.

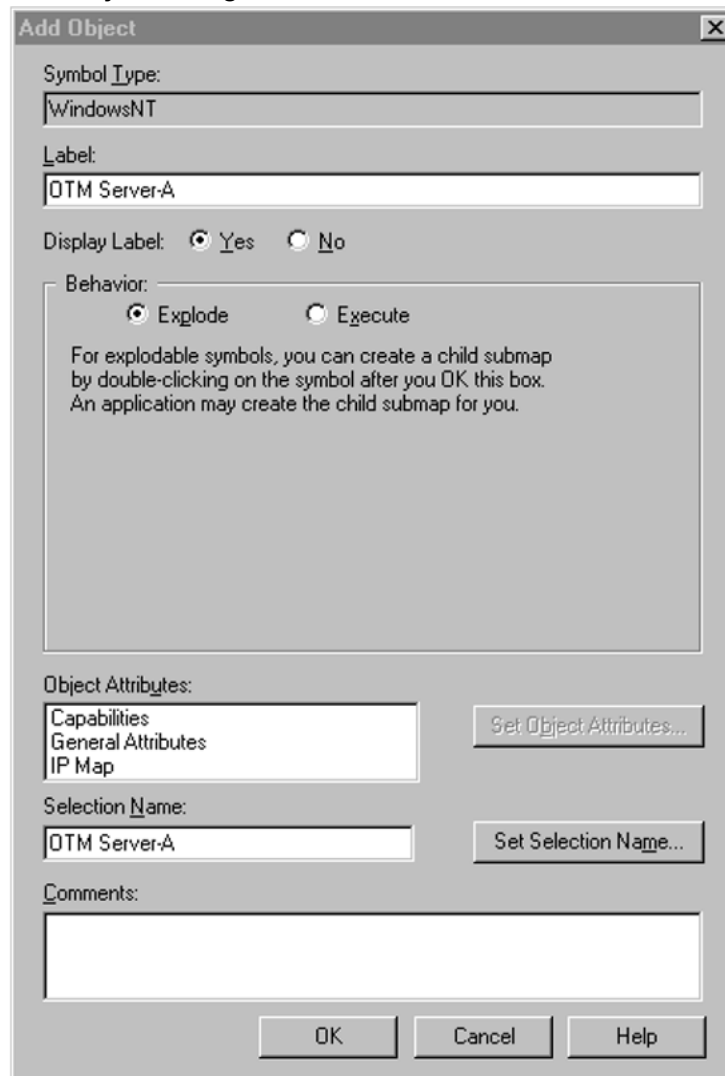
The Add Object dialog box appears.

Figure 126
Add Object Palette dialog box II



- 5 Fill in the Label field (Telephony Manager 3.1 server-A in this example). See [Figure 127 "Add Object dialog box" \(page 222\)](#).

Figure 127
Add Object dialog box



The 'Add Object' dialog box is a standard Windows-style window with a title bar containing a close button (X). It contains several sections for configuring a new object:

- Symbol Type:** A text field containing 'WindowsNT'.
- Label:** A text field containing 'OTM Server-A'.
- Display Label:** Two radio buttons, 'Yes' (selected) and 'No'.
- Behavior:** Two radio buttons, 'Explode' (selected) and 'Execute'. Below them is a text box containing the instruction: 'For explodable symbols, you can create a child submap by double-clicking on the symbol after you OK this box. An application may create the child submap for you.'
- Object Attributes:** A list box containing 'Capabilities', 'General Attributes', and 'IP Map'. To the right is a button labeled 'Set Object Attributes...'. The 'IP Map' option is currently selected.
- Selection Name:** A text field containing 'OTM Server-A'. To the right is a button labeled 'Set Selection Name...'. The 'OTM Server-A' text is also present in the list box above.
- Comments:** A large empty text area for additional notes.
- Buttons:** At the bottom are three buttons: 'OK', 'Cancel', and 'Help'.

- 6 Select **IP Map** under Object Attributes, and click **Set Object Attributes**. See [Figure 128 "Add Object - IP Map" \(page 223\)](#).

Figure 128
Add Object - IP Map

The 'Add Object' dialog box is shown with the following fields and options:

- Symbol Type:** WindowsNT
- Label:** OTM Server-A
- Display Label:** ☒ Yes ☐ No
- Behavior:** ☒ Explode ☐ Execute
- Object Attributes:** Capabilities, General Attributes, IP Map (selected)
- Selection Name:** OTM Server-A
- Comments:** (empty text area)

Buttons at the bottom: OK, Cancel, Help.

- 7 Select and enter the Hostname, IP Address, and Subnet Mask. See [Figure 129 "Add Object - Set Attributes dialog box"](#) (page 224).

Figure 129
Add Object - Set Attributes dialog box

Name	Value
*Hostname :	pmpkzs5.engwest.baynetworks.com
*IP Address :	134.177.222.127
Subnet Mask :	255.255.255.0
Physical Address :	

Messages:

This information is valid. Press OK to continue.

OK Verify Cancel Help

- 8 Click **OK**. You are returned to the Add Object dialog box. In the Selection Name field, enter the same value as that of the Hostname in the previous step (pmpkzs5.engwest.baynetworks.com in this example). See [Figure 130 "Add Object - Selection Name"](#) (page 225).

Figure 130
Add Object - Selection Name

Add Object

Symbol Type:
WindowsNT

Label:
OTM Server-A

Display Label: ☒ Yes ☐ No

Behavior:
☒ Explode ☐ Execute

For explodable symbols, you can create a child submap by double-clicking on the symbol after you OK this box. An application may create the child submap for you.

Object Attributes:
Capabilities
General Attributes
IP Map

Selection Name:
pmpkzs5.engwest.baynetworks.com

Comments:

Set Object Attributes...
Set Selection Name...
OK Cancel Help

- 9 Click **OK**. The object is created on the Network Map.



CAUTION
Service Interruption

The value for Hostname must be the domain name server (DNS) representation of the IP address (if the IP address can be resolved locally). Use the command **nslookup** to retrieve the DNS representation if you do not already know it. See [Figure 131 "nslookup command" \(page 226\)](#). If the IP address cannot be interpreted locally, then enter the dotted decimal representation.

Figure 131
nslookup command

```

Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

D:\>nslookup 134.177.222.127
Server:  zmpkhg01.us.nortel.com
Address:  47.239.48.3

Name:     pmpkzs5.engwest.baynetworks.com
Address:  134.177.222.127

D:\>_

```

- 10 If you want to indicate the status of the Telephony Manager 3.1 server through the color of the object on the map, be sure to set the Status Source under Symbol Properties to Object. See [Figure 132 "NNM Main Menu - Symbol Properties"](#) (page 226) and [Figure 133 "Symbol Properties dialog box"](#) (page 227).

Figure 132
NNM Main Menu - Symbol Properties

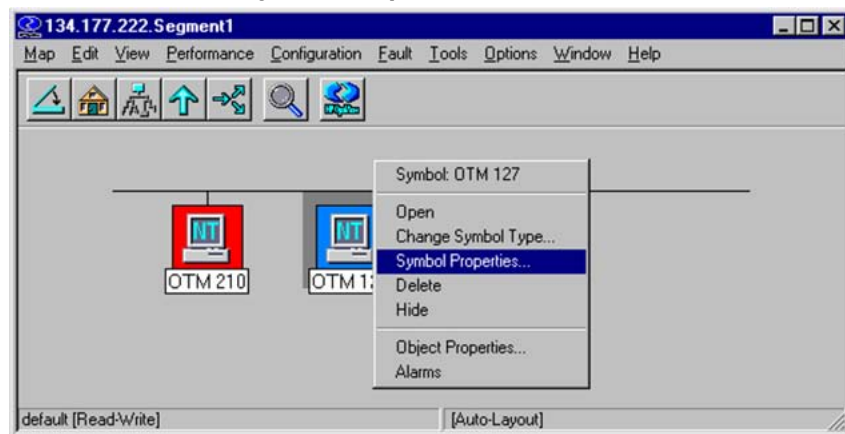
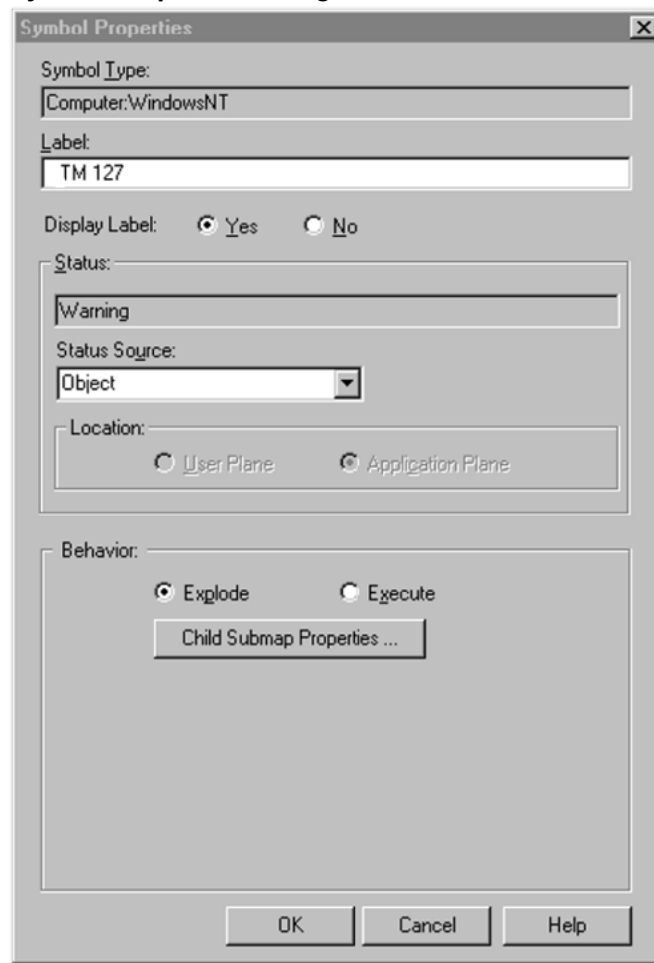


Figure 133
Symbol Properties dialog box



—End—

The Management URL can also be configured to access the Telephony Manager 3.1 server. See [Figure 134 "Object Properties dialog box" \(page 228\)](#) and [Figure 135 "Attributes for Object dialog box" \(page 229\)](#). For an object on the Network Map, under General Attributes in the Object Properties dialog box, follow the procedure [Procedure 57 "Configuring Telephony Manager 3.1 Web server Access" \(page 228\)](#).

Procedure 57**Configuring Telephony Manager 3.1 Web server Access****Step Action**

- 1 Enter the address (IP address or the DNS name) of the Telephony Manager 3.1 server in the ManagementURL field.
- 2 Set isHTTPSupported to **True**.

Figure 134
Object Properties dialog box

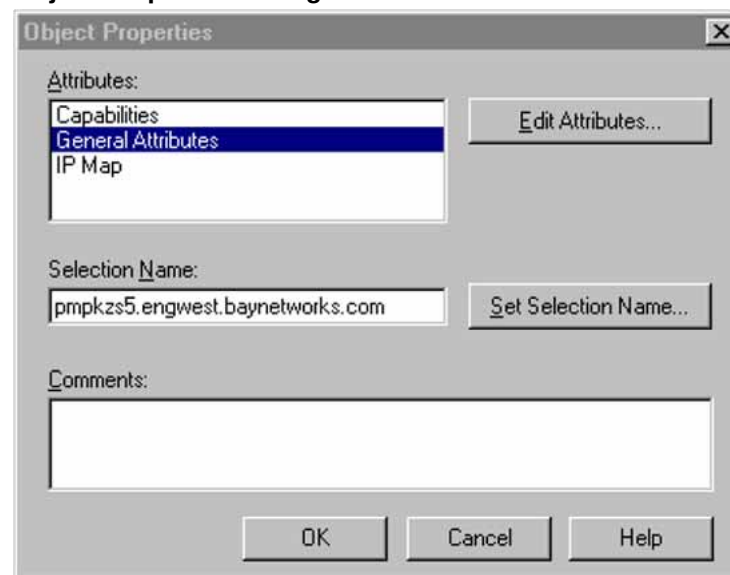
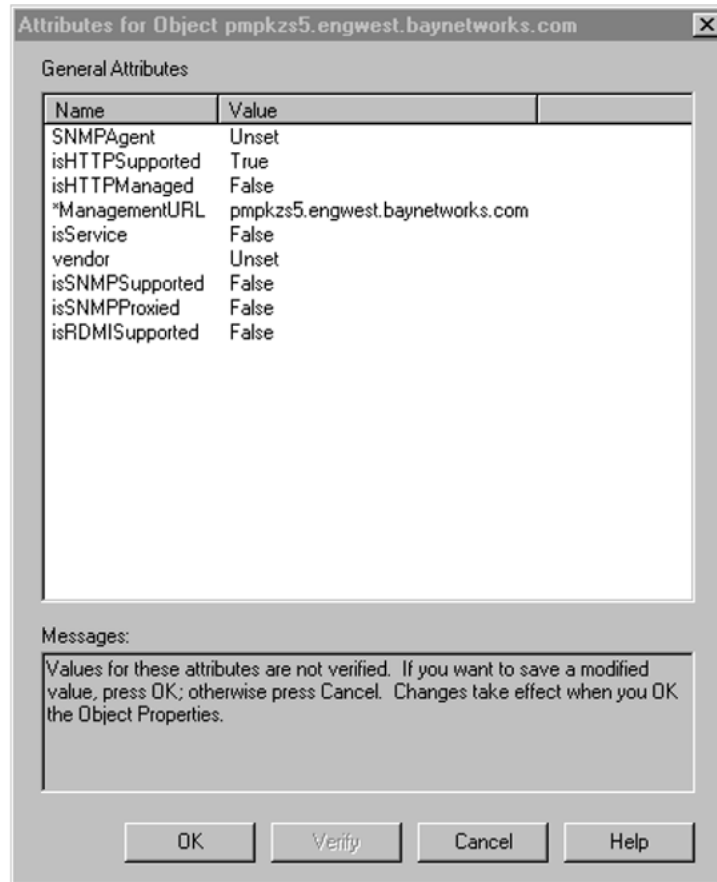


Figure 135
Attributes for Object dialog box



—End—

Telephony Manager 3.1 configuration (Telephony Manager 3.1 PC)

Refer to the Alarm Management section in *Telephony Manager 3.1 System Administration (NN43050-601)* for information about configuring the Telephony Manager 3.1 server to forward SNMP traps to HP OV NNM or other remote systems.

Converting Systems in Telephony Manager

Contents

This chapter contains information about converting the following:

Procedure 58 "Converting a CS 1000S to CS 1000E CPPM" (page 232)

Procedure 59 "Converting a CS 1000M Cabinet/Chassis to CS 1000E CPPM " (page 232)

Procedure 60 "Converting a Meridian 1 system to CS 1000M/E system" (page 233)

Procedure 61 "Converting a Branch Media gateway CS 1000M Cabinet/Chassis system to CS 1000E CPPM" (page 233)

Overview

This chapter contains information about how to convert systems in Telephony Manager 3.1. There is no automatic conversion utility in Telephony Manager, so the user must manually convert the system. This is a one-time operation.

ATTENTION

During conversion, it is possible that the set TN license limit is temporarily exceeded, prompting a warning message that this has occurred. No action is required. Once the old system is deleted, after verification that the data in the new system is correct, the number of set TN licenses should return to the pre-conversion number.

To convert a CS 1000S system to CS 1000E CPPM in Telephony Manager, follow [Procedure 58 "Converting a CS 1000S to CS 1000E CPPM" \(page 232\)](#).

Procedure 58**Converting a CS 1000S to CS 1000E CPPM****Step Action**

- 1 Perform backup of TBS and Traffic data.
- 2 From Telephony Manager Navigator, add a new CS 1000M/E system. See "Adding a System" section in *Telephony Manager 3.1 System Administration (NN43050-601)*.
- 3 Retrieve all Station, List Manager, and ESN data from the switch.
- 4 Restore TBS and Traffic data from the backup location. See to "Backup and Restore" section in *Telephony Manager 3.1 System Administration (NN43050-601)*.
- 5 Verify that the data is correct for the new CS 1000E CPPM system.
- 6 Delete the old CS 1000S system from Telephony Manager.

—End—

To convert a CS 1000M Cabinet/Chassis system to CS 1000E CPPM in Telephony Manager, follow [Procedure 59 "Converting a CS 1000M Cabinet/Chassis to CS 1000E CPPM "](#) (page 232).

Procedure 59**Converting a CS 1000M Cabinet/Chassis to CS 1000E CPPM****Step Action**

- 1 Run **Update System Data** in the system window.
- 2 Retrieve all Station data from the switch.
Before retrieving the Station data, ensure that all the telephone records are in Sync status **Transmitted** (use Global Edit, if required).

—End—

To convert a Meridian 1 to CS 1000M/E, follow [Procedure 60 "Converting a Meridian 1 system to CS 1000M/E system"](#) (page 233).

Procedure 60**Converting a Meridian 1 system to CS 1000M/E system**

Step	Action
1	Select Signaling server present check box in the Network tab.
2	Run Update system data from the system window.
3	If the old system is Meridian 1 11C Cabinet/Chassis and if the new system is CS 1000E CPPM, then retrieve all Station data from the switch. Before retrieving the Station data, ensure that all the telephone records are in Sync status Transmitted (use Global Edit, if required).

—End—

To convert a Branch Office CS 1000M Cabinet/Chassis to CS 1000E CPPM, follow [Procedure 61 "Converting a Branch Media gateway CS 1000M Cabinet/Chassis system to CS 1000E CPPM" \(page 233\)](#).

Procedure 61**Converting a Branch Media gateway CS 1000M Cabinet/Chassis system to CS 1000E CPPM**

Step	Action
1	Run Update system data from the system window.
2	Retrieve all Station data from the switch. Before retrieving the Station data, ensure that all the telephone records are in Sync status Transmitted (use Global Edit, if required).

—End—

ATTENTION

If the Meridian 1 11C Cabinet/Chassis system or CS 1000M Cabinet/Chassis system has a survivable cabinet or survivable media gateway attached, and if the system is converted to CS 1000E CPPM, then the media gateways will be deleted from Telephony Manager during update system data.

Uninstalling Telephony Manager 3.1

Contents

This chapter contains information about the following topics:

["Overview" \(page 235\)](#)

["Uninstalling Telephony Manager 3.1" \(page 235\)](#)

Overview

This chapter contains information about using Uninstall to remove software that is no longer needed, or that has become damaged or was incorrectly installed.

In Telephony Manager 3.1, the installation application is flexible, permitting uninstallation of both Telephony Manager Client and Telephony Manager Server separately when they are not accessible to each other.

Previously, the user could uninstall the Telephony Manager Server when there were no clients, and uninstall the Telephony Manager Client prior to uninstalling the Telephony Manager Server.

The enhanced installation application permits the additional uninstallation situations:

- The Telephony Manager 3.1 Server can be uninstalled prior to uninstalling the Telephony Manager Clients.
- The Telephony Manager Client can be uninstalled when the Telephony Manager Server is not accessible or is already uninstalled.

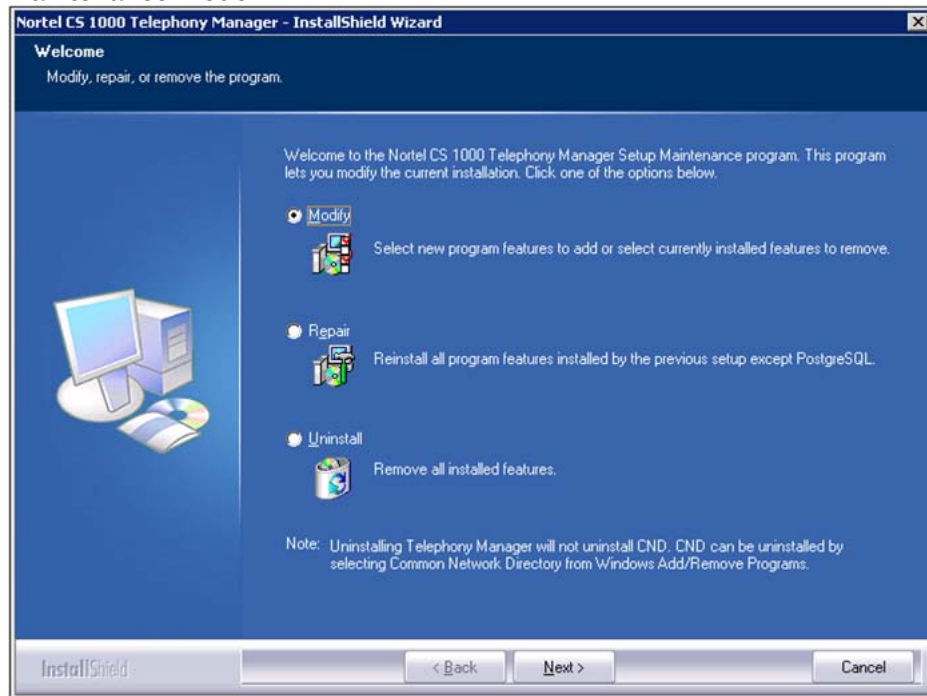
Uninstalling Telephony Manager 3.1

When the Telephony Manager Client and Telephony Manager Server are not accessible to each other, uninstallation of either can be performed.

Maintenance mode

With Telephony Manager 3.1 successfully installed, run Setup.exe from the installation CD ROM to enter the InstallShield Wizard Maintenance mode (see [Figure 136 "Maintenance mode" \(page 236\)](#)).

Figure 136
Maintenance mode

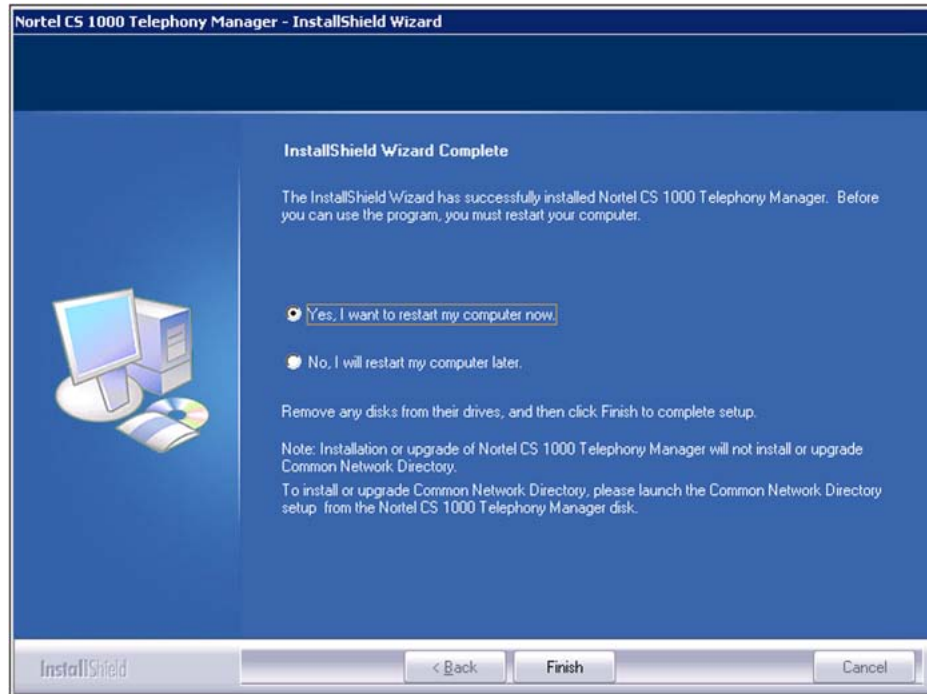


Maintenance mode provides the following options:

- **Modify:** Using the modify option, the user can perform an install and uninstall of Telephony Manager 3.1 components such as Web Help.
- **Repair:** The Repair option performs a reinstall of the existing installation, application files of the existing installation without modifying the data files.
- **Uninstall:** The Uninstall option performs an uninstall of the Telephony Manager 3.1 installation. A warning is issued and the user is prompted to proceed. Upon completion, the Uninstall Complete window appears (see [Figure 144 "Uninstall Complete" \(page 242\)](#)).

Upon completion of the selected Maintenance operation, the Maintenance Complete window appears (see [Figure 137 "Maintenance Complete" \(page 237\)](#)),

Figure 137
Maintenance Complete



Uninstallation of Telephony Manager Client or Telephony Manager Server

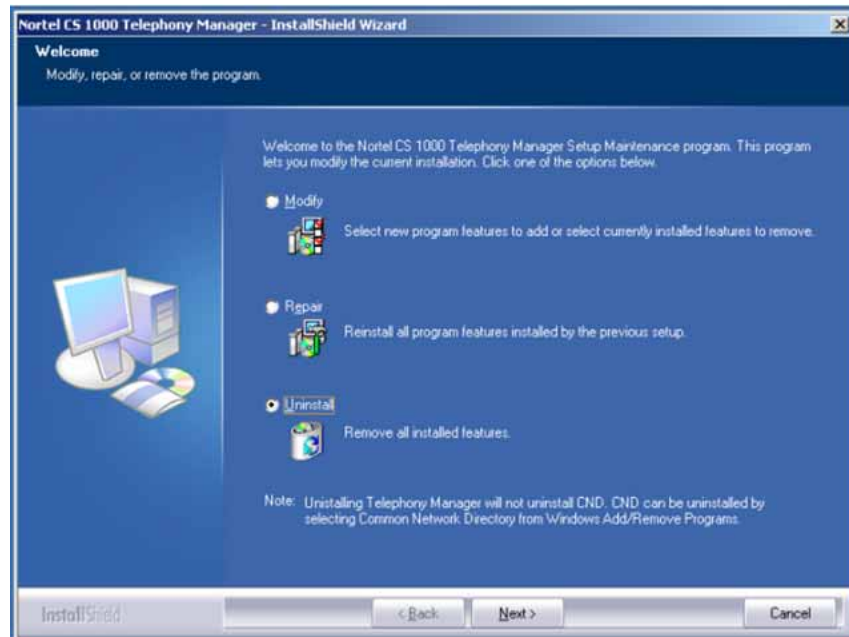
The Telephony Manager client or Telephony Manager Server can be uninstalled separately, regardless of whether or not they are accessible to each other.

Procedure 62

Uninstalling Telephony Manager Server with no clients associated

Step	Action
1	Select the Uninstall radio button from the Telephony Manager InstallShield Wizard, as shown in Figure 138 "Telephony Manager InstallShield wizard" (page 238).

Figure 138
Telephony Manager InstallShield wizard



If no clients are associated prior to uninstallation of the Telephony Manager Server, a confirmation message displays, as seen in [Figure 139 "Telephony Manager Server uninstall confirmation--no client"](#) (page 238).

Figure 139
Telephony Manager Server uninstall confirmation--no client



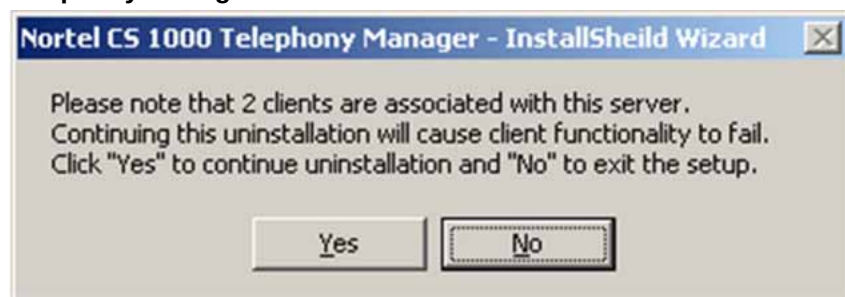
- 2 Click **Yes** to continue the Telephony Manager Server uninstallation.
- 3 Click **No** to cancel the uninstallation.

—End—

Procedure 63**Uninstalling Telephony Manager Server with clients associated****Step Action**

- 1 Select the **Uninstall** radio button from the Telephony Manager InstallShield Wizard, as shown in [Figure 138 "Telephony Manager InstallShield wizard"](#) (page 238).

If any clients are associated with the server prior to uninstallation, a confirmation message displays, as seen in [Figure 140 "Telephony Manager Server uninstall confirmation--with clients"](#) (page 239).

Figure 140**Telephony Manager Server uninstall confirmation--with clients**

- 2 Click **Yes** to continue the Telephony Manager Server uninstallation.
- 3 Click **No** to cancel the uninstallation.

—End—

When clients are associated with the server, uninstallation of the server creates problems in the functionality of the client. In this case, the functionality of the Telephony Manager Client fails.

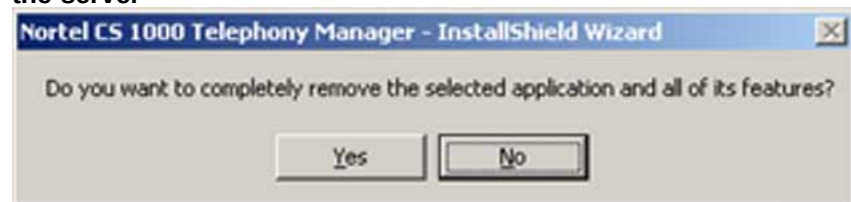
Procedure 64**Uninstalling Telephony Manager Client if able to access Common Data path of Telephony Manager Server****Step Action**

- 1 Select the **Uninstall** radio button from the Telephony Manager InstallShield Wizard, as shown in [Figure 138 "Telephony Manager InstallShield wizard"](#) (page 238).

If the Telephony Manager Client can access the Common Data path of the Telephony Manager Server during uninstallation, a confirmation message displays, as shown in [Figure 141 "Telephony Manager Client uninstall confirmation--with access to the server"](#) (page 240).

Figure 141

Telephony Manager Client uninstall confirmation--with access to the server



- 2 Click **Yes** to continue the Telephony Manager Client uninstallation.
- 3 Click **No** to cancel the uninstallation.

—End—

Procedure 65

Uninstalling Telephony Manager Client if unable to access Common Data path of Telephony Manager Server

Step	Action
------	--------

- | | |
|---|---|
| 1 | Select the Uninstall radio button from the Telephony Manager InstallShield Wizard, as shown in Figure 138 "Telephony Manager InstallShield wizard" (page 238). |
|---|---|

If the Telephony Manager Client can not access the Common Data path of the Telephony Manager Server during uninstallation, a confirmation message displays, as shown in [Figure 142 "Telephony Manager Client uninstall confirmation--with no access to the server"](#) (page 240).

Figure 142

Telephony Manager Client uninstall confirmation--with no access to the server



- 2 Click **Yes** to continue the Telephony Manager Client uninstallation.
- 3 Click **No** to cancel the uninstallation.

—End—

Procedure 66

Deleting client information on the server manually

Step	Action
------	--------

- | | |
|---|--|
| 1 | Select Navigator > Utilities > Manage . |
| 2 | Select appropriate client. |
| 3 | Click delete . |

ATTENTION

A client IP can be deleted if you do a fresh installation of Telephony Manager 3.1.
The only way to restore a deleted client is to reinstall the Telephony Manager software on the client PC.

—End—

Reasons the Telephony Manager Client fails to map the Common Data path of the Telephony Manager Server are:

- The Telephony Manager Server is uninstalled.
- The Telephony Manager Server is not accessible, due to hard disc crash.
- The network between the Telephony Manager Server and the Client is down.
- The Telephony Manager Server is shut down.

Uninstall using Add/Remove Programs

Telephony Manager 3.1 can also be uninstalled by using the Add/Remove Programs window. A confirmation dialog box appears (see [Figure 143 "Uninstall confirmation"](#) (page 242)).

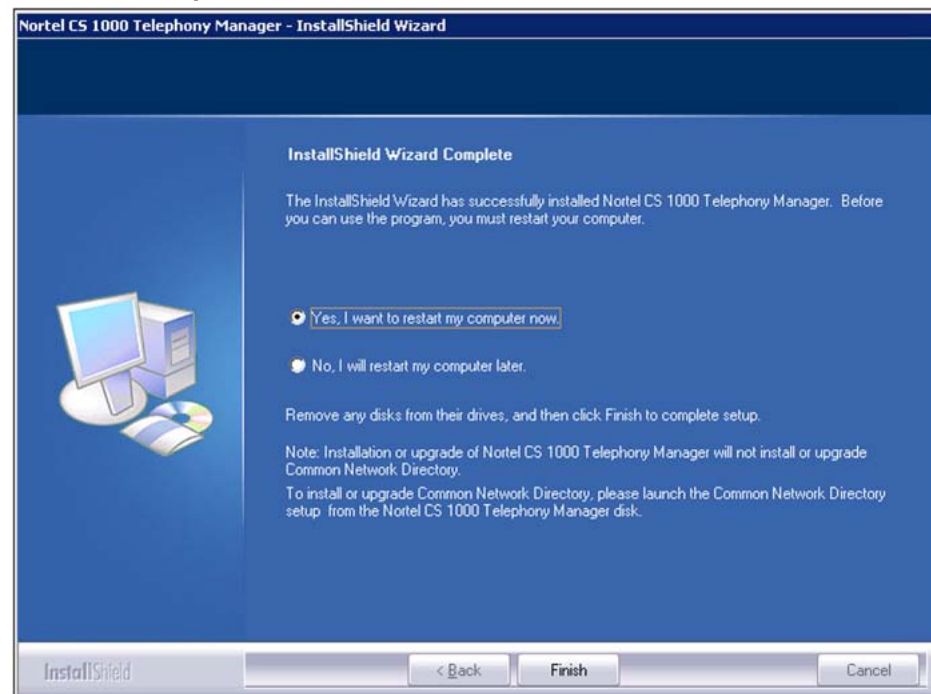
Figure 143
Uninstall confirmation



The CND components, if installed, are not removed during a Telephony Manager uninstallation. The machine requires a reboot after the uninstall is performed.

Upon completion of the uninstall operation, the Uninstall Complete window appears (see [Figure 144 "Uninstall Complete"](#) (page 242)).

Figure 144
Uninstall Complete



Windows 2000 Server reference

Contents

This chapter contains information about the following topics:

"Overview" (page 243)

"Installing Telephony Manager 3.1 on Windows 2000 Server" (page 243)

"Installing Network Adapter software" (page 246)

"Testing network cards" (page 253)

Overview

This chapter describes Windows® 2000 installation. Due to hardware and software differences, this example may not match your installation.

If a certain component is already correctly installed, then skip the installation of that component.

Installing Telephony Manager 3.1 on Windows 2000 Server

Hardware compatibility check

Check all hardware against the documentation available on Microsoft's Web site at www.microsoft.com/windows2000/support/onlinedocs/default.mspx.

Running the Windows setup program

Procedure 67

Installing the Windows server by using the Windows setup program

Step	Action
------	--------

This procedure shows you how to install Windows server using the setup program:

- | | |
|---|---|
| 1 | Make sure the first bootup option on CD-ROM in the BIOS is enabled. |
| 2 | Insert the Windows server setup CD-ROM into the CD-ROM drive. |

- 3 Boot the system.
- 4 In the Windows server Setup Welcome dialog box, press Enter to set up the Windows server.
- 5 In the Windows Licensing Agreement dialog box, press Page Down to go to the bottom of the page, and then choose F8.
- 6 Press C to create a partition, and then type the size of the partition that you want to create.
- 7 Use the up and down arrow keys to select the partition created on the first disk in step 6.
- 8 Press Enter to set up Windows server on the selected partition.
- 9 Use the up and down arrow keys to select Format partition using the NTFS files system, and then press Enter.
- 10 Wait while the setup program formats the partition. This takes several minutes.
- 11 Wait while the setup program copies files to the Windows installation folders. This takes several minutes.
- 12 Reboot the system.
When the system reboots, press F2 to instruct the system to boot from the hard drive instead of the CD-ROM.

—End—

Installing Windows server components

Procedure 68

Installing Windows server components

Step	Action
------	--------

Windows server setup continues after the reboot.

- | | |
|---|---|
| 1 | The Installing Devices dialog box appears. This takes several minutes. |
| 2 | The Regional Settings dialog box appears. Select the default values or configure as needed, and then click Next . |
| 3 | The Personalize Your Software dialog box appears. Enter your name and the name of your organization, and then click Next . |

- 4 The Your Product Key dialog box appears. Enter the product key, and then click **Next**.
- 5 The Licensing Modes dialog box appears. Select the default value, or choose Per server or Per Seat, as appropriate, and then click **Next**.
- 6 The Computer Name and Administrator Password dialog box appears. Enter the computer name and the administrator password, and then click **Next**.
- 7 The Windows Components dialog box appears. Select the default values or select specific components, as appropriate, and then click **Next**.
- 8 The Date and Time Settings dialog box appears. Adjust the Date, Time, and Time Zone, as appropriate, and then click **Next**.
- 9 Wait for the Network Settings dialog box to appear. This takes several minutes.
- 10 When the Network Settings dialog box appears, accept the default value, Typical Settings, and then click **Next**.
- 11 The Workgroup or Computer Domain dialog box appears. Make the appropriate selection, and then click **Next**.
- 12 Wait while the set up program installs components. This takes several minutes.
- 13 Wait while the set up program performs final tasks. This takes several minutes.
- 14 The Completing the Windows Setup Wizard dialog box appears. Click **Finish** to reboot the system.

—End—

Allowing Telephony Manager 3.1 client access without constant server log on (optional)

Telephony Manager windows and Web clients require an administrator account to be logged into the server at all times, since it uses the identity of the logged-in user for access.

To allow Telephony Manager 3.1 client access without logging into the server at all times, the following configuration change for Windows server is required.

Procedure 69**Allowing Telephony Manager 3.1 client access without constant server log on (optional)**

Step	Action
1	log on to the Windows server.
2	Go to Start > Programs > Administrative Tools > Component Services .
3	From the Component Services window, expand Computers > My Computer > COM+ Applications .
4	Select Telephony Manager 3.1 Application , and open the Properties window.
5	Select the Identity tab and click on the This User radio button.
6	Enter the local administrator account and password.
7	Click OK .

ATTENTION

This procedure works for all applications except DECT.

—End—

Installing Network Adapter software

Before configuring the network adapters, make sure that the adapters are inserted properly into the slots and RJ45 cables are plugged into the adapters. The Nortel server Subnet Interface card is recommended to install on the top PCI slot and ELAN subnet on the second-from-the-top PCI slot.

Procedure 70**Installing Network Adapter software**

Step	Action
1	In Windows 2000 Setup, verify that the Wired to the network check box is selected, and then click Next .
2	In the Install Microsoft Internet Information server dialog box, clear the box, and then click Next .
3	Click Select from the List in the Network Adapter dialog box.

- 4 Click **Have Disk** and insert the CD from the manufacturer (shipped with the network card). Click **OK** and select the appropriate driver from the list. Click **OK** to continue.
- 5 The next window appears your LAN card. Because the server has two LAN cards, click on **Select from the list** to install the Nortel server Subnet Interface card driver, and follow the previous step to install the Nortel server Subnet Interface card.
- 6 In the Network Protocol dialog box, only select **TCP/IP** protocol, and then click **Next** to continue.
- 7 In the Network Services dialog box, you see the following services:
 - RPC configuration
 - NetBIOS Interface
 - Workstation
 - server

Click to select the desired services.
- 8 Click **Next** to install selected components.
- 9 Click **OK** for Adapter Properties.
- 10 If the ELAN subnet card is the same type as the previously installed Nortel server Subnet Interface card, the following message can appear: "A network card of this type is already installed in the system. Do you want to continue?" Select **OK**.
- 11 The Adapter Properties dialog box appears for the second LAN card. Click **OK** to continue.

—End—

Configuring TCP/IP

"Typical configurations" (page 277) in Appendix A for information about different network configurations that are possible with Telephony Manager 3.1.

Procedure 71

Configuring TCP/IP settings on a Windows server

Step	Action
------	--------

- | | |
|---|---|
| 1 | Choose Start > Settings > Network and Dialup Connections . |
|---|---|

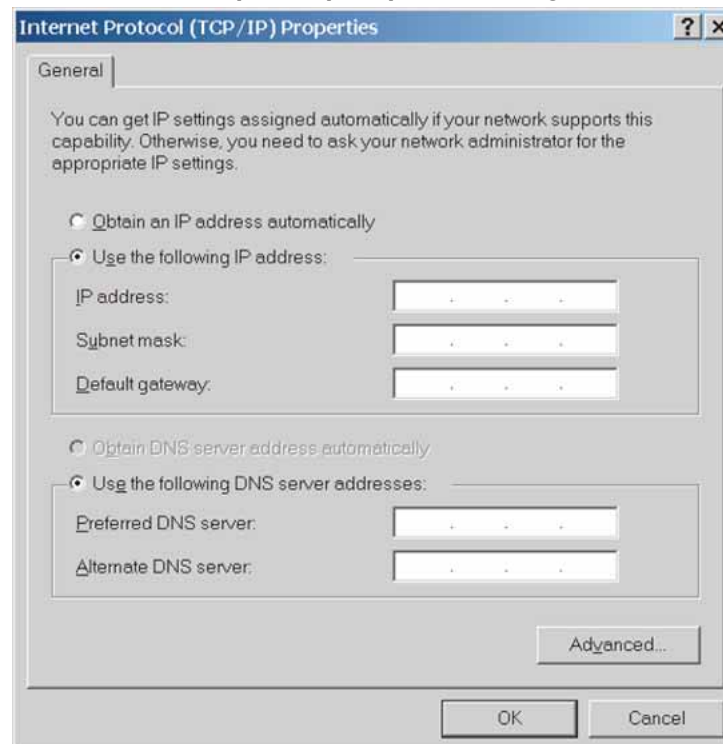
- 2 In the Network and Dialup Connections dialog box, right-click the Local Area Connection icon, and then select Properties.
- 3 In the Local Area Connection Properties dialog box, click to select Internet Protocol (TCP/IP), and then click **Properties**.

The Internet Protocol (TCP/IP) Properties dialog box appears. See [Figure 145 "Internet Protocol \(TCP/IP\) Properties dialog box"](#) (page 248).

ATTENTION

Ensure that the DHCP IP address is a static address as the host name and IP address are used for client licensing. If the client's IP address changes, the client is not able to log on until the licence file is adjusted.

Figure 145
Internet Protocol (TCP/IP) Properties dialog box



- 4 If you have a DHCP server and you want to configure the IP address from the DHCP server, select the Use the following IP address radio button. Enter the IP address, Subnet Mask, Default gateway, and DNS server information.

For PCs with two adapters, only one default gateway is required.

To enter WINS server information, click **Advanced** in the Internet Protocol (TCP/IP) Properties dialog box.

Click **OK**.

- 5 Reboot the system.

—End—

Configuring second adapter in a Dual Network Interface arrangement

The Telephony Manager 3.1 server (or client) can have a second network interface card (NIC) installed to connect to the ELAN subnet of a managed system. This can result in the multicast traffic sent on the ELAN rather than on the intended Nortel server Subnet (formerly referred to as the CLAN). The ELAN subnet must be protected from such traffic.

To prevent this type of multicast traffic, the metric value of the ELAN network interface card must be modified so that it is greater than that of the network interface card connecting to the Nortel server Subnet. This causes the server to prefer the Nortel server Subnet network interface for multicast traffic, rather than the ELAN network interface.

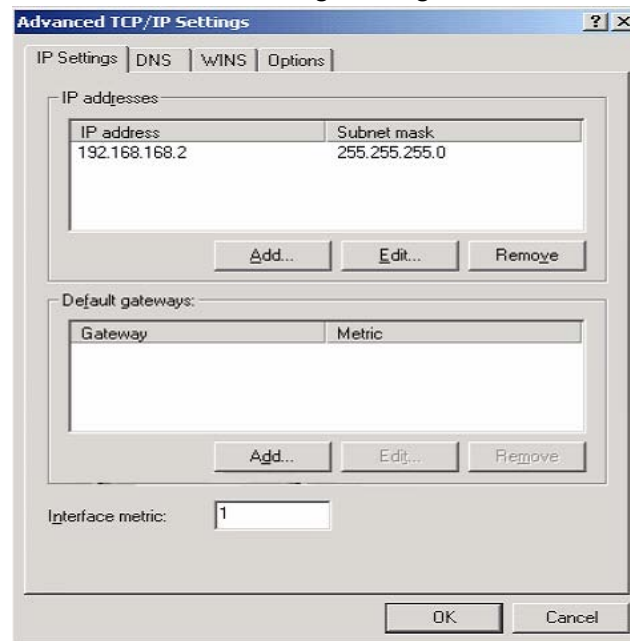
The binding order of the network interfaces is also important; the Nortel server Subnet network interface is first in the binding order. Network services not used on the ELAN subnet are disabled as well.

Procedure 72

Configuring Telephony Manager 3.1 Dual Network Interface

Step	Action
1	Right- click on My Network Places , and select Properties .
2	Right- click on the ELAN network interface card, and select Properties . Ensure that the Client for Microsoft Networks and File and Printer Sharing for Microsoft Networks check boxes are selected. If not, then clear and save the changes.
3	Select Internet Protocol (TCP/IP) and then click Properties . The IP Address and Subnet mask is set. The Default gateway field must be left empty to avoid transmission of unintentional traffic on the ELAN subnet.
4	Click Advanced . The Advanced TCP/IP Settings dialog box appears. See Figure 146 "Advanced TCP/IP Settings dialog box" (page 250) .

Figure 146
Advanced TCP/IP Settings dialog box



- 5 In the **IP Settings** tab, modify the **Interface Metric** value to a value greater than that of the Nortel server Subnet network interface. Click **OK** to save all changes.
- 6 Alter the binding order of the Nortel server Subnet network interface to a number-one position by completing the following procedure:
 - a. Select **Start > Settings > Control Panel**.
 - b. Double-click **Network and Dial-up Connections**.
 - c. On the Advanced menu, click **Advanced Settings**. The Connections box appears the network adapters.
 - d. Select the Nortel server Subnet network interface adapter.
 - e. Use the arrows on the right side of the box to move the adapter ahead (higher than) of the ELAN network interface adapter (if necessary), and then click **OK**.
 - f. If you are prompted to restart the computer, click **Yes**.
- 7 Ensure that all changes are saved and the server restarted. When the server restarts, check that all settings are applied. Launch a command prompt window and check the routing table using the **route print** command. The interface metric value has changed.

—End—

Installing a modem

Procedure 73

Installing a modem on a Windows server

Step	Action
1	Choose Start > Settings > Control Panel .
2	Double-click the Phone and Modem Options icon.
3	In the Phone and Modem Options dialog box, click the Modems tab.
4	If the modem on the computer is not already installed, click Add . If the modem is attached to the computer, Windows can detect and install a modem automatically.
5	In the Install New Modem dialog box, click Next to continue.
6	If the system is unable to detect the modem, you must insert the modem manufacturer's disk that came with the modem, and then select Have disk to install.
7	If the system does not have a modem attached, select Standard 28800 bps Modem from the list.
8	Click Finish to close the dialog box.

—End—

Installing Remote Access Service

Procedure 74

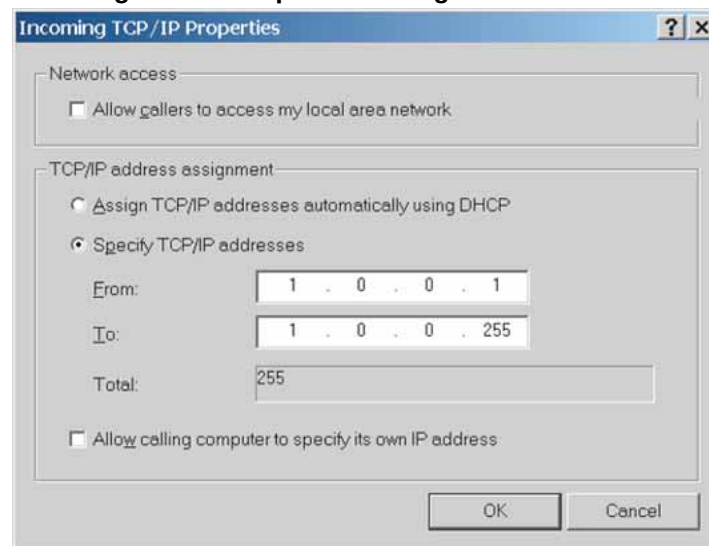
Installing Remote Access Service (RAS) on a Windows server

Step	Action
1	Choose Start > Settings > Network and Dialup Connections .
2	Double-click the Make New Connection icon.
3	In the Network Connection Wizard welcome dialog box, click Next .
4	In the Network Connection Type dialog box, select Accept incoming connections , and then click Next .

- 5 In the **Devices for Incoming Connections** dialog box, select the appropriate connection device, and then click **Next**.
- 6 In the **Incoming Virtual Private Connection** dialog box, select **Do not allow virtual private connections** check box, and then click **Next**.
- 7 In the **Allowed Users** dialog box, select the users that are allowed to connect to the server, and then click **Next**.
- 8 In the Networking Components dialog box, select **Internet Protocol (TCP/IP)**, and then click **Properties**.

The Incoming TCP/IP Properties dialog box appears. See [Figure 147 "Incoming TCP/IP Properties dialog box"](#) (page 252).

Figure 147
Incoming TCP/IP Properties dialog box



- 9 In the **Incoming TCP/IP Properties** dialog box, clear the **Allow callers to access my local area network** check box. Click the Specify TCP/IP address radio button. Enter the initial range as From 1 . 0 . 0 . 1 to 1 . 0 . 0 . 255, and then click **OK**.
- 10 In the Networking Components dialog box, click **Next**.
- 11 In the Completing the Network Connection Wizard dialog box, type the connection name, and then click **Finish**.

—End—

Testing network cards

Test the network cards after you complete the Windows server installation.

Testing the Nortel server subnet interface

Procedure 75

Testing the Nortel server subnet interface

Step	Action
1	Network connectivity can be verified by pinging a server or workstation known to be accessible only through the Nortel server subnet. This could be an Telephony Manager 3.1 Web client or other server. From Command Prompt window on the Telephony Manager 3.1 server, enter the command ping <IP address> .

—End—

Testing the Embedded LAN interface

Procedure 76

Testing the Embedded LAN interface

Step	Action
1	Network connectivity can be verified by pinging a system on the ELAN. This could be the ELAN Network interface IP address of a Call Server, for example: From a Command Prompt window on the Telephony Manager 3.1 server, enter the command ping <IP address> .

—End—

Setting up Metabase Editor utility

Contents

This chapter contains information about the following topics:

["Overview" \(page 255\)](#)

["Setting up the Metabase Editor utility" \(page 255\)](#)

Overview

The metabase editor utility is only required when working with a Windows XP operating system.

To modify the ASP session timeout value in Windows XP, you must update the IIS metadatabase directly. Use an application provided by Microsoft called the Metabase Editor to view or edit the Metabase.bin file in C:\Windows\system32\inetsrv. This file has the hierarchical configuration information and schema that are used to configure IIS. The IIS configuration of folders in the Default Web Site are stored in the Metabase.bin.

Setting up the Metabase Editor utility

The following procedure sets up the Metabase Editor utility.

Procedure 77

Setting up the Metabase Editor utility

Step	Action
1	Launch the utility Metabase Editor .
2	Open Metabase.bin and go to LM > W3SVC > 1 > Roots . This path has the folders used in Telephony Manager. See
3	Change the value of Session Timeout to 90-120 minutes, depending on the requirement. On the right side, there is a Session Timeout value, configured as ASPSessionTimeout .

- 4 The **Session Timeout value** must be entered in all other folders with **ASPSessionTimeout** as a parameter.
- 5 Select **Administrative Tools > IIS > Default Website > Properties**.
- 6 Select **HomeDirectory Tab > Configuration**.
- 7 Select **Options Tab** and change the **SessionTimeout** value to 90-120 minutes, the same as that selected in step 3.
- 8 Save the changes.
- 9 Open the **Web.xml file** of Tomcat in the path **<TM installed path>\Tomcat\conf\Web.xml** and change the **SessionTimeout** value to that which was entered in the Metabase.bin.
- 10 Save the changes
- 11 Restart the computer.

—End—

Appendix A

Telephony Manager 3.1 engineering guidelines

Contents

This appendix contains information about the following topics:

"Overview" (page 257)

"Capacity factors" (page 258)

"Hardware and software comparisons" (page 259)

"Software limits" (page 260)

"PC hardware" (page 274)

"Network bandwidth" (page 277)

"Telephony Manager 3.1 system performance" (page 285)

"Telephony Manager 3.1 port usage" (page 291)

"FTP Server configuration" (page 295)

Overview

This appendix provides a set of guidelines to help you determine the configuration and distribution of Telephony Manager 3.1 servers within a network to efficiently manage Communication Server 1000 and Meridian 1 systems.

Capacity factors

This appendix examines the following areas where capacity is a factor:

- Features running on the Telephony Manager 3.1 server and their impact to its resources, such as CPU usage, physical memory (RAM), and disk storage
- Web and Telephony Manager 3.1 clients and their impact on Telephony Manager 3.1 server resources
- Communication Server 1000 and Meridian 1 systems and their impact on Telephony Manager 3.1 server resources
- Communications between the Telephony Manager 3.1 server and Communication Server 1000 and Meridian 1 systems, Telephony Manager 3.1/Web clients, and so on, and their impact on the network to which they are connected.

The Billing applications result in a processor load that is not possible to predict. The exact impact depends on several factors, including types of reports generated and quantity of data merged. It is not possible to derive a general formula to predict the impact of these applications. Nortel recommends that these applications be run during off-hours, and that they not be run in parallel with other resource-intensive applications.

Impact analysis

Analysis was performed on the majority of Telephony Manager 3.1 features. To simplify analysis, only those features that impact these resources are highlighted here.

Based upon this analysis, recommendations are made as to:

- The resources required on the Telephony Manager 3.1 server
- The number of clients and systems that can be connected to a single Telephony Manager 3.1 server
- Network bandwidth and routing considerations

[Table 17 "Network bandwidth usage per system" \(page 283\)](#) and [Figure 153 "Response Time versus Round Trip Time" \(page 286\)](#) show an analysis of the results of benchmark testing, which can be used to calculate the resources and connections possible for various Telephony Manager 3.1 server usage scenarios.

- [Table 17 "Network bandwidth usage per system" \(page 283\)](#) highlights the peak and average transfer rates for various Telephony Manager 3.1 activities.
- [Figure 153 "Response Time versus Round Trip Time" \(page 286\)](#) presents a graphical representation of station response time compared with round-trip time (RTT).

To aid in this process, this appendix analyzes four typical Telephony Manager 3.1 server configurations. Use these configurations as examples and the raw table data to extrapolate configurations specific to a given customer or distributor setup.

These guidelines provide minimum PC configurations for the Telephony Manager 3.1 server, Telephony Manager 3.1 client, Web client, and Telephony Manager 3.1 running in a stand-alone mode.

Hardware and software comparisons

Table 13 "Hardware Machine Type with CS 1000 Release 5.0" (page 259) shows a list of machine types for Meridian 1 with CS 1000 Release 5.0.

Table 13
Hardware Machine Type with CS 1000 Release 5.0

Hardware with CS 1000 Release 5.0	When Signaling server check box in Network page is cleared		When Signaling server check box in Network page is selected	
	System type	Machine type	System type	Machine type
11C/Mini	Meridian1	11C/11C Mini	Communication server 1000	CS 1000S Small System
51C 060	Meridian1	51C 060	Communication server 1000	CS 1000M Half Group 060
51C 060E	Meridian1	51C 060E	Communication server 1000	CS 1000M Half Group 060E
61C 060E	Meridian1	61C 060	Communication server 1000	CS 1000M Single Group 060
61C 060E	Meridian1	61C 060E	Communication server 1000	CS 1000M Single Group 060E
61C PII	Meridian1	61C PII	Communication server 1000	CS 1000M Single Group PII
61C CPPIV	Meridian1	61C CPPIV	Communication server 1000	CS 1000M Single Group CPPIV
81, 81C 060	Meridian1	81, 81C 060	Communication server 1000	CS 1000M/E Multi Group 060
81, 81C 060E	Meridian1	81, 81C 060E	Communication server 1000	CS 1000M/E Multi Group 060E
81C PII	Meridian1	81C PII	Communication server 1000	CS 1000M/E Multi Group PII
81C CPPIV	Meridian1	81C CPPIV	Communication server 1000	CS 1000M/E Multi Group CPPIV

Software limits

Coresidency support

Table 14 "Coresidency support" (page 260) shows the current list of available coresidency support for Telephony Manager 3.1.

Table 14
Coresidency support

Operating system	Browser	Office components	Telephony Manager 3.1 installed	Other coresident applications
Windows XP Professional	IE 6 English	- Excel 2003 - Word 2003 (from Office XP) in English	3.1 English client or standalone	- Enterprise Subscriber Manager (ESM) 1.1 - Common Network Directory (CND) 2.1 - Enterprise Network Management System (ENMS) 10.4 Client - CallPilot 4.0/5.0 Application Builder - Contact Center Manager Administration 6.0 client - Remote Gateway 9100 series Configuration Mgr (previously known as Remote Office) 1.5.2, 1.6.0, 1.7 - PCAnywhere 11.5 - Timbuktu Pro 7, 8 - WebEx 2.4.1 - Norton Antivirus (standard and professional) 2006 - McAfee VirusScan 9.0 - NetIQ Agent 6.0 SP2 - Concord Edge Agent 5.7

Operating system	Browser	Office components	Telephony Manager 3.1 installed	Other coresident applications
Windows 2000 Professional	IE 6 English	• Excel 2003 • Word 2003 (from Office XP) in English	3.1 English client or standalone	• ENMS 10.4 • CallPilot 4.0/5.0 Application Builder • Contact Center Manager Administration 6.0 client • Remote Gateway 9100 series Configuration Mgr (previously known as Remote Office) 1.5.2, 1.6.0, 1.7 • PC Anywhere 11.5 • Timbuktu Pro 7, 8 • WebEx 2.4.1 • Norton Antivirus (standard & professional) 2006 • McAfee VirusScan 9.0 • NetIQ Agent 6.0 SP2 • Concord Edge Agent 5.7
Windows Server 2003	IE 6 or IE 7	• Excel 2003 • Word 2003 (from Office XP) in English	3.1 English client or standalone	• ESM 1.1 • CND 2.1 • PCAnywhere 11.5 • WebEx 2.4.1 • Norton Antivirus (standard and professional) 2006 • McAfee VirusScan Enterprise 8.0i • NetIQ Agent 6.0 SP2
Windows 2000 Server	IE 6 English	• Excel 2003 • Word 2003 (from Office XP) in English	3.1 English server installation	• CND 2.1 • PCAnywhere 11.5 • WebEx 2.4.1 • Norton Antivirus (standard and professional) 2006 • McAfee VirusScan Enterprise 8.0i • NetIQ Agent 6.0 SP2

Operating system	Browser	Office components	Telephony Manager 3.1 installed	Other coresident applications
Windows 2000 Professional in French	IE 6 French	• Excel 2003 • Word 2003 (from Office XP) in French	3.1 French client or standalone	• ENMS 10.4 • CallPilot 4.0/5.0 Application Builder • Contact Center Manager Administration 6.0 client • Remote Gateway 9100 series Configuration Mgr (previously known as Remote Office) 1.5.2, 1.6.0, 1.7 • PC Anywhere 11.5 • Timbuktu Pro 7, 8 • WebEx 2.4.1 • Norton Antivirus (standard & professional) 2006 • McAfee VirusScan 9.0 • NetIQ Agent 6.0 SP2 • Concord Edge Agent 5.7
Windows 2000 Professional in German	IE 6 German	• Excel 2003 • Word 2003 (from Office XP) in German	3.1 German client or standalone	• ENMS 10.4 • CallPilot 4.0/5.0 Application Builder • Contact Center Manager Administration 6.0 client • Remote Gateway 9100 series Configuration Mgr (previously known as Remote Office) 1.5.2, 1.6.0, 1.7 • PC Anywhere 11.5 • Timbuktu Pro 7, 8 • WebEx 2.4.1 • Norton Antivirus (standard & professional) 2006 • McAfee VirusScan 9.0 • NetIQ Agent 6.0 SP2 • Concord Edge Agent 5.7

Operating system	Browser	Office components	Telephony Manager 3.1 installed	Other coresident applications
Windows 2000 Professional in Japanese	IE 6 Japanese	• Excel 2003 • Word 2003 (from Office XP) in Japanese	3.1 English client or standalone	• ENMS 10.4 • CallPilot 4.0/5.0 Application Builder • Contact Center Manager Administration 6.0 client • Remote Gateway 9100 series Configuration Mgr (previously known as Remote Office) 1.5.2, 1.6.0, 1.7 • PC Anywhere 11.5 • Timbuktu Pro 7, 8 • WebEx 2.4.1 • Norton Antivirus (standard & professional) 2006 • McAfee VirusScan 9.0 • NetIQ Agent 6.0 SP2 • Concord Edge Agent 5.7
Windows 2000 Professional in Simplified Chinese	IE 6 Simplified Chinese	• Excel 2003 • Word 2003 (from Office XP) in Simplified Chinese	3.1 English client or standalone	• ENMS 10.4 • CallPilot 4.0/5.0 Application Builder • Contact Center Manager Administration 6.0 client • Remote Gateway 9100 series Configuration Mgr (previously known as Remote Office) 1.5.2, 1.6.0, 1.7 • PC Anywhere 11.5 • Timbuktu Pro 7, 8 • WebEx 2.4.1 • Norton Antivirus (standard & professional) 2006 • McAfee VirusScan 9.0 • NetIQ Agent 6.0 SP2 • Concord Edge Agent 5.7

Operating system	Browser	Office components	Telephony Manager 3.1 installed	Other coresident applications
Windows 2000 Professional in Spanish	IE 6 Spanish	• Excel 2003 • Word 2003 (from Office XP) in Spanish	3.1 English client or standalone	• ENMS 10.4 • CallPilot 4.0/5.0 Application Builder • Contact Center Manager Administration 6.0 client • Remote Gateway 9100 series Configuration Mgr (previously known as Remote Office) 1.5.2, 1.6.0, 1.7 • PC Anywhere 11.5 • Timbuktu Pro 7, 8 • WebEx 2.4.1 • Norton Antivirus (standard & professional) 2006 • McAfee VirusScan 9.0 • NetIQ Agent 6.0 SP2 • Concord Edge Agent 5.7
Windows 2000 Professional in Brazilian-Portuguese	IE 6 Brazilian-Portuguese	• Excel 2003 • Word 2003 (from Office XP) in Brazilian-Portuguese	3.1 English client or standalone	• ENMS 10.4 • CallPilot 4.0/5.0 Application Builder • Contact Center Manager Administration 6.0 client • Remote Gateway 9100 series Configuration Mgr (previously known as Remote Office) 1.5.2, 1.6.0, 1.7 • PC Anywhere 11.5 • Timbuktu Pro 7, 8 • WebEx 2.4.1 • Norton Antivirus (standard & professional) 2006 • McAfee VirusScan 9.0 • NetIQ Agent 6.0 SP2 • Concord Edge Agent 5.7

Operating system	Browser	Office components	Telephony Manager 3.1 installed	Other coresident applications
Windows 2000 Server in Japanese	IE 6 Japanese	• Excel 2003 • Word 2003 (from Office XP) in Japanese	3.1 English server installation	• CND 2.1 • PCAnywhere 11.5 • Norton Antivirus (standard and professional) 2006 • McAfee VirusScan Enterprise 8.0i • NetIQ Agent 6.0 SP2
Windows Server 2003 in Japanese	IE 6 or IE 7 Japanese	• Excel 2003 • Word 2003 (from Office XP) in Japanese	3.1 English server installation	• ESM 1.1 • CND 2.1 • PCAnywhere 11.5 • Norton Antivirus (standard and professional) 2006 • McAfee VirusScan Enterprise 8.0i • NetIQ Agent 6.0 SP2
Windows 2000 Server in Simplified Chinese	IE 6 Simplified Chinese	• Excel 2003 • Word 2003 (from Office XP) in Simplified Chinese	3.1 English server installation	• CND 2.1 • PCAnywhere 11.5 • Norton Antivirus (standard and professional) 2006 • McAfee VirusScan Enterprise 8.0i • NetIQ Agent 6.0 SP2
Windows Server 2003 in Simplified Chinese	IE 6 or IE 7 Simplified Chinese	• Excel 2003 • Word 2003 (from Office XP) in Simplified Chinese	3.1 English server installation	• ESM 1.1 • CND 2.1 • PCAnywhere 11.5 • WebEx 2.4.1 • Norton Antivirus (standard and professional) 2006 • McAfee VirusScan Enterprise 8.0i • NetIQ Agent 6.0 SP2
Web clients:				

Operating system	Browser	Office components	Telephony Manager 3.1 installed	Other coresident applications
Any PC OS listed in above table that supports IE 6	IE 6	N/A	Telephony Manager 3.1 Web client (Administrator UI)	• CallPilot 4.0/5.0 Web client (Administrator CallPilot Web client) • Contact Center Manager Administration 6.0 client • BCM 3.6 & 3.7 Web Management Interface
Any PC OS listed in above table that supports IE 6	IE 6	N/A	Telephony Manager 3.1 Web client (Desktop UI)	• CallPilot 4.0/5.0 Web client (Administrator CallPilot Web client) • Contact Center Manager Administration 6.0 client • BCM 3.6 & 3.7 Web Management Interface

Supported versions of co-resident applications provides the supported versions of coresident applications.

ATTENTION

The sections OS and browser requirements, Third-party software requirements and Coresidency support list the baseline configuration that Nortel has tested and supports. Any deviation from the configurations has not been tested and is supported by Nortel only on a best-effort basis, unless otherwise indicated.

Hard-coded limits

This section lists the hard-coded limits in the Telephony Manager 3.1 software.

Table 15 "Telephony Manager 3.1 capacity parameters" (page 266) outlines the maximum value for many of the parameters associated with the various components of Telephony Manager 3.1.

Table 15
Telephony Manager 3.1 capacity parameters

Parameter	Maximum Value
Windows Common Services	
Maximum number of Sites that can be created on a Telephony Manager 3.1 server	3,000

Parameter	Maximum Value
Maximum number of MG 1000B systems can be created under a specific site	256
Maximum number of synchronization/Update tasks (number of Log Windows) that can be executed at the same time	5
Number of Customers	100
Range of DN	0-9,999,999
Maximum number of Survivable Expansion Cabinet	4
Maximum number of modem scripts that can be created	3,000
Windows Common Services	
Maximum number of application jobs that can be scheduled in the Scheduler application	2,000
Max String Length for:	
Site name	31
System name	31
Address	44
City	24
State/Province	24
Country	24
Zip/Postal Code	16
Comments	255
IP Address	15
Timeout	60
Phone Number	50
Modem Access ID	50
Modem Password	50
Modem Installation String	50
Issue	99
System ID	16
Maximum Speed Call Lists	8,191
Maximum ACD Agents	1,200
PDT password	16
Customer Name	31
Directory Numbers	24
Customer Password	16

Parameter	Maximum Value
HLOC	9,999
Dial Intercom Group	2,045
User ID	2,045
Corporate Directory	
Maximum number of reports that can be generated at the same time	1
Maximum string length of all parameters	255 characters
Maximum number of entries in Corporate Directory file uploaded to Large systems (for example, 61C)	120,000
Maximum number of entries in Corporate Directory file uploaded to Small systems (for example, CS 1000S)	16,000
Maximum number of entries in Corporate Directory file uploaded to Meridian 1 PBX 11C Chassis	2,000
Data Buffering and Access (DBA)	
Maximum number of Action records that can be defined in a DBA session	1,000
Maximum number of Rule records that can be defined in a DBA session	1,000
Maximum number of CDRs that can be collected	5,000,000
List Manager	
Maximum number of speed call lists that can be created	8,190
Maximum number of group call lists that can be created	63
Maximum number of group hunt lists that can be created.	8,190
Maximum String length for:	
Speed Call List	
List Name	50
Entry Name	50
Dialed Digits	31
Speed Call List	
Entry Number	999
PLDN	31
Group Call list:	

Parameter	Maximum Value
List Name	50
Entry Name	50
Entry Number	19
Group Hunt List:	
List Name	50
Maximum String length for:	
Group Hunt List:	
PLDN	50
Dialed Digits	31
Entry Name	50
Entry Number	95
Telephony Manager 3.1 DECT	
Maximum number of DECT Systems	500
Maximum String length for:	
DECT system name	255
Password	Unlimited
IP Address	15
Telephony Manager 3.1 server IP Interface	15
Phone Number	64
PARI (Access Right Identification tab)	8
SARI (Access Right Identification tab)	8
Upstream Manager IP address (Access Right Identification tab)	15
Web Maintenance	
Maximum number of maintenance commands that can be executed at the same time in Web Maintenance	10
Telephony Manager 3.1 Web	
Maximum supported number of clients that can log on to the Administration page of the same Telephony Manager 3.1 server at the same time	5
Maximum number of telephones that can be assigned to an end user	200
Data Buffering and Access (DBA)	
Maximum number of systems	256

Parameter	Maximum Value
Organizational Hierarchy	
Maximum number of organizational levels	20
Virtual Terminals	
Maximum number of Virtual Terminals that can be enabled at one time	256
Billing applications (TBS, CCCR, CRS, and GCAS)	
Maximum number of call records per costing configuration in TBS	2,500,000
Maximum number of call records for CCCR (across all systems)	5,000,000
Maximum number of call records for GCAS	4,000,000
Maximum number of call records for CRS (TBS & GCAS combined)	2,500,000
Maximum number of managed systems for TBS Billing General and TBS Billing Enhanced (TBS,CCCR,CRS, and GCAS)	10
Maximum number of lines in a PBX for TBS Billing General and TBS Billing Enhanced (TBS,CCCR,CRS, and GCAS)	3,500
Maximum number of Consolidated Multi-site Reports for TBS Billing General	0
Maximum number of Consolidated Multi-site Reports for TBS Billing Enhanced (TBS,CCCR,CRS, and GCAS)	5 (CCCR)
CCCR operates only within a single Telephony Manager server and can only be run on a Telephony Manager server or standalone system	
Alarm Management	
Maximum number of traps in the circular queue	1,360

Rate of alarm production

A single system produces alarms, on average, at the rate of one every ten seconds. This means the queue can hold 3.7 hours worth of alarms from a single system without losing alarm information.

Starting with Release 25 of Meridian 1 system software and in all releases of Communication server 1000 software, there is the capability of filtering traps, on the PBX, based upon their categorization (for example, minor, major, critical, and so on). This can greatly reduce the alarm rate by permitting only major and critical alarms to be sent to Telephony Manager 3.1.

Filtering increases the number of systems that can be connected. However, when a single system begins having a problem, it begins reporting major or critical alarms at the rate of 1 every 2 seconds. This means that the queue can hold only the last 45-minutes worth of alarms from the offending system, assuming that alarms from the other systems are minimal.

Billing applications sizing guidelines

The Telephony Manager 3.1 billing application is intended for use in small to medium sized customer networks. Telephony Manager 3.1 billing is most suitable for networks that do not require substantial data processing or those with many nodes.

There are two considerations for determining whether Telephony Manager 3.1 billing is suitable for a particular customer network. The first is the size of the largest system for which billing is used, and the other is the total number of systems in the network. [Table 15 "Telephony Manager 3.1 capacity parameters" \(page 266\)](#) for some practical guidelines on determining if the Telephony Manager 3.1 billing application meets your customer's requirements.

When CDR is collected and costed, the Telecom Billing System (TBS) generates a separate Microsoft Access database for each individual costing configuration (PBX system). Each PBX system defined in TBS has a capacity limit of 2.5 million costed call records which is a limitation of the Microsoft Access database used in the billing application. While TBS does not enforce a maximum number of systems that is supported, we recommend using the above guideline of 10 systems per Telephony Manager 3.1 server configuration to ensure that adequate resources are available. The size of the database determines how often call records are archived to ensure that there is adequate capacity to receive additional call records. However, the larger the database, the more often archiving is required to achieve the desired result. The recommended maximum of 3,500 lines per PBX is a conservative limit based upon the assumption that a PBX with 3,500 lines generates approximately 800,000 call records per month. This leads to an archival interval of 12.5 weeks and allows reporting on 3 months of calling activity within a single database. Note that call record generation varies depending upon how the switch is used, so having a good understanding of the customers call volume is highly recommended.

The sizing guidelines are provided to help ensure that Telephony Manager 3.1 performs optimally. Telephony Manager 3.1 billing still operates past these limitations, but with degraded performance. Performance concerns that arise from using Telephony Manager 3.1 past the recommended limitation is not considered a product deficiency.

ATTENTION

The time to cost CDR records and generate reports is directly proportional to the size of the call record database. For larger or busier switches, the response time for costing CDR and generating reports are slower than with a smaller switch that doesn't generate as many call records.

Operational limits**Telephony Manager 3.1 Web interface**

The Telephony Manager 3.1 Web interface provides the ability to access the Telephony Manager 3.1 server from any PC with a Web browser. Usage of the Telephony Manager 3.1 Web interface does not require installation of the Telephony Manager 3.1 client, however, using the Web interface places a heavier workload on the Telephony Manager 3.1 server as processing is concentrated at the Telephony Manager 3.1 server instead of distributed across the Telephony Manager 3.1 clients.

Telephone manager

Full station administration capability is available through telephone manager. A station change operation from the Web would include the following tasks:

- 2 seconds to find the telephone
- 6 seconds to display the details
- 5 seconds to validate and save
- 4 seconds to schedule transmission task
- 22 seconds for the actual transmission to the PBX

The times listed above measure the time lapse as experienced by the user. They do not represent the actual CPU time consumed on the server. Only the final task of transmitting to the PBX involves 100% of server time. Other tasks consist primarily of time spent rendering HTML on the client browser.

Web Desktop Services for end-users

When you configure the write capability for end users in Web Desktop Services, you also place a higher workload on the Telephony Manager 3.1 server.

However, the ability for end users to make changes may decrease the need for the network administrator to make changes; therefore, the impact of configuring the write capability for end-users in Web Desktop Services may not be significant in certain configurations.

Web support on server and Workstation platforms

Table 16 "Web support on servers and workstations" (page 273) outlines the differences observed in Web support when Telephony Manager 3.1 is running on server grade platforms and workstation platforms.

Table 16

Web support on servers and workstations

	IIS on Supported Windows OS
Concurrent Internet Explorer sessions	Only limited by Telephony Manager 3.1 capacity
Restricted Access by IP address and domain name	Yes

When additional clients attempt to access Web Services and there are no available connections, an error message appears. See Figure 148 "Too-many-users-are-connected error message" (page 273).

Figure 148

Too-many-users-are-connected error message



IIS support on the Telephony Manager server

To access Telephony Manager Web applications, IIS must be running on the Telephony Manager server. "IIS support on the Telephony Manager server" (page 273) depicts the versions of IIS supported on the OS platforms.

Operating system	Web server
Windows Server 2000	IIS 5.0

Windows XP Professional	IIS 5.1
Windows Server 2003	IIS 6.0

PC hardware

This section describes the PC hardware requirements necessary to run Telephony Manager 3.1 optimally. Use the guidelines provided in the sections ["Physical memory" \(page 274\)](#), ["Hard disk" \(page 275\)](#), and ["Processor speed" \(page 276\)](#):

See ["Telephony Manager 3.1 hardware requirements" \(page 33\)](#) for the following information:

- Add additional serial interface cards as needed.
- Calculate disk storage requirements based on applications usage.
- Implement a backup and restore strategy.
- Follow regular maintenance instructions as documented for Telephony Manager 3.1 features to maintain the integrity and capacity of the hard disk.
- Add disk redundancy as required.
- Increase performance by:
 - Adding more system memory
 - Utilizing a faster hard disk or SCSI interface, or both
 - Using a faster CPU
- Scale your PC for future growth, and utilize a PC that:
 - Has a reserve PCI Card slot for a SCSI Interface Card (See ["Hard disk" \(page 275\)](#) for details.)
 - Has a spare storage bay and power for adding an internal hard disk
 - Can accommodate increasing the memory capacity to 1 GB or greater (Most PCs have 2 to 4 memory card slots that can accommodate DIMMS of various capacity.)

Response-time testing is based upon the recommended configuration, not the minimum configuration. Response-time performance is only supported on the recommended configuration.

Physical memory

The amount of physical memory installed on the server is critical in achieving maximum performance on the PC. Microsoft Windows systems have a feature called Virtual Memory. Virtual Memory allows the PC to continue running programs that require more memory than there is physical

memory available. It borrows memory using a memory-swapping scheme from available space on the main hard disk. Although this feature permits the PC to perform operations without worrying about running out of physical memory and, thus, crashing the computer, it sacrifices performance of these operations by requiring access of the hard disk while memory swapping. This degrades performance because:

- Physical memory access is much faster than disk access.
- Accessing the disk while memory swapping steals disk resources away from applications that need to read and write to the hard disk.

Hard disk

Disk performance

Much of the time spent by Telephony Manager 3.1 Features is in reading and writing data to the hard disk. Features that spend a significant percentage of their time accessing the disk are called disk-intensive applications. For these features, the access time is critical in terms of the time it takes for a feature to complete an operation.

Telephony Manager 3.1 disk-intensive applications analyzed in this document include:

- CDR and traffic collection
- TBS report generation
- Simultaneous Update of Station Data

Station Update from a single system is not affected by disk performance, as the speed of transmission from the system is slower than the PC accessing its disk.

- telephone manager Access

"Physical memory" (page 274) recommends a hard disk using the ATAPI interface. It also recommends a single hard disk.

To improve performance you can:

- Use the fastest Ultra-Wide SCSI Interface (15K RPM).

Disk performance increases by a factor of 2 or better. This can translate to an increase in feature performance (reduce elapsed time and increase simultaneous operations) by 50 percent or better.

SCSI disk drives come in various speeds.

- Add a hard disk to store Telephony Manager 3.1 Data separate from the OS and Programs.

If the server PC used is using an ATAPI interface for its main disk, C:, then installing a SCSI interface card and second hard disk to store

Telephony Manager 3.1 Data can achieve the majority of the SCSI performance increase.

Disk size

The Telephony Manager 3.1 server (standalone) software with default installation (software and English WebHelp) requires approximately 700 MB of disk space (without any systems configured).

The minimum required server memory is 512 MB. Each Telephony Manager 3.1 client connection to the Telephony Manager 3.1 server requires an additional 3 MB of memory.

You must reserve approximately 300 MB of disk space for virtual memory and normal OS operations.

Each CDR record needs 250 bytes of disk space, At peak rates over a one-day period, this creates a 700 MB file.

Telephone manager requires approximately 14 GB per 100,000 telephones. This does not include the disk space requirements for records in the Common Network Directory (CND). If CND coresides with Telephony Manager on the same PC, add the space requirements for CND. For more information, see *Common Network Directory 2.1 Administration Guide (NN43050-101)*.

Processor speed

An increase in CPU power does not, by itself, greatly increase the capacity of the server.

The PC is so I/O bound, from accessing memory to accessing the hard disk, that a two-fold increase in CPU power may result in only a 10 percent increase in Telephony Manager 3.1 capacity.

Replacement of the motherboard, not just the CPU chip, can further increase CPU performance, Because the newer motherboard is designed to take advantage of the high processor speeds (for example, faster CPU bus, faster memory, and so on). The PC is still heavily bound to disk access and network speeds.

Network bandwidth

Typical configurations

Telephony Manager 3.1 interface access

While the connection from Telephony Manager 3.1 to the managed systems may be either serial or an IP connection, the Telephony Manager 3.1 applications may be accessed by a variety of means:

- The Windows GUI and Web interfaces can be used directly on the Telephony Manager 3.1 server.
- Remote users can dial up to the Telephony Manager 3.1 server and use CLI to access the Communication server 1000 and Meridian 1 systems.
- Telephony Manager 3.1 Web clients can also be used to connect to the Telephony Manager 3.1 server.
- For full access to Telephony Manager 3.1 features, the Telephony Manager 3.1 client GUI interface can be used.
- Connect to the Telephony Manager 3.1 server/client using a supported remote access software package (for example, pcAnywhere). This is particularly useful if Telephony Manager 3.1 clients cannot be deployed remotely due to bandwidth limitations.

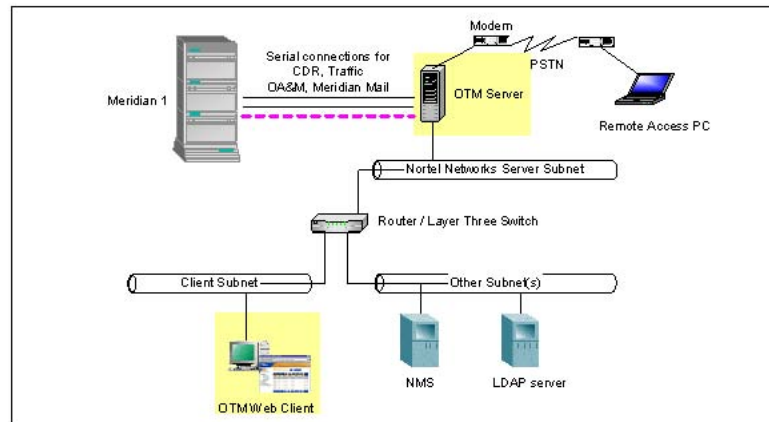
Serial connections to systems

[Figure 149 "Connecting Telephony Manager 3.1 to legacy systems \(pre-Ethernet\)" \(page 278\)](#) shows how Telephony Manager 3.1 connects to systems that do not support Ethernet. In this scenario, Telephony Manager 3.1 is connected to these systems through their serial ports. Physical limitations on serial connections limit Telephony Manager 3.1 to be placed within 15.24 meters (50 feet) of these systems to minimize noise, which can cause transmission errors. It is also possible for the serial connection to be established over a modem connection. Note that some Telephony Manager 3.1 applications cannot work over a serial connection. For more information, see [Table 9 "CS 1000 and Meridian 1 software requirements" \(page 41\)](#).

The diagram only shows the Telephony Manager 3.1 server, but it is possible for a Telephony Manager 3.1 client to be used. The Telephony Manager 3.1 client requires the same serial connections to the managed systems as the Telephony Manager 3.1 server. The usual limitations of the Telephony Manager 3.1 client apply, such as the need for a high bandwidth connection between the Telephony Manager 3.1 client and the Telephony Manager 3.1 server.

It is possible for the same Telephony Manager 3.1 PC to have serial connections to some systems and IP connections to others.

Figure 149
Connecting Telephony Manager 3.1 to legacy systems (pre-Ethernet)



IP connections to systems

IP connection overview

The Telephony Manager 3.1 solution consists of the Telephony Manager 3.1 server, Telephony Manager 3.1 clients, and Telephony Manager 3.1 Web clients. These may be connected in several different configurations. The particular configuration chosen depends on the tasks to be performed and the network environment.

The following are some of the considerations when deciding on the configuration:

- Are there multiple administrators? Do they require full administration capabilities available with Telephony Manager 3.1 clients, or is Web client functionality sufficient? The answers to these questions determine the need for Telephony Manager 3.1 clients.
- The Telephony Manager 3.1 clients connection to the Telephony Manager 3.1 server must have high bandwidth and low Round Trip Time (RTT) characteristics, as documented in the "[Telephony Manager 3.1 server and client overview](#)" (page 61) and, in this appendix, "[Network bandwidth](#)" (page 277). Because a WAN connection is not generally suitable this affects the placement of Telephony Manager 3.1 clients.
- The Telephony Manager 3.1 clients require connections to the systems they are managing.
- The Telephony Manager 3.1 server requires connections to the systems if the Web client is used or if applications are run on the Telephony Manager 3.1 server (for example, DBA collection of CDR, Station administration by the server Windows GUI interface). Note that if Telephony Manager 3.1 clients are used, the connection to the systems

is directly from the Telephony Manager 3.1 clients, not through the Telephony Manager 3.1 server.

- The number of systems administered by Telephony Manager 3.1, and what network connectivity is available to these systems. A key point is that a high quality connection is required between the Telephony Manager 3.1 server and Telephony Manager 3.1 clients. On the other hand, the connection between the Telephony Manager 3.1 server and Web clients or between the Telephony Manager 3.1 server and managed systems requires significantly lower bandwidth, and most WAN connections should be adequate.

Data networking guidelines

The Data Networking NTP *Data Networking for Voice over IP (553-3001-160)* gives an overview of all network connections, together with guidelines for their usage. It is important to understand and follow the recommendations in it. Only a few key points are mentioned here and the Data Networking NTP should be consulted for details.

- If it is planned to connect the ELAN subnet to the enterprise IP network, a layer three switch or router capable of packet filtering **MUST** be used to separate the ELAN subnet from the enterprise IP network. The packet filter **MUST** be configured to prevent broadcast, multicast and unauthorized traffic from entering the ELAN subnet.
- If the ELAN subnet is connected to the enterprise IP network without a packet filtering router, the system's call handling ability may be adversely affected. It is recommended to use a layer two or layer three Ethernet switch for all subnets. This is particularly important on the ELAN subnet when other application servers (for example, SCCS) are present. The use of shared media hubs can result in adverse system impact under some conditions.

ELAN connection options

The Telephony Manager 3.1 server and Telephony Manager 3.1 client require connectivity to the ELAN subnets of the managed systems. There are two choices for this ELAN configuration:

- The Telephony Manager 3.1 server or client is connected only to the Nortel server subnet (or another subnet of the customer's Enterprise IP network) and has a routed connection to the ELAN subnets of managed systems. This is the more flexible and preferred configuration.
- The Telephony Manager 3.1 server or client has a network interface that connects directly to the ELAN subnet. A second network interface is also present to connect to the Nortel server subnet. This is referred to as a Dual NIC configuration. Such a setup is suitable if there is only one Telephony Manager 3.1 PC (for example, server but no Telephony

Manager 3.1 clients) that requires access to the ELAN subnet. Note that if multiple systems are managed, the ELAN Network interface on the Telephony Manager 3.1 server or Telephony Manager 3.1 client only allows access to a single ELAN subnet, and the other ELAN subnets have to be accessed by a routed connection from the Nortel server subnet.

Telephony Manager 3.1 clients that also serve as desktop PCs generally have a routed connection to the ELAN subnets of the managed systems because they are located on the client subnet.

In making the decision regarding which configuration to choose, a factor is whether a routed connection to the ELAN subnet is required for other purposes (for example, the CS 1000 Call Servers send traps directly to an NMS).

ELAN and Nortel server subnet connectivity requirements

Connectivity from the Telephony Manager 3.1 server or client to the ELAN is required for the following operations:

- All system management, configuration, and maintenance of Meridian 1 and CS 1000 devices. Several protocols may be used (for example, Rlogon, SNMP).
- Access is required from the Telephony Manager 3.1 server/client to the signaling server and Voice Gateway Media Card ELAN interfaces (for example, to pull OM reports for IP Telephony).
- Access from the Telephony Manager 3.1 client or Web client for Element Manager access when launched from the Telephony Manager 3.1 Navigator.

Connectivity from the Telephony Manager 3.1 server or client to the Nortel server subnet is required for the following operations:

- If an ELAN Network interface is not present to the ELAN subnet of any managed system, a routed connection is required from the Nortel server subnet interface to the ELAN subnet.
- Telephony Manager 3.1 client access to the Telephony Manager 3.1 server. Due to the high bandwidth requirements of this connection it is important that the Telephony Manager 3.1 client to Telephony Manager 3.1 server connection not be made through the ELAN subnet.
- Web client access to the Telephony Manager 3.1 server.
- Access by a remote access software package (for example, pcAnywhere).
- CND synchronization with the customer CND server.

- Forwarding of SNMP traps to a NMS (could be just Telephony Manager 3.1 traps or notification traps for managed systems events).

Telephony Manager 3.1 network configuration scenarios

The following are some typical Telephony Manager 3.1 configuration scenarios:

Standalone Telephony Manager 3.1 server This is the simplest configuration, consisting of an Telephony Manager 3.1 server with no Telephony Manager 3.1 clients. There may be optional Web clients. There are two possible setups:

- The server has the Dual NIC configuration, with a dedicated ELAN subnet network interface. Generally only a standalone Telephony Manager 3.1 server that is managing a single system is set up with an ELAN Network interface. [Figure 150 "Standalone Telephony Manager 3.1 server with Dual NIC configuration" \(page 281\)](#) illustrates this configuration.
- Routed connections are used from the Telephony Manager 3.1 server to the ELAN subnets of managed systems (through the Nortel server subnet). This configuration is preferred over the Dual NIC configuration. [Figure 151 "Standalone Telephony Manager 3.1 server with routed connections" \(page 282\)](#) illustrates this configuration.

Figure 150
Standalone Telephony Manager 3.1 server with Dual NIC configuration

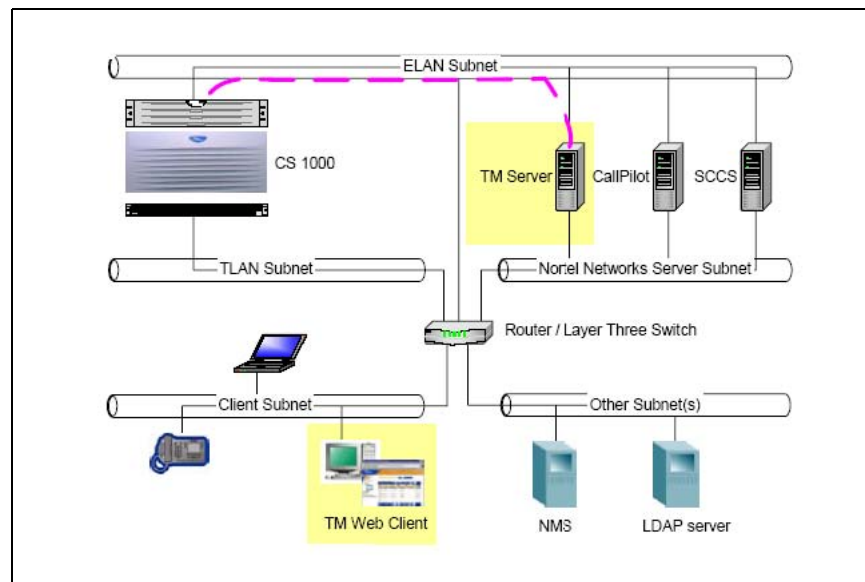
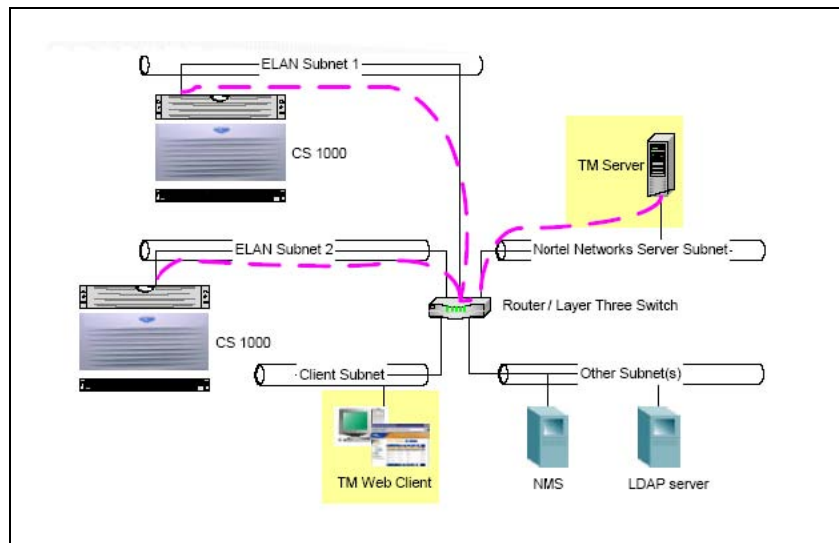


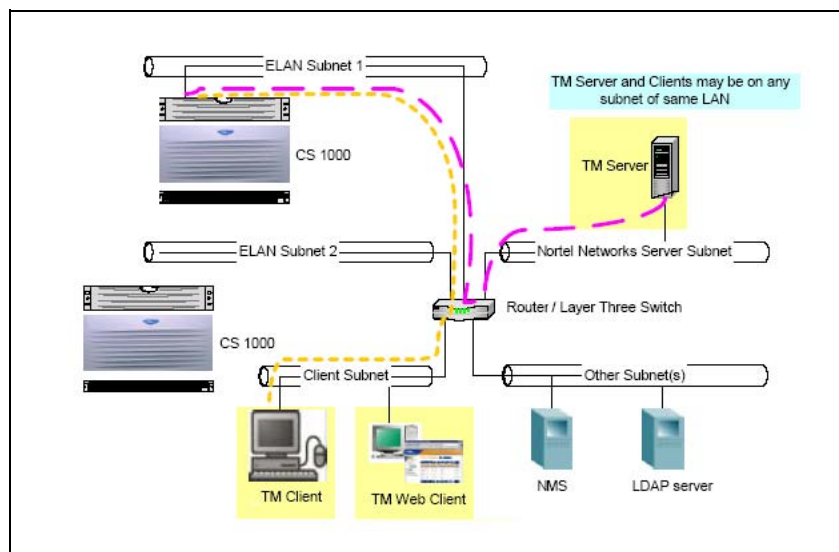
Figure 151
Standalone Telephony Manager 3.1 server with routed connections



Telephony Manager 3.1 server with Telephony Manager 3.1 clients

In this configuration the Telephony Manager 3.1 server is connected to a number of Telephony Manager 3.1 clients, all on the same LAN (due to bandwidth and other restrictions). There may be optional Web clients. Here, routed connections are used from the Telephony Manager 3.1 server/clients to the ELAN subnets of managed systems (through the Nortel server subnet). Figure 152 "Telephony Manager 3.1 server with Telephony Manager 3.1 clients" (page 282) illustrates this configuration.

Figure 152
Telephony Manager 3.1 server with Telephony Manager 3.1 clients



Because Telephony Manager 3.1 clients cannot be connected to the Telephony Manager 3.1 server across a WAN, to get full GUI capabilities across a WAN, Nortel recommends that pcAnywhere be used to connect to the Telephony Manager 3.1 server or Telephony Manager 3.1 clients.

VPN connections Telephony Manager 3.1 does not have any special support for Virtual Private Network (VPN) connections. It is possible for Telephony Manager 3.1 to use a VPN connection as long as this is transparent to the Telephony Manager 3.1 application. One example would be for a remote user to use the Telephony Manager 3.1 Web client using a VPN connection over the Internet into the customer Enterprise IP network to access the Telephony Manager 3.1 server.

Bandwidth utilization

The trade-off is the cost of Telephony Manager 3.1 versus the cost of increased network bandwidth or network subnets. When Telephony Manager 3.1 servers are attached to the WAN, the customer's network may be impacted, but there is a saving on the number of Telephony Manager 3.1 servers needed.

Never expect to fully utilize Ethernet bandwidth. Performance degrades quickly as the utilization exceeds a certain threshold (approximately 35 percent). Consult the network administrator for details on network bandwidth utilization.

Table 17 "Network bandwidth usage per system" (page 283) lists the average and peak traffic for the ELAN subnet and Nortel server subnet. This is based upon traffic analysis of a system running on a CP4 CPU. For a Cabinet system, divide the ELAN subnet numbers by 2, except for alarms. For the CPP CPU, multiply the ELAN subnet numbers by 4, except for alarms.

Table 17
Network bandwidth usage per system

Telephony Manager 3.1 Activity	Transfer rate (bits/second)	
	Average	Peak
Station Add/Chg/Del, Nortel server subnet	32 KB	32 KB
Station Sync with PBX, ELAN subnet	NA	48 KB
CDR, ELAN subnet	35 KB	70 KB
Traffic, ELAN subnet	24 KB	48 KB
Alarm, ELAN subnet	1 KB	3 KB
Total, ELAN subnet	~92 KB	~129 KB
Total, Nortel server subnet		~32 KB

Alarm Processing

There are Telephony Manager 3.1 alarms and IP Line managed system alarms.

Telephony Manager 3.1 alarm details The Telephony Manager 3.1 Trap server can handle 25–50 incoming SNMP traps per second. However, this limitation varies considerably with network load, PC processing power, and CPU availability.

Traps are stored in a circular queue of 1360 traps. You can view the queue using the Web Alarm Browser. If the rate of trap arrival is heavy, some traps are not entered into the queue even though they are received by the Trap server and Alarm Notification application. The circular queue can handle an incoming rate of 50 traps in 10 seconds without any loss of information.

An SNMP trap has an average size of approximately 400 bytes. You can use this information to approximate the bandwidth requirements for trap processing. For example, 1000 devices, each producing one trap every 10 seconds, would require a bandwidth of 320 Kbps:

$$400 \text{ bytes/trap} * 8 \text{ bits/byte} * 1000 \text{ devices} * 0.1 \text{ trap/sec/device} = 320 \text{ Kbps}$$

IP Line/IP Trunk /Switch alarm details Under normal conditions, a system generates one trap approximately every ten seconds. Beginning with X11 Release 25, you can use filtering on the system to reduce the output of traps. However, there is no filtering capability on IP Line/IP Trunk. IP Line/IP Trunk does not generate traps under normal operating conditions. In an abnormal situation, IP Line/IP Trunk could be expected to generate an alarm every 5 seconds.

IP Line/ IP Trunk may generate a large number of alarms when Quality of Service (QoS) monitoring is enabled. When QoS monitoring is enabled, an alarm is raised or cleared for every QoS threshold crossing (excellent, good, or fair) per codec. A network with varying QoS has many threshold crossings resulting in a large number of alarms.

Recommended usage For bandwidth and processing reasons, alarm traffic should be minimized. If alarms from the switch are sent to Telephony Manager 3.1, use filtering to limit the traffic to only important alarms. Because it is unlikely that multiple Voice Gateway Media cards simultaneously exhibit problems, the alarms generated by Voice Gateway Media cards should not create traffic problems. To limit alarm traffic, Nortel recommends that you not enable Network QoS Monitoring. Changes to IPLine/IP Trunk to allow filtering helps this situation. The incoming rate of alarms must match the handling capabilities of the Telephony Manager 3.1 configuration.

The alarm circular queue can be quickly exhausted if there is significant alarm traffic.

Operational measurement processing

Voice Gateway Media cards collect operational measurement (OM) information about an hourly basis. This data is stored on the cards until it is retrieved by Telephony Manager 3.1 using an FTP operation. The data can be retrieved on demand, however, the FTP operation is normally scheduled to occur on a daily basis. The data file generated by an Voice Gateway Media card in a 24-hour period is approximately 5 KB.

When retrieval occurs, the information is collected from all cards on all nodes. There is no capability to retrieve the information about an individual node basis.

The retrieved information is parsed and written to comma separated values (CSV) files on the Telephony Manager 3.1 server. The number of files created is dependent upon the number of records retrieved.

If there are many cards in the system, the retrieval operation should be scheduled to occur during off-hours.

Telephony Manager 3.1 system performance

Network impact on Telephony Manager 3.1 Windows client/server

As mentioned in "[Telephony Manager 3.1 server and client overview](#)" (page 61), the Telephony Manager 3.1 Windows clients do not operate in a typical client-server mode. All data is stored on the Telephony Manager 3.1 server and accessed by the Telephony Manager 3.1 client.

The network performance has a significant impact on Telephony Manager 3.1 Windows client/server applications. In particular, the applications are sensitive to the RTT and bandwidth. The RTT is important because numerous smaller packets of data are sent between the server and the client. Very high bandwidth is consumed because Microsoft Access database accesses by the client require transfer of the entire databases. If the RTT or bandwidth is limited, it results in performance degradation. This is manifested by slow response times, and if sufficiently poor may result in failure of operations (for example, timeouts).

The demands on the network are illustrated below for the scenario of a logon to Telephony Manager 3.1 from the client, followed by opening up an application. The measurements were done in a lab environment with a dedicated LAN connection. Performance in the customer environment varies depending on network utilization and system size (for example, number of lines, number of managed systems). During this operation over 2 MB of

data was transferred, and over 7000 packets were transferred between the Telephony Manager 3.1 server and the Telephony Manager 3.1 client. Subsequent operations would result in substantially smaller data transfers.

The impact of the high bandwidth consumption on other customer network applications should be considered when deploying Telephony Manager 3.1 clients on the customer enterprise IP network.

Figure 153 "Response Time versus Round Trip Time" (page 286) shows the relationship between application response time and RTT in a lab environment.

Figure 153
Response Time versus Round Trip Time

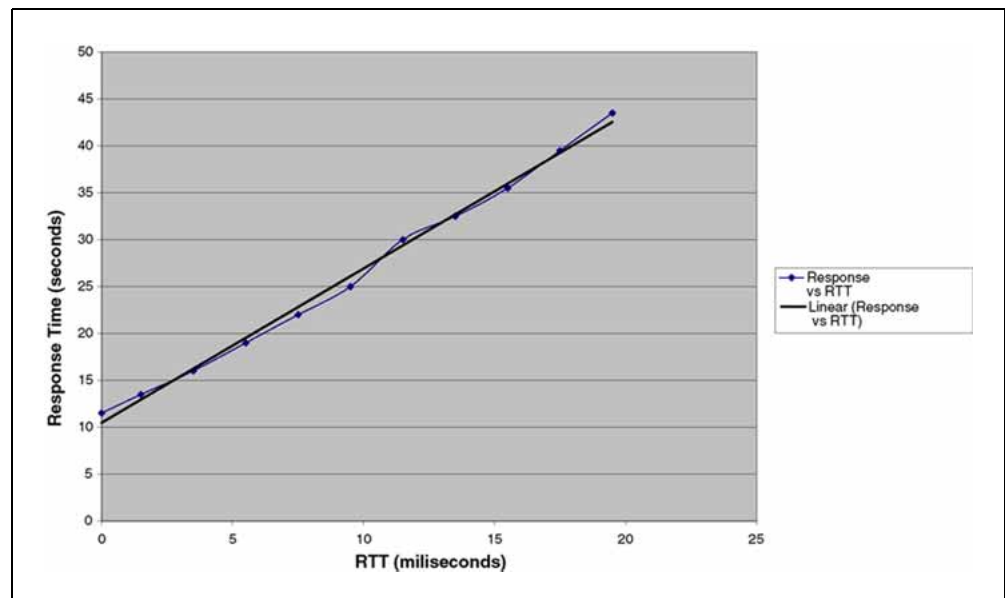
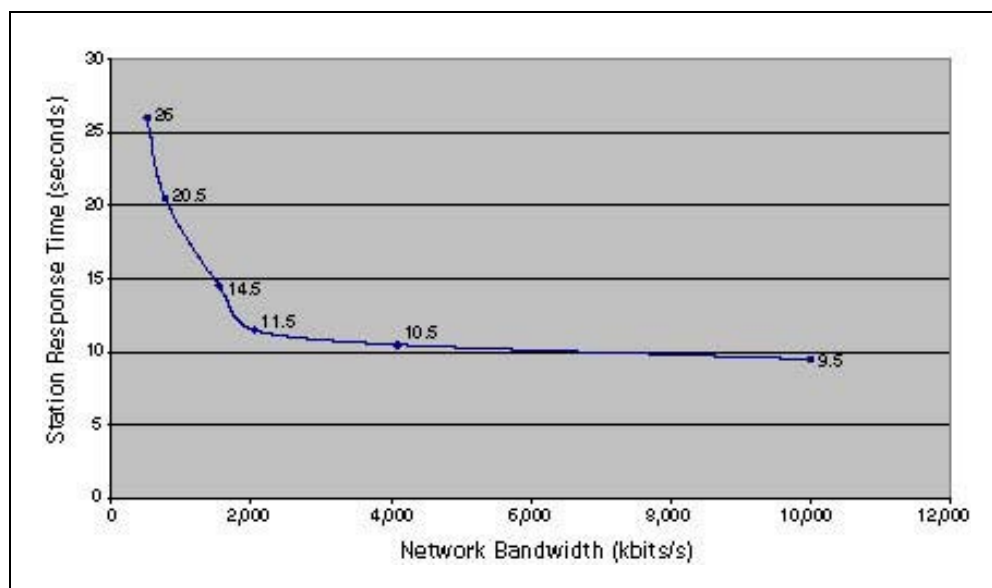


Figure 154 "Response Time versus Network Bandwidth" (page 287) shows the relationship between response time and Bandwidth in a lab environment. Note the negative exponential impact of using bandwidth that is less than 2 Mbps.

Figure 154
Response Time versus Network Bandwidth



Hostname resolution

LMHOSTS file

When Microsoft TCP/IP is used on a local network with any combination of computers running Windows 2000, Windows XP, and so on, server names are automatically matched to their corresponding IP addresses. However, to match server names across remote networks connected by routers (or gateways), the LMHOSTS file can be used if WINS servers are not available on the network. [Figure 155 "Example of LMHOSTS file \(part 1\)" \(page 288\)](#) and [Figure 156 "Example of LMHOSTS file \(part2\)" \(page 289\)](#) show an example of an LMHOSTS file.

The LMHOSTS file is commonly used to locate remote computers for Microsoft networking file, printer, and remote access services, and for domain services such as login, browsing, replication, and so on.

Microsoft TCP/IP loads the LMHOSTS file into memory when the computer is started. The LMHOSTS file is a text file in the Windows directory that lists the IP addresses and computer names of remote Windows networking servers with which you want to communicate. The LMHOSTS file should list all the names and IP addresses of the servers you regularly access.

For example, the LMHOSTS table file entry for a computer with an address of 192.53.63.2 and a NetBIOS computer name of Building1 would be:

```
192.53.63.2 Building1
```


Procedure 78

Creating an LMHOSTS file

Step	Action
------	--------

- | | |
|---|---|
| 1 | Use a text editor to create a file named LMHOSTS. |
|---|---|

Or

Edit the default file named LMHOSTS.SAM.

This file is in the **<system root>\system 32\drivers\etc** directory for Windows 2000 and Windows XP systems.

- | | |
|---|--|
| 2 | In the LMHOSTS file, type the IP address and the host name of each computer that you want to communicate with. |
|---|--|

For example, on each Telephony Manager 3.1 client machine add the Telephony Manager 3.1 server name and its IP address. Separate the items with at least one space.

Note that entries in the LMHOSTS file are not case-sensitive.

Figure 155
Example of LMHOSTS file (part 1)

```

# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample LMHOSTS file used by the Microsoft TCP/IP For Windows.
#
# This file contains the mappings of IP addresses to computernames
# (NetBIOS) names. Each entry should be kept on an individual line.
# The IP address should be placed in the first column followed by the
# corresponding computername. The address and the computername
# should be separated by at least one space or tab. The "#" character
# is generally used to denote the start of a comment (see the exceptions
# below).
#
# This file is compatible with Microsoft LAN Manager 2.x TCP/IP lmhosts
# files and offers the following extensions:
#
#      #PRE
#      #DOM:<domain>
#      #INCLUDE <filename>
#      #BEGIN_ALTERNATE
#      #END_ALTERNATE
#      \0xnn (non-printing character support)
#
# Following any entry in the file with the characters "#PRE" will cause
# the entry to be preloaded into the name cache. By default, entries are
# not preloaded, but are parsed only after dynamic name resolution fails.
#
# Following an entry with the "#DOM:<domain>" tag will associate the
# entry with the domain specified by <domain>. This affects how the
# browser and logon services behave in TCP/IP environments. To preload
# the host name associated with #DOM entry, it is necessary to also add a
# #PRE to the line. The <domain> is always preloaded although it will not
# be shown when the name cache is viewed.
#
# Specifying "#INCLUDE <filename>" will force the RFC NetBIOS (NBT)
# software to seek the specified <filename> and parse it as if it were
# local. <filename> is generally a UNC-based name, allowing a
# centralized lmhosts file to be maintained on a server.
#
# It is ALWAYS necessary to provide a mapping for the IP address of the
# server prior to the #INCLUDE. This mapping must use the #PRE directive.
#
# In addition the share "public" in the example below must be in the
# LanManServer list of "NullSessionShares" in order for client machines to
# be able to read the lmhosts file successfully. This key is under
# \machine\system\currentcontrolset\services\lanmanserver\parameters\nullsessionshares
# in the registry. Simply add "public" to the list found there.

```


Figure 156
Example of LMHOSTS file (part2)

```

#
# The #BEGIN_ and #END_ALTERNATE keywords allow multiple #INCLUDE
# statements to be grouped together. Any single successful include
# will cause the group to succeed.
#
# Finally, non-printing characters can be embedded in mappings by
# first surrounding the NetBIOS name in quotations, then using the
# \0xnn notation to specify a hex value for a non-printing character.
#
# The following example illustrates all of these extensions:
#
# 102.54.94.97      rhino          #PRE #DOM:networking  #net group's DC
# 102.54.94.102     "appname \0x14" #special app server
# 102.54.94.123     popular        #PRE                #source server
# 102.54.94.117     localsrv       #PRE                #needed for the include
#
# #BEGIN ALTERNATE
# #INCLUDE \\localsrv\public\lmhosts
# #INCLUDE \\rhino\public\lmhosts
# #END_ALTERNATE
#
# In the above example, the "appname" server contains a special
# character in its name, the "popular" and "localsrv" server names are
# preloaded, and the "rhino" server name is specified so it can be used
# to later #INCLUDE a centrally maintained lmhosts file if the "localsrv"
# system is unavailable.
#
# Note that the whole file is parsed including comments on each lookup,
# so keeping the number of comments to a minimum will improve performance.
# Therefore it is not advisable to simply add lmhosts file entries onto the
# end of this file.

102.54.94.123      otaserver1      #PRE                #OTH server

```

3 Save the file as LMHOSTS.

The filename is LMHOSTS with no extension.

—End—

LMHOSTS is normally used for smaller networks or to find hosts on remote networks that are not part of the WINS database (because name query requests are not broadcast beyond the local subnetwork). If WINS servers are in place on an internetwork, users do not have to rely on broadcast queries for name resolution because WINS is the preferred method for name resolution. Therefore, with WINS servers in place, LMHOSTS may not be necessary.

The LMHOSTS file is read when WINS or broadcast name resolution fails. Resolved entries are stored in a system cache for later access. When the computer uses the replicator service, and does not use WINS, LMHOSTS entries are required on import and export servers for any computers on different subnetworks participating in the replication.

Procedure 79**Configuring TCP/IP to use LMHOSTS on a Windows PC**

Step Action

- 1 Open Network and Dial-up Connections.
 - 2 Right-click the network connection you want to configure, and then click **Properties**.
 - 3 On the General tab (for local area connection) or the Networking tab (all other connection), click Internet Protocol (TCP/IP), and then click **Properties**. Click **Advanced**, click the WINS tab. Select the Enable LMHOSTS lookup check box. This option is selected by default.
 - 4 To specify the location of the file that you want to import into the LMHOSTS file, click Import LMHOSTS, and then select the file in the Open dialog box.
 - 5 To complete the configuration, either:
 - a. Reboot the computerOr
 - b. Go to the command prompt, and enter the following text:

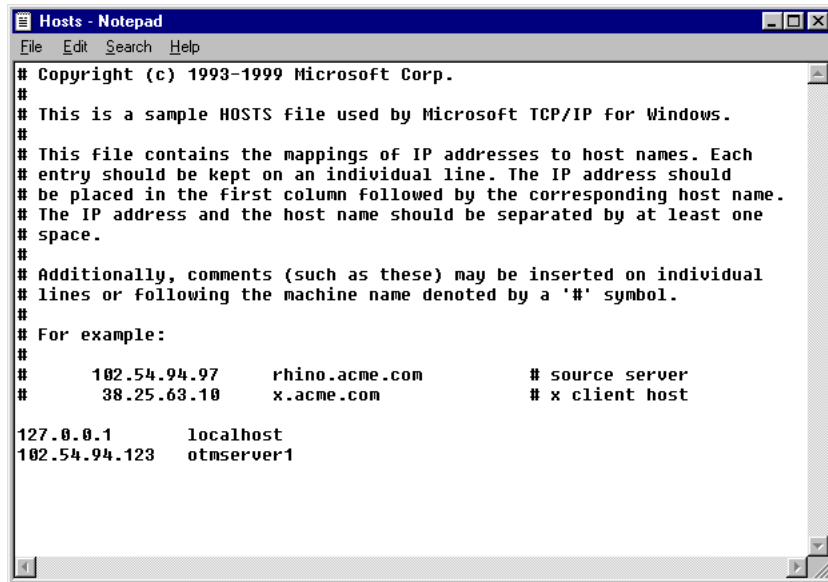
`nbstat -R`
`nbstat -c`
-

—End—

HOSTS file

The HOSTS file contains a list of host name to IP address mappings. It is a regular text file. The HOSTS file is located in the **<system root>**\system32\drivers\etc directory for Windows XP and Windows 2000 systems. See [Figure 157 "Sample HOSTS file" \(page 291\)](#).

Figure 157
Sample HOSTS file



```

# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97      rhino.acme.com      # source server
#      38.25.63.10     x.acme.com         # x client host

127.0.0.1      localhost
102.54.94.123  otmserver1

```

Use a text editor to edit the HOSTS file. In the HOSTS file, type the IP address and the host name of each computer with which you want to communicate, for example, on each Telephony Manager 3.1 client computer add the Telephony Manager 3.1 server IP address followed by its name. Separate the items with at least one space. Entries in the HOSTS file are not case-sensitive. Note that the HOSTS filename has no extension.

Telephony Manager 3.1 port usage

When using Telephony Manager 3.1 to monitor and maintain systems, various ports and protocols are used to communicate between Telephony Manager 3.1 and the desired client, server, or application. [Table 18 "Telephony Manager 3.1 Port Usage" \(page 292\)](#) lists typical port usage based on the flow of information between Telephony Manager 3.1 and these system components.

Table 18
Telephony Manager 3.1 Port Usage

Telephony Manager 3.1 Sending To	Port	Type	Protocol	Component	Remarks
Meridian 1 or Communication server 1000 system	513	TCP	Rlogon	Session Connect, System Terminal, Station Admin, CPND, List manager, ESN.	Using netstat
Meridian 1 or Communication server 1000 system	161	UDP	SNMP	Alarm Management, Maintenance Window	Microsoft Default Port
Meridian 1 or Communication server 1000 system	21	TCP	FTP	Corporate Directory & DBA	Microsoft Default Port
Meridian 1 or Communication server 1000 system	20	TCP	FTP	Corporate Directory & DBA	Microsoft Default Port FTP -data
SMTP server	25	TCP	SMTP	Alarm Notification	Microsoft Default Port
IP Line/IP Trunk	21	TCP	FTP	Telephony Manager 3.1	Microsoft Default Port
Win client	139	TCP	NetBEUI	Windows client File Sharing	Microsoft Default Port
CND server	389	TCP	CND	CND Synchronization	Microsoft Default Port
CND server Over SSL	636	TCP		CND synchronization	Microsoft Default Port (CND SSL)
Telephony Manager 3.1 Receiving From	Port	Type	Protocol	Component	Remarks
Web client	80	TCP	HTTP	Web CS, Desktop Services, Web telecom billing system	Microsoft Default Port
Web client	8080	TCP	HTTP	telephone manager	Apache Tomcat Web Server

Telephony Manager 3.1 Sending To					
To	Port	Type	Protocol	Component	Remarks
Web client	4789-5045	TCP		Virtual System Terminal <i>VT uses 1 port per session. Start with 4789.</i>	The base port can be changed from 4789.
Win client	139	TCP	NetBEUI	Windows client File Sharing	Microsoft Default Port
Win client	135	TCP/UDP		logon	RPC, SCM used by DCOM
Meridian 1 or Communication server 1000 sending to					
	Port	Type	Protocol	Component	Remarks
Telephony Manager 3.1	162	UDP	SNMP	Alarm Traps (LD 117), Maintenance window	Microsoft Default Port
Telephony Manager 3.1	1929-2058	UDP		DBA <i>1 port per session. Start from 1929 till 2057.</i> 2058 and onward is used as Data ports till 2185.	
DECT	5099	TCP	RMI	Telephony Manager 3.1 DECT	Using netstat command

Telephony Manager 3.1 language support

Telephony Manager 3.1 supports the following language configurations:

Telephony Manager 3.1 Languages supported for English and Regional OS								
client language locale should be set to the language in which Telephony Manager 3.1 is to be run								
server OS & Locale	client Regional OS							
	English		Japanese	Simplified Chinese	Portuguese	Spanish	French	German
	WinXP Pro	Win2K Pro	Win2K/XP Pro	Win2K/XP Pro	Win2K/XP Pro	Win2K/XP Pro	Win2K/XP Pro	Win2K/XP Pro
English Win2003 server (English Locale)	English Telephony Manager 3.1	English Telephony Manager 3.1			English Telephony Manager 3.1	English Telephony Manager 3.1	English Telephony Manager 3.1	English Telephony Manager 3.1
English Win2003 server (French Locale)							French Telephony Manager 3.1	
English Win2003 server (German Locale)								German Telephony Manager 3.1
English Win2K server (English Locale)	English Telephony Manager 3.1	English Telephony Manager 3.1			English Telephony Manager 3.1	English Telephony Manager 3.1	English Telephony Manager 3.1	English Telephony Manager 3.1
English Win2K server (French Locale)							French Telephony Manager 3.1	
English Win2K server (German Locale)								German Telephony Manager 3.1

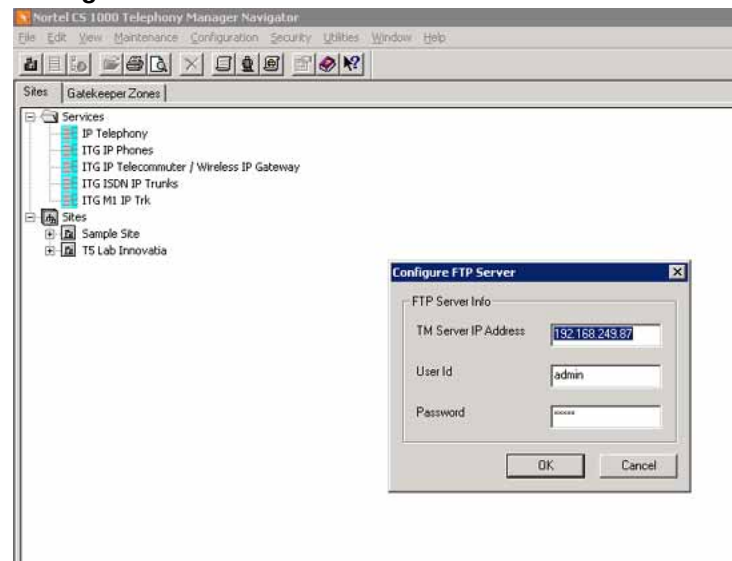
Telephony Manager 3.1 Languages supported for English and Regional OS								
client language locale should be set to the language in which Telephony Manager 3.1 is to be run								
server OS & Locale	client Regional OS							
	English		Japanese	Simplified Chinese	Portuguese	Spanish	French	German
	WinXP Pro	Win2K Pro	Win2K/XP Pro	Win2K/XP Pro	Win2K/XP Pro	Win2K/XP Pro	Win2K/XP Pro	Win2K/XP Pro
Japanese Win2K or 2003 server			English Telephony Manager 3.1					
Simplified Chinese Win2K or 2003 server				English Telephony Manager 3.1				
Standalone machine (no Telephony Manager 3.1 client)	English Telephony Manager 3.1	English Telephony Manager 3.1	English Telephony Manager 3.1	English Telephony Manager 3.1	English Telephony Manager 3.1	English Telephony Manager 3.1	English or French Telephony Manager 3.1	English or German Telephony Manager 3.1

FTP Server configuration

Telephony Manager 3.1 uses the FTP service from Microsoft Internet Information Server. The correct Telephony Manager 3.1 Server IP address and FTP user account information must be configured in order to support file transfer operations in ITG Services and Corporate Directory applications.

To configure, go to Start>Programs>Telephony Manager Navigator. From the Configuration menu, select **Configure FTP Server** and enter the correct Telephony Manager Server IP address, username and password. See [Figure 158 "Configure FTP server" \(page 296\)](#).

Figure 158
Configure FTP server



Appendix B

Installation checklist

Contents

This appendix contains information about the following topics:

["Overview" \(page 297\)](#)

["Installation requirements" \(page 297\)](#)

["Programming the switch" \(page 298\)](#)

["PC/server installation requirements" \(page 298\)](#)

Overview

Use the following quick reference as a checklist or reminder when starting a new Telephony Manager 3.1 installation.

Installation requirements

Software and memory

- [] Required X11 packages (296, 315, and 351 depending on applications installed)

Ethernet connections

- [] Release 24B or later for Data Buffering and Access
- [] IOP, IOP/CMDU, or IODU/C cards for Meridian 1 PBX 51C, 61C, 81, or 81C
- [] Ethernet AUI cables to be attached to each IOP (Meridian 1 PBX 51C, 61C, 81, or 81C)
- [] NTDK27 Ethernet cable for Meridian 1 PBX 11C CA
- [] Transceivers to connect to the LAN
- [] Router

PPP connections

- ☐ Hayes-compatible modem
- ☐ SDI port available on the system (configured for SCH only)
- ☐ Serial cable to connect the modem to the SDI port

Serial connections

- ☐ SDI port available on the switch (configured for SCH only)
- ☐ Hayes-compatible modem for remote connection (optional)
- ☐ Serial cable to connect the modem to the SDI port

Programming the switch

- ☐ Enable Name Option in LD 17.
- ☐ Define Limited Access Password in LD 17.
- ☐ For Serial communication: Configure a TTY with User = SCH in LD 17.
- ☐ For Ethernet or PPP communication: Configure a pseudo TTY (PTY) with User = SCH MTC BUG in LD 17.
- ☐ Configure Ethernet at the switch in LD 117.
- ☐ Define the Gateway (router) IP address on the switch in LD 117.
- ☐ Configure PPP at the switch in LD 117.
- ☐ INIT the switch.
- ☐ Enable the new IP address (defined in LD 117) in LD 137.
- ☐ Enable Database Disaster Recovery (DDR) in LD 117.
- ☐ Set open alarm destination in LD 117.
- ☐ Set up Data Buffering and Access in LD 117.
- ☐ Set up filtering in the system to filter out information and minor messages.

PC/server installation requirements

For detailed Telephony Manager 3.1 minimum hardware and software requirements, see ["Preparing for installation" \(page 29\)](#).

Appendix C

Configuring a USB modem

Contents

This appendix contains information about the following topics:

["Overview" \(page 299\)](#)

["Checking for a virtual COM port" \(page 299\)](#)

["Changing the virtual COM port to USB modem association" \(page 300\)](#)

Overview

The installation program for your USB modem creates a virtual COM port. The virtual COM port allows various communications programs to seamlessly operate with USB modems. This section shows you how to determine if a virtual COM port is created and how to change which virtual COM port is associated with your USB modem.

Checking for a virtual COM port

Ensure your USB modem is associated with a virtual COM port by completing the steps in the following procedure (see [Procedure 80 "Checking for a virtual COM port" \(page 299\)](#)).

Procedure 80

Checking for a virtual COM port

Step	Action
1	If running Windows 2000, go to Start > Settings > Control Panel > Phone and Modem Options.
2	From Windows XP, go to Start > Control Panel > Phone and Modem Options.

Figure 159
Phone and modem options



- 3 Click the Modems tab (see [Figure 159 "Phone and modem options" \(page 300\)](#)). The modem appears in the list.
- 4 If the modem is not connected to the computer, it does not appear in the installed modems list. Connect the modem and repeat steps 1-3. If your modem is connected to your server, and is properly installed, but still does not appear in this list, Telephony Manager 3.1 does not support your modem.
- 5 Take note of the COM port your modem is associated with as indicated in the Attached To column in [Figure 159 "Phone and modem options" \(page 300\)](#). This is the COM port you need to select when configuring the Dial-up parameters for a collection task in the Telecom Billing System.

—End—

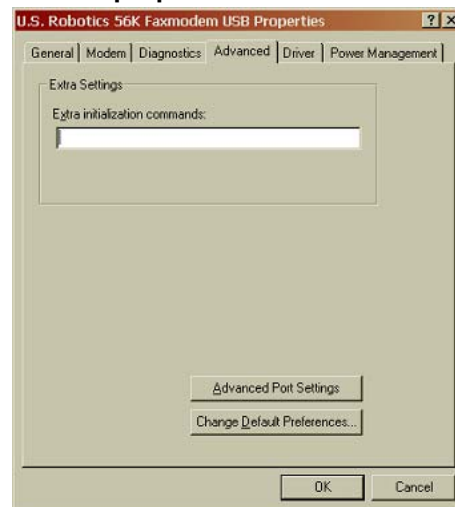
Changing the virtual COM port to USB modem association

Telephony Manager 3.1 requires your USB modem to be associated with a COM port in the range between COM1 and COM10. If the virtual COM port identified in [Procedure 80 "Checking for a virtual COM port" \(page 299\)](#) is not within the supported range, complete the following steps ([Procedure 81 "Changing the virtual COM port to USB modem association" \(page 301\)](#)) to change the association.

Procedure 81**Changing the virtual COM port to USB modem association**

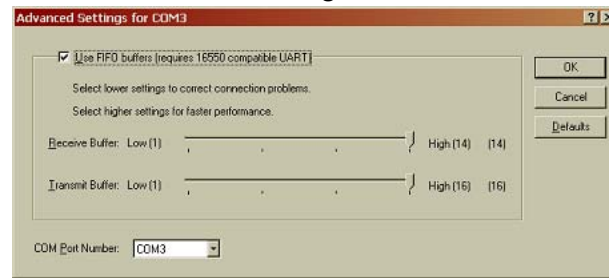
Step	Action
1	Close all applications using a COM port on your Telephony Manager 3.1 server.
2	Open the System Properties dialog.
3	If running Windows 2000, go to Start > Settings > Control Panel > System.
4	If running Windows XP, go to Start > Control Panel > System.
5	Click the Hardware tab.
6	Click the Device Manager button.
7	Expand the Modems node of the tree and select your USB modem.
8	Right-click and select Properties from the popup menu.
9	Click the Advanced tab. Figure 160 "Modem properties" (page 301) shows an example for the U.S. Robotics USB modem.

Figure 160
Modem properties



- 10 Select the Advanced Port Settings button. A dialog similar to [Figure 161 "Advanced modem settings" \(page 302\)](#) appears.

Figure 161
Advanced modem settings



- 11 The COM Port Number select drop-down list allows you to change the COM port to which the USB modem is associated, and correspondingly change the virtual COM port. Select from the list a COM port not in use and which is within the range of COM1 to COM10.

ATTENTION

If your server has a COM1, the list shows COM1 (in use) because this is a physically present COM port that cannot also be a virtual COM port. If you have installed a multi-modem or other multiple-serial port cards, these cards create virtual COM ports. Typically, they create 2, 4, or 8 virtual COM ports numbered beginning at 3, 4, or 5. You may need to change their first virtual COM port, so your USB modem is mapped to a virtual COM port in the range of COM1 to COM10.

- 12 When you have made your selection, click the OK button. If you have changed the COM port, the old virtual COM port is removed, and the new one created. You can now use this virtual COM port in the Telecom Billing System.
- 13 Close all open Device Manager and property dialogs.

—End—

Appendix

TBS to CND file header conversion

The following table provides sample information for CVS Subscriber Import utilizing the TBS file header to CND file header conversion.

See ["Migrating employee data" \(page 81\)](#) for further information regarding migrating employee data.

Table 19
TBS file header to CND file header conversion

TBS File Header	CND File Header
UserID or EmpFNameEmpLName	cn
EmpFName	givenName
EmpMName	initials
EmpLName	sn
blank field	employeeNumber
Abbr1,Abbr2,Abbr3,... Abbr20	departmentNumber
JobTitle	title
Email	mail
Address	street
City	l
ProvState	st
Postal	postalCode
Country	country
DisplayNameAttribute	cpndName
UserGroupAttribute	tmUserGroup
WebReportingAccessRightsAttribute	billingWebReportingAccessRights
AccountCodeAsset_	billingAccountCode
AuthorizationCodeAsset_	billingAuthorizationCode

ExtensionAsset_	preferredDirectoryNumber
PhoneNumberAsset_	preferredExternalTelephoneNumber
StationLocationAsset_	officeLocation

Index

A

access
 restriction 167
 rights 159
access permissions 137
 administrators 137
add object to ENMS 194
Administrators user group 165
alarms 210
applications 99, 197
authentication 160, 168, 175

B

bandwidth 283

C

capacity factors 258
configure
 Desktop Services 147
 modem
 high-speed smart modem
 considerations 150
configuring Telephony Manager 175
 users 167
connection, test 94
customer LAN 253, 283

D

Desktop Services 147, 272
dongle 91

E

embedded LAN 283
end users 163
EndUser user group 165
engineering guidelines 257
ENMS
 adding Telephony Manager 3.1 Server
 object 194
 start Telephony Manager 3.1 Web
 applications 197

F

Fault Summary 200
 set up 201

G

General Cost Allocation System 258

H

hard disk 275
hardware requirements
 disk size 276
 HP OpenView 208
 processor speed 276
HelpDesk user group 165
HP OpenView
 configure OTM Server 229
 hardware and software requirements 208
 installation and configuration 211

I

installation

Desktop Services 147
HP OpenView 211
Windows 2000 243
Windows NT
 component installation 244
 network adapter software 246

J

Java Runtime Environment 190, 198

K

keycode 89

L

licenses
 Reporting Unit 90
 Terminal Number 89
limitations
 software
 hard-coded 266
 operational 272
local users 163
logon 136, 163

M

memory requirements 274
Meridian 1
 programming 298
 software requirements 297
modem 251
 high-speed smart modem
 considerations 150
 troubleshooting 151

N

Navigator access 141
Navigator users 162
network connection 183
network map 209
Network Node Manager
 access Telephony Manager Server 210
 Alarm Browser 210
 configure OTM Server 229
 configure OTM Web Server Access 228
 network map 209

 set up Network Map 219
 Telephony Manager 3.1 Status
 Monitor 218
Novell 34

O

Optivity Integration Toolkit 190

P

password policy 161
programming, Meridian 1 298

R

Remote Access Service (RAS) 251
remote users 163
requirements
 Ethernet connections 297
 PPP connections 298
 serial connections 298
 software
 Meridian 1 297
RU license 90

S

security 136
security device 91
serial connection 182
serial number 89
serial ports 182
Server installation requirements 298
set up
 applications 99
 communications information 94, 94
 customer information 97, 97
 system data 101
 Windows 2000 243, 243
software requirements
 HP OpenView 209
 Meridian 1 297
supported systems 30
supported upgrade paths 32

T

TCP/IP 247
Telephone access 144

- Features tab 146
- General tab 144
- Keys tab 144
- Telephone Manager 272
- Telephony Manager 3.1 administrators 136
- Telephony Manager 3.1 Client License 91
- Telephony Manager 3.1 Directory 148
- Telephony Manager 3.1 Help desk
 - users 136
- Telephony Manager 3.1 Server 194
- Telephony Manager 3.1 Status Monitor 218
- Telephony Managers folder 194
- Terminal server 179
- Terminal Server 182
- test
 - connection 94
 - network cards 253
- TN license 89
- troubleshooting
 - modem connections 151
- U**
 - uninstall Telephony Manager 235
 - user
 - adding 173
 - authentication 168, 175
 - configuring 167
 - restricting access 167
 - user authentication 160
 - user group 168
 - creating 170
 - deleting 167
 - properties 142
 - user groups 157
 - User Groups 164
 - user management 162, 166
 - users
 - Default 136
 - Telephony Manager 3.1 administrators 136
 - Telephony Manager 3.1 Help desk 136
- V**
 - virtual ports 181
 - Virtual System Terminal
 - Web 184
- W**
 - Web reporting role 148
 - Web Virtual System Terminal 184
 - Windows 2000
 - installing 243
 - setup program 243, 243
 - Windows NT
 - component installation 244
 - network adapter software installation 246
- X**
 - X11 packages 297

Nortel Communication Server 1000

Telephony Manager 3.1 Installation and Commissioning

Copyright © 2003-2008, Nortel Networks
All Rights Reserved.

Publication: NN43050-300
Document status: Standard
Document version: 01.07
Document date: 3 June 2009

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Nortel, the Nortel Logo, the Globemark, SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

