Part No. 321536-A
14-February-2006

4655 Great America Parkway
Santa Clara, CA 95054

Implementing Nortel Enterprise Network Management System Security

NORTEL

>THIS IS THE WAY
>THIS IS NORTEL™

Copyright © 2006 Nortel Networks

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 Inc.

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.

Trademarks

Nortel Networks, the Nortel logo, the Globemark, Accelar, Bay Networks, BayStack, Centillion, Meridian, Optivity, Passport, Unified Networks, and Versalar are trademarks of Nortel Networks.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Alteon is a trademark of Alteon Websystems Incorporated.

HyperHelp is a trademark of Bristol Technology.

Cisco and Cisco Systems are trademarks of Cisco Systems, Incorporated.

HP-UX and OpenView are trademarks of Hewlett-Packard Corporation.

Oracle is a trademark of Oracle Corporation.

IBM, NetView, RS/6000, Tivoli, TME, and TME 10 are trademarks of IBM Corporation.

Intel and Pentium are registered trademarks of Intel Corporation.

Microsoft, MS-DOS, Win32, Windows, Windows 2003, and Windows NT are registered trademarks of Microsoft Corporation.

Netscape Navigator is a trademark of Netscape Communications Corporation.

UNIX is a registered trademark of X/Open Company Limited.

SPARC and SPARCstation are trademarks of Sparc International, Inc.

Sun, Solaris, and Java are trademarks or registered trademarks of Sun Microsystems, Incorporated.

The asterisk after a name denotes a trademarked item.

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.

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. Enterprise network management software license agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying Enterprise network management software or installing the hardware unit with pre-enabled Enterprise network management 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. Open Source. Open sources used in Nortel Enterprise Network Management System include: JBoss: 4.0.2; Apache Commons BeanUtils: 1.7.0; Apache Commons Net: 1.4.0; Apache Commons Collections: 3.1; Apache Commons Pool: 1.2; Apache Commons DBCP: 1.2.1; Apache Logging Log4J: 1.2.11; JUnit: 3.8.1; SNMP4J: 1.1.1. Copyright and license information is provided at: http://www.gnu.org/copyleft/lesser.html.

10. 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.

Contents

Chapter 1
Getting Started

About this guide

Implementing Nortel Enterprise Network Management System Security covers the following topics:

- instructions for running Enterprise NMS server software behind a firewall and setting access to Enterprise NMS according to the client IP address ("Managing Enterprise NMS firewall support" on page 17)
- instructions for configuring access to Enterprise NMS applications ("Specifying access to applications with Access Control Administration" on page 21)
- instructions for building a database of SNMP community strings ("Specifying access to devices with the Community Strings Editor" on page 49).

Audience

This guide is intended for network managers working with Enterprise NMS in a UNIX or Windows-based environment. This guide assumes that you have the following background:

- Working knowledge of your operating system environment: Solaris*, HP-UX, Windows 2000 client/server, Windows XP, or Windows 2003 server.
- Familiarity with managing and troubleshooting large, complex networks.
- Experience with working with Nortel and standards-based networking devices.
- Working knowledge of the transmission and management protocols used on your network.

- If Enterprise NMS is installed with HP* OpenView* Network Node Manager or Tivoli* TME 10* Netview), familiarity with the network management applications.

Acronyms

The following is a list of acronyms used in this guide:

ATM	Asynchronous Transfer Mode
IP	Internet Protocol
LAN	Local Area Network
MIB	Management Information Base
NMS	Network Management System
SNMP	Simple Network Management Protocol
DIT	Device Integration Toolkit
VLAN	Virtual LAN
WAN	Wide Area Network

Symbols and text conventions

These symbols are used to Highlight critical information for the Enterprise NMS system:

Caution: Alerts you to conditions where you can damage the equipment.

Danger: Alerts you to conditions where you can get an electrical shock.

Warning: Alerts you to conditions where you can cause the system to fail or work improperly.

Note: A Note alerts you to important information.

Tip: Alerts you to additional information that can help you perform a task.

Security note: Indicates a point of system security where a default should be changed, or where the administrator needs to make a decision about the level of security required for the system.

Warning: Alerts you to ground yourself with an antistatic grounding strap before performing the maintenance procedure.

Warning: Alerts you to remove the Enterprise NMS main unit and expansion unit power cords from the ac outlet before performing any maintenance procedure.

These text conventions are used in this guide to indicate the information described:

angle brackets (< >)

Indicate that 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 `ping` *<ip_address>*, you enter `ping 192.32.10.12`

`bold Courier text`

Indicates command names and options and text that you need to enter.

Example: Use the **`dinfo`** command.

Example: Enter **`show ip`** {**`alerts`**|**`routes`**}.

braces ({})

Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command.

Example: If the command syntax is `show ip {alerts|routes}`, you must enter either `show ip alerts` or `show ip routes`, but not both.

brackets ([ ])

Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.

Example: If the command syntax is `show ip interfaces [-alerts]`, you can enter either `show ip interfaces` or `show ip interfaces -alerts`.

ellipsis points (. . .)

Indicate that you repeat the last element of the command as needed.

Example: If the command syntax is `ethernet/2/1 [`*<parameter> <value>*`]...`, you enter `ethernet/2/1` and as many parameter-value pairs as needed.

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: If the command syntax is `show at` *`<valid_route>`*, *`valid_route`* is one variable and you substitute one value for it.
`plain Courier text`	Indicates command syntax and system output, for example, prompts and system messages. Example: `Set Trap Monitor Filters`
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is `show ip {alerts|routes}`, you enter either `show ip alerts` or `show ip routes`, but not both.

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:

http://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 phone 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:

http://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:

http://www.nortel.com/erc

Getting Help through a Nortel distributor or reseller

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

Chapter 2
Managing Enterprise NMS firewall support

This chapter describes how to manage the Enterprise NMS firewall support feature. This feature lets you run Enterprise NMS server software behind a firewall. It also lets you allow or deny access to Enterprise NMS according to the client IP address.

Firewall support overview

Enterprise NMS incorporates a redirection server that manages communication between the Enterprise NMS server and its clients. When enabled, this redirection server manages all communication through a single port in your firewall.

In addition to the redirection server, Enterprise NMS 10.4 also lets you restrict communication with Enterprise NMS server applications to only a list of trusted IP addresses. See "Restricting access according to IP address" on page 19 for more information.

Required firewall ports

In order to use the Enterprise NMS firewall support feature, you must allow communication through at least five ports in your firewall for the following Enterprise NMS components:

- Apache web server: default is port 80
- webOptSrvr: must be port 391
- Redirection server: any port greater than 1024
- Enterprise JBOSS remote port: default is 5400
- Enterprise Java Naming and Directory Interface port: default is 1099

You must set the ports both in your firewall configuration and in the Enterprise NMS installation. You are prompted for the port numbers during the initial Enterprise NMS software installation. You can also change the setting for the redirection server port after installation. See "Installing or activating the firewall support feature," next for more information.

Installing or activating the firewall support feature

You can enable the firewall support feature during the installation of Enterprise NMS, or you can enable it after the installation:

- To enable the firewall support feature during the installation, respond yes when the installation prompts you if Enterprise NMS servers will be running behind a firewall.
- To enable the firewall support feature after the installation, you edit the firewall support configuration file to change the enable setting and also to specify the firewall port for client/server communication.

The firewall support configuration file is located as follows:

- On UNIX: $LNMSHOME/conf/weboptsrvr.conf
- On Windows: %LNMSHOME%\conf\weboptsrvr.conf

The firewall support configuration file contains two parameters and their settings, for example:

```
STATUS=OFF
PORT=50000
```

To enable the firewall support feature, edit the file so that the STATUS parameter is set to ON. To change the firewall port through which Enterprise NMS communicates with the client applications, set the PORT parameter to any desired port number greater than 1024.

After editing the firewall support configuration file, you must stop and then restart all of the Enterprise NMS daemons or services.

Restricting access according to IP address

Enterprise NMS lets you specify a list of trusted IP addresses that are allowed to communicate with Enterprise NMS server applications. Access attempts by non-listed IP addresses is automatically blocked.

You can also specify a list of the client IP addresses that are behind the firewall and thus require no redirection by the redirection server.

You maintain the lists of IP addresses in the following file on the Enterprise NMS server:

- On UNIX: $LNMSHOME/conf/restrictedIP.conf
- On Windows: %LNMSHOME%\conf\restrictedIP.conf

This file contains descriptions and examples of its features in a comment block at its beginning, followed by actual tags and variables.

After editing the IP restriction file, you must stop and then restart all of the Enterprise NMS daemons or services.

Chapter 3
Specifying access to applications with Access Control Administration

This chapter is divided into the following major sections:

- "Access Control Administration overview," next
- "Getting started with Access Control Administration" on page 22
- "Working with Access Control Administration" on page 31
- "Troubleshooting Access Control Administration" on page 45

Access Control Administration overview

Access Control Administration lets you control user access to Enterprise NMS applications, components, services, and view domains. By default, access control is disabled, letting any Enterprise user log in to InfoCenter and run all Enterprise NMS applications.

The following sections describe operations that Enterprise NMS access administrators can perform with Access Control Administration:

- "Enabling and disabling access control" on page 32
- "Adding Enterprise NMS users" on page 33
- "Removing Enterprise users" on page 34
- "Setting user permissions" on page 35
- "Changing permission settings" on page 36
- "Adding permission groups" on page 38
- "Attaching permission groups" on page 40
- "Assigning view domains to Enterprise NMS users" on page 42
- "Assigning services to Enterprise NMS users" on page 44

Getting started with Access Control Administration

The following sections introduce Access Control Administration and tell how to get started using it:

- "Access Control Administration features," next
- "Enterprise NMS access administrators" on page 23
- "Access permission tokens" on page 24
- "Starting Access Control Administration" on page 25
- "Access Control Administration window" on page 27

Access Control Administration features

Network managers control user access to Enterprise NMS in the InfoCenter Access Control Administration window.

The Access Control Administration window uses a system of permission tokens to represent Enterprise NMS applications and functions. You manage access by adding, removing, or modifying permission tokens for configured Enterprise NMS users.

Table 1 describes the main features of Enterprise NMS Access Control Administration.

Table 1 Access Control Administration features

Feature	Description
Enterprise user	Operating system user who can view or modify Enterprise NMS components. You can configure any user that has a valid operating system user ID as an Enterprise user. See "Enterprise NMS access administrators" on page 23 for information about Enterprise superusers.
Access administrator	Enterprise NMS user with read/write access to all permission tokens. The two fixed access administrators are: • Administrator • root
Permission token	Identification label for the Enterprise NMS application components you can administer with Access Control Administration. Some applications have more than one permission token. You cannot add or delete available tokens. See "Attaching and detaching permissions" on page 36 for more information.

Table 1 Access Control Administration features (continued)

Feature	Description
Access permission	A permission token setting that establishes the level of access to Enterprise NMS components for individual users and groups of users. Valid permission settings are: • Read – Users can view data, but cannot change or add data. • Read/write – Users can modify database information and window preferences. See “Attaching and detaching permissions” on page 36 for more information.
Permission group	Set of permission tokens with preconfigured access permissions. For example, the default ENTERPRISE_ADMIN permission group contains all of the available tokens set to read/write access. The default ENTERPRISE_VIEW permission group contains all tokens set to read-only. You can save time setting permissions by attaching a permission group to Enterprise users who have similar access requirements. For more information, see “Attaching permission groups” on page 40, “Changing permission groups” on page 41, and “Adding permission groups” on page 38.

Enterprise NMS access administrators

The following users are automatically configured as Enterprise NMS access administrators:

- Administrator
- root

The access administrator has read/write access to all permission tokens. You cannot delete or modify access permissions for the Administrator or root, and cannot remove them as Enterprise users.

Enterprise NMS access administrators inherit the password of the operating system root and Administrator users on the Enterprise NMS server.

Any Enterprise NMS user configured with read/write access to every token can administer all Access Control Administration features, but the root and Administrator access administrators remain fixed as a security protection.

Access permission tokens

Table 2 lists the permission tokens you can control with Access Control Administration.

Table 2 Access permission tokens

Token name	**Provides access to...**
ACCESS_CONTROL	InfoCenter Access Control Administration window.
BAY_SECURE	BaySecure LAN Access application.
COMMUNITY_STRINGS	InfoCenter Community Strings Editor window.
CV_VIEW	Call View ATM window.
DB_ADMIN_ACCT	InfoCenter Database Admin Tool.
DISCOVERY_ADMIN	Lets users configure rediscovery preferences and auto rediscovery parameters, stop all discoveries including discoveries started by other users, view log messages, and change discovery preferences. Can only be assigned with read/write permission.
DIV	Device Inventory Viewer.
FS_ACCESS	Fault Summary application.
IC	InfoCenter folder manipulation.
IC_ADMIN	InfoCenter folder access and Monitor Options window
IPSM_ACCESS	IP Service Manager
NPT_ACCESS	InfoCenter Path Trace window.
OM_READ_STATS	OmniView read statistics and preferences.
OM_SNMP_SETS	OmniView SNMP Set actions.
OM_CONF_ALLUSERS	OmniView global templates.
OM_CONF_TEMPL	OmniView individual templates.
SE_READ_STATS	Expanded View read statistics and preferences
SE_SNMP_SETS	Expanded View SNMP Set actions.
SERVICE_ASSIGN	Lets users assign services to other users. Can only be assigned with read/write permission.
TOPUI_ACCESS	With Read only privileges, users can open AutoTopology Manager, view discovery status details, and view view domain information. Read/Write grants full access to all Autotopology Manager functions, including starting a discovery process.
TDC_READ_STATS	TD Continuity Read Stats and preference changes

Table 2 Access permission tokens (continued)

Token name	Provides access to…
TDC_SNMP_SETS	TD Continuity SNMP set actions.
VIEW_DOMAIN_MGMT	Lets users create, delete, edit, and assign view domains to other users. Can only be assigned with read/write permission.

Starting Access Control Administration

To start Access Control Administration:

1 Take one of the actions shown in Table 3.

Table 3 Starting Access Control Administration

To start Access Control Administration from:	Do this:
InfoCenter	Choose Admin > Access Control **Note:** If the Access Control menu command is disabled, it means you do not have the proper access permissions to use Access Control Administration.
Windows Start menu	Choose Start > Programs > Enterprise > AccessAdmin

Windows command prompt	**`cd %lnmshome%\bin`**
	`accessadmin`

Table 3 Starting Access Control Administration (continued)

To start Access Control Administration from:	**Do this:**

UNIX command prompt	**`cd $LNMSHOME/bin`**
	`accessadmin`

Web browser	Point your Web browser to: **`http://`**`[IP or hostname of Enterprise NMS server]` Click the Access Control Administration icon on the Enterprise Web page. **Note:** You can use your Web browser's Bookmark or Favorites feature to bookmark the Access Control Administration application. Doing so saves the URL for Access Control Administration.

If you are not starting Access Control Administration from InfoCenter, the Connect to Enterprise Server dialog box opens.

2 If prompted, enter your login information and click OK.

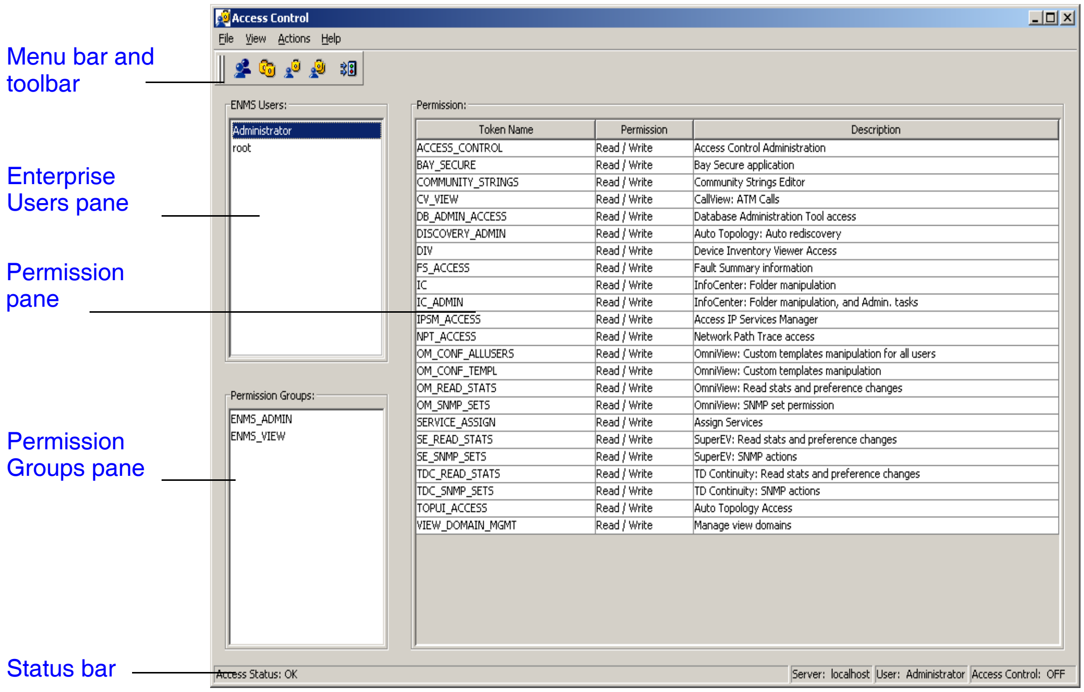
The Access Control Administration window opens.

To begin using Access Control Administration features, enable access control. See "Enabling and disabling access control" on page 32 for more information.

Access Control Administration window

The Access Control Administration window has six parts as shown in Figure 1.

Figure 1 Access Control Administration window



Token Name	Permission	Description
ACCESS_CONTROL	Read / Write	Access Control Administration
BAY_SECURE	Read / Write	Bay Secure application
COMMUNITY_STRINGS	Read / Write	Community Strings Editor
CV_VIEW	Read / Write	CallView: ATM Calls
DB_ADMIN_ACCESS	Read / Write	Database Administration Tool access
DISCOVERY_ADMIN	Read / Write	Auto Topology: Auto rediscovery
DIV	Read / Write	Device Inventory Viewer Access
FS_ACCESS	Read / Write	Fault Summary information
IC	Read / Write	InfoCenter: Folder manipulation
IC_ADMIN	Read / Write	InfoCenter: Folder manipulation, and Admin. tasks
IPSM_ACCESS	Read / Write	Access IP Services Manager
NPT_ACCESS	Read / Write	Network Path Trace access
OM_CONF_ALLUSERS	Read / Write	OmniView: Custom templates manipulation for all users
OM_CONF_TEMPL	Read / Write	OmniView: Custom templates manipulation
OM_READ_STATS	Read / Write	OmniView: Read stats and preference changes
OM_SNMP_SETS	Read / Write	OmniView: SNMP set permission
SERVICE_ASSIGN	Read / Write	Assign Services
SE_READ_STATS	Read / Write	SuperEV: Read stats and preference changes
SE_SNMP_SETS	Read / Write	SuperEV: SNMP actions
TDC_READ_STATS	Read / Write	TD Continuity: Read stats and preference changes
TDC_SNMP_SETS	Read / Write	TD Continuity: SNMP actions
TOPUI_ACCESS	Read / Write	Auto Topology Access
VIEW_DOMAIN_MGMT	Read / Write	Manage view domains

Access Status: OK | Server: localhost | User: Administrator | Access Control: OFF

Table 4 describes the Access Control Administration window parts.

Table 4 Parts of the Access Control Administration window

Part	Description
Menu bar and toolbar	Provides access to all available commands. See "Menu bar and toolbar," next for information about the menu commands and toolbar buttons.
Enterprise Users pane	Lists the system users configured to use Enterprise NMS. See "Enterprise Users pane" on page 30 for more information.
Permission pane	Lists the permission tokens configured for a selected Enterprise user or permission group. See "Permission pane" on page 30 for more information.

Table 4 Parts of the Access Control Administration window (continued)

Part	Description
Permission Groups pane	Lists the permission groups configured. See "Permission Groups pane" on page 30 for more information.
Status bar	Provides information about current activity in the window, including the Enterprise NMS server host name, user name, and whether Access Control Administration features are enabled or disabled. See "Status bar" on page 31 for more information.

Menu bar and toolbar

The Access Control Administration menu bar and toolbar let you configure access permissions, change the appearance of the Access Control Administration window, get online Help, and exit the window.

If you open Access Control Administration in a Web browser, the menu bar does not display. Instead, you use the Menu tool on the toolbar to open a shortcut menu of Access Control Administration menus.

Table 5 describes the menu bar commands and toolbar buttons.

Table 5 Access Control Administration menu commands and toolbar buttons

Menu	Command	Toolbar button	Description
File	Exit		Exits Access Control Administration.
View	Display Toolbar		Turns the display of the toolbar on and off in the Access Control Administration window.
	Display Status Bar		Turns the display of the status bar on and off in the Access Control Administration window.
	Look and Feel		Provides options for choosing a familiar window interface Access Control Administration window interface. You can choose Metal, CDE/Motif, or Microsoft Windows as the user interface type.

Table 5 Access Control Administration menu commands and toolbar buttons (continued)

Menu	Command	Toolbar button	Description
Actions	Add/Remove Enterprise Users		Opens the Add/Remove Enterprise Users dialog box, where you can add or remove users who can log in to Enterprise NMS. See “Adding Enterprise NMS users” on page 33, and “Removing Enterprise users” on page 34 for more information.
	Add Permission Group		Opens the Add Permission Group dialog box, where you can create a new permission group. See “Adding permission groups” on page 38 for more information.
	Attach/Detach Permission		Opens the Attach/Detach Permissions dialog box, where you can attach and detach individual permission tokens to or from users or permission groups. See “Attaching and detaching permissions” on page 36 for more information.
	Attach Permission Group		Opens the Attach Permission Group dialog box, where you can attach a permission group to an Enterprise NMS user. See “Attaching permission groups” on page 40 for more information.
	Assign View Domain		Opens the Assign View Domains and Services dialog box to let you assign view domains to Enterprise NMS users. See “Assigning view domains to Enterprise NMS users” on page 42 for more information.
	Assign Services		Opens the Assign View Domains and Services dialog box to let you assign services to Enterprise NMS users. See “Assigning services to Enterprise NMS users” on page 44 for more information.
	Access Control Switch		Opens the Access Control Switch dialog box, where you can enable or disable access control. See “Enabling and disabling access control” on page 32, for more information.
Help	Access Control Help		Opens the Access Control Administration window Help.
	Using Help		Displays a Help topic describing how to use the Access Control Administration window Help system.
	About Access Control Administration		Displays the startup screen for the Access Control Administration window. This screen includes copyright and version information.

Enterprise Users pane

The Enterprise Users pane, located in the upper left area of the Access Control Administration window, lists all system users configured for Enterprise NMS access.

Permission pane

The Permission pane, located on the right side of the Access Control Administration window, lists the Enterprise NMS application tokens currently set for a user or permission group. The table in the Permission pane contains the token name, current permission setting, and a brief description of each token.

To view the tokens configured for a user:

➔ Click the user name in the Enterprise Users pane.

To view the tokens configured for a permission group:

➔ Click the group name in the Permission Groups pane.

To change the permission setting of a listed token:

1. Right-click the permission setting.

   A shortcut menu opens.

2. Choose Read/Write or Read Only.

Permission Groups pane

The Permission Groups pane, located in the lower left area of the Access Control Administration window, lists configured permission groups.

Select a permission group by clicking the group name. The current permission settings for that group are displayed in the Select a permission group by clicking the group name. The current permission settings for that group are displayed in the Permission pane.

The default groups are:

- ENTERPRISE_ADMIN (all tokens read/write)
- ENTERPRISE_VIEW (all tokens read-only)

Status bar

The status bar, located along the bottom of the Access Control Administration window, lists:

- The result of the most recent operation (usually this value is “OK”)
- The Enterprise NMS server host name
- The current user name
- Whether Access Control Administration features are enabled or disabled

Working with Access Control Administration

The following sections describe how to work with Access Control Administration:

- “Enabling and disabling access control,” next
- “Adding Enterprise NMS users” on page 33
- “Removing Enterprise users” on page 34
- “Setting user permissions” on page 35
- “Changing permission settings” on page 36
- “Attaching and detaching permissions” on page 36
- “Adding permission groups” on page 38
- “Attaching permission groups” on page 40
- “Changing permission groups” on page 41
- “Assigning view domains to Enterprise NMS users” on page 42
- “Assigning services to Enterprise NMS users” on page 44
- “Changing the look and feel of the window” on page 45

Enabling and disabling access control

Access control is disabled by default. With access control disabled, any user with a valid system user ID can access any Enterprise NMS component. To use Access Control Administration features you must turn on access control.

Note: Only Enterprise NMS access administrators or users with read/write access control permission to the ACCESS_CONTROL token can enable access control.

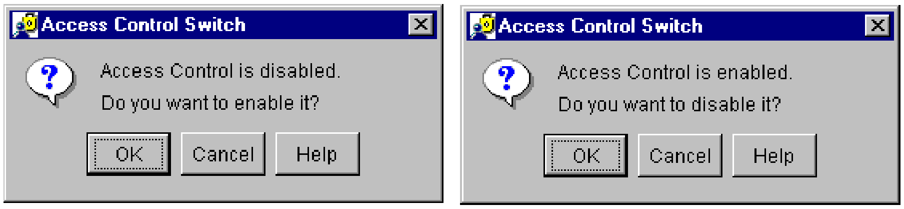
To enable access control on the connected Enterprise NMS server:

1 If you have not already done so, start Access Control Administration. For more information, see “Starting Access Control Administration” on page 25.

2 On the Access Control Administration toolbar, click Access Control Switch.

The Access Control Switch dialog box (Figure 2) opens. The dialog box shows the whether access control is enabled or disabled, and prompts whether you want to change it.

Figure 2 Access Control Switch dialog box (enabled and disabled)



Access Control Switch

Access Control is disabled.
Do you want to enable it?

Access Control Switch

Access Control is enabled.
Do you want to disable it?

For detailed information about the Access Control Switch dialog box, click Help in the dialog box.

3 Click OK to change the state of access control, or click cancel to leave it as it is.

Note: After you enable access control, only root and Administrator can access Enterprise NMS. You must add users and configure their permission tokens to allow access to other Enterprise users.

If you disable access control after configuring permission settings, the most recent configuration is active if you re-enable access control.

Note: After you change the access control state, users who are logged into InfoCenter and Autotopology Manager are prompted to log out and reconnect.

Adding Enterprise NMS users

When you first enable access control, the default Enterprise NMS users are Administrator and root. No other system user can log in to view or modify Enterprise NMS database objects.

Note: Only users with read/write permission to the ACCESS_CONTROL token can enable access control.

To add an Enterprise NMS user:

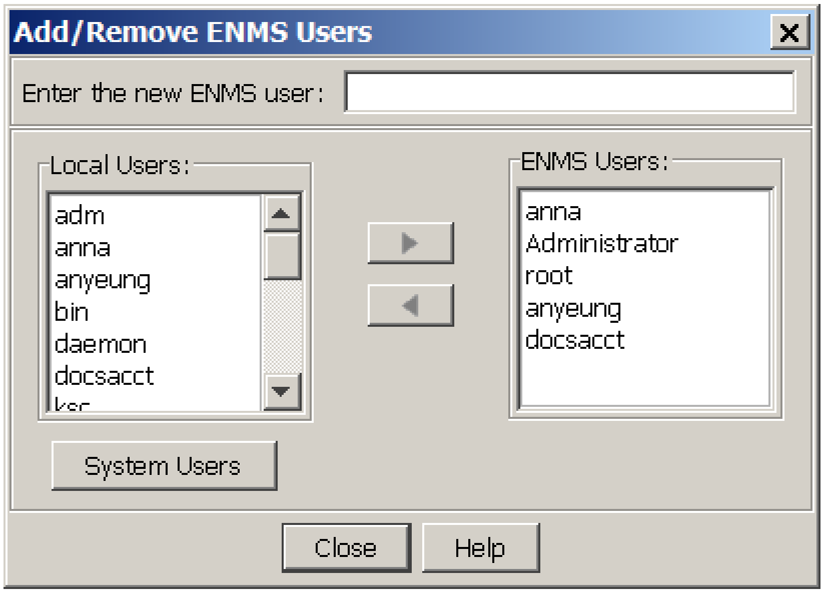
1 Open the Access Control Administration window.

For more information, see "Starting Access Control Administration" on page 25.

2 Open the Add/Remove Enterprise Users dialog box (Figure 3) in one of the following ways:

- From the Access Control Administration menu bar, choose Actions > Add/Remove Users.
- On the toolbar, click Add/Remove Users.

Figure 3 Add/Remove Enterprise Users dialog box



For detailed information about the Add/Remove Enterprise Users dialog box, click Help in the dialog box.

3 Type a user name or select a user to add from the Local Users or System Users list.

4 Click the > button between the two lists to move the selected user into the Enterprise Users list.

5 When you are done adding users, click Close.

6 Set access permissions for the new user.

See “Setting user permissions” on page 35 for more information.

Removing Enterprise users

When you delete an Enterprise user, the user can no longer access any Enterprise NMS applications unless you disable Access Control Administration.

➡ **Note:** Only users with read/write permission to the ACCESS_CONTROL token can remove an Enterprise user. You cannot delete Administrator, root, or your own user name.

To remove an Enterprise user:

1 Open the Access Control Administration window.

For more information, see "Starting Access Control Administration" on page 25.

2 Open the Add/Remove Enterprise Users dialog box in one of the following ways:

- From the Access Control Administration menu bar, choose Actions > Add/Remove Users.
- On the toolbar, click Add/Remove Users.

For detailed information about the Add/Remove Enterprise Users dialog box, click Help in the dialog box.

3 Select a user in the Enterprise Users pane.

4 Click the < button between the two lists to remove the selected user from the Enterprise Users list.

5 Click OK.

Setting user permissions

After you add an Enterprise NMS user, you must add tokens for the Enterprise NMS components the user can access.

Choose one of the following methods:

- Attach the preconfigured set of tokens in a permission group.

  To attach a permission group to an Enterprise user, see "Attaching permission groups" on page 40.

- Attach the token for each Enterprise NMS application the user will access.

  To attach user tokens individually, see "Attaching and detaching permissions" on page 36.

➡ **Note:** Only users with read/write permission to the ACCESS_CONTROL token can configure access permissions.

Changing permission settings

After you assign tokens for a user or permission group, you can change the read-only or read/write permission value of each token.

Note: Only users with read/write permission to the ACCESS_CONTROL token can configure access permissions.

To change the permission setting of a configured token:

1. Open the Access Control Administration window.

   For more information, see "Starting Access Control Administration" on page 25.

2. Select an Enterprise user in the Enterprise Users pane or a permission group in the Permission Groups pane.
3. Select a token in the Permission pane.
4. To the right of the token name, right-click in the Permission column.

   A shortcut menu opens.

5. Choose Read/Write or Read Only.

Note: To grant access to any InfoCenter component, you must also grant access to the IC and IC_ADMIN tokens. To restrict user access to components, be sure to deny read/write access to the ACCESS_CONTROL token for that user. Otherwise, the user can set their own permissions in the Access Control Administration window.

Attaching and detaching permissions

To configure access permissions for Enterprise users and permission groups, do the following:

- Attach or detach the permission tokens for Enterprise NMS applications.
- Set the attached tokens to read-only or read/write access.

To attach and detach permission tokens for an Enterprise user or permission group:

1 Open the Access Control Administration window.

For more information, see "Starting Access Control Administration" on page 25.

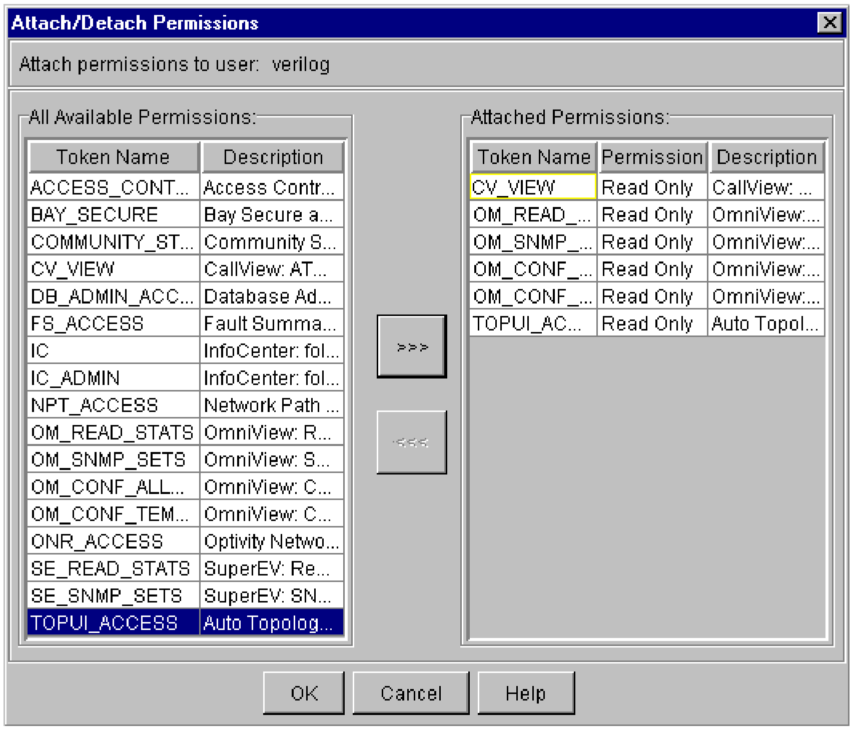
Select a user in the Enterprise Users pane or a permission group in the Permission Groups pane.

➡ **Note:** Only users with read/write permission to the ACCESS_CONTROL token can configure access permissions.

2 Open the Attach/Detach Permissions dialog box (Figure 4) in one of the following ways:

- From the Access Control Administration menu bar, choose Actions > Attach/Detach Permissions.
- On the toolbar, click Attach/Detach Permissions.

Figure 4 Attach/Detach Permissions dialog box.



Attach/Detach Permissions

Attach permissions to user: verilog

All Available Permissions:

Token Name	Description
ACCESS_CONT...	Access Contr...
BAY_SECURE	Bay Secure a...
COMMUNITY_ST...	Community S...
CV_VIEW	CallView: AT...
DB_ADMIN_ACC...	Database Ad...
FS_ACCESS	Fault Summa...
IC	InfoCenter: fol...
IC_ADMIN	InfoCenter: fol...
NPT_ACCESS	Network Path ...
OM_READ_STATS	OmniView: R...
OM_SNMP_SETS	OmniView: S...
OM_CONF_ALL...	OmniView: C...
OM_CONF_TEM...	OmniView: C...
ONR_ACCESS	Optivity Netwo...
SE_READ_STATS	SuperEV: Re...
SE_SNMP_SETS	SuperEV: SN...
TOPUI_ACCESS	Auto Topolog...

Attached Permissions:

Token Name	Permission	Description
CV_VIEW	Read Only	CallView: ...
OM_READ_...	Read Only	OmniView:...
OM_SNMP_...	Read Only	OmniView:...
OM_CONF_...	Read Only	OmniView:...
OM_CONF_...	Read Only	OmniView:...
TOPUI_AC...	Read Only	Auto Topol...

For detailed information about the Attach/Detach Permissions dialog box, click Help in the dialog box.

3 Attach or detach tokens.

- To attach a token, select the token in the All Available Permission pane; then, click the >>> button.
- To detach a token, select the token in the Attached Tokens pane; then, click the <<< button.

Adding permission groups

You create permission groups to establish preconfigured sets of permission tokens. You can then attach the permission group to Enterprise users who have similar access requirements rather than attaching each permission token to each user.

The default ENTERPRISE_ADMIN permission group contains all of the available tokens set to read/write access. The default ENTERPRISE_VIEW permission group contains all tokens set to read-only.

➡ **Note:** Only users with read/write access to the ACCESS_CONTROL token can configure permission groups.

To add a permission group:

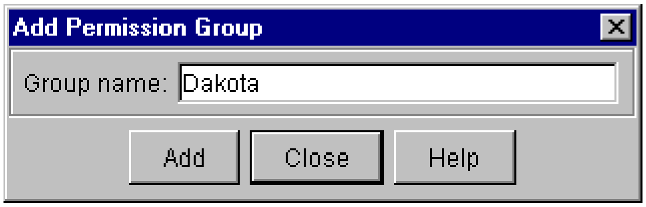
1 Open the Access Control Administration window.

For more information, see "Starting Access Control Administration" on page 25.

2 Open the Add Permission Group dialog box (Figure 5) in one of the following ways:

- From the Access Control Administration menu bar, choose Actions > Add Permission Group.
- On the toolbar, click Add Permission Group.

Figure 5 Add Permission Group dialog box



Add Permission Group

Group name: Dakota

For detailed information about the Add Permission Group dialog box, click Help in the dialog box.

3 Enter a group name.

4 Click Add.

The new group name is now displayed in the Permission Groups pane.

5 Attach the permission tokens for this group.

See "Attaching and detaching permissions" on page 36.

Attaching permission groups

Attach a permission group to quickly assign a preconfigured set of tokens to one or more Enterprise user. After you attach the permission group, you can customize the configured permissions for each user as necessary.

> **Note:** Only users with read/write permission to the ACCESS_CONTROL token can attach a permission group. Group permissions override any previously configured user tokens.

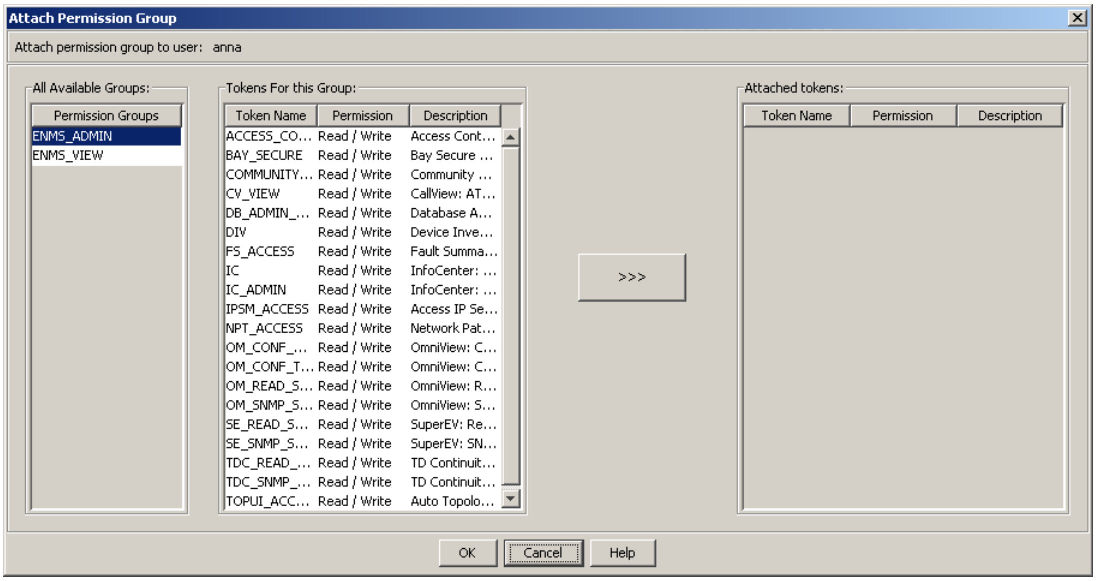
To attach a permission group to an Enterprise user:

1 Select a user in the Enterprise Users pane.

2 Open the Attach Permission Group dialog box (Figure 6) in one of the following ways:

- From the Access Control Administration menu bar, choose Actions > Attach Permission Group.
- In the toolbar, click Attach Permission Group.

Figure 6 Attach Permission Group dialog box



Attach permission group to user: anna

Permission Groups
ENMS_ADMIN
ENMS_VIEW

Token Name	Permission	Description
ACCESS_CO...	Read / Write	Access Cont...
BAY_SECURE	Read / Write	Bay Secure ...
COMMUNITY...	Read / Write	Community ...
CV_VIEW	Read / Write	CallView: AT...
DB_ADMIN_...	Read / Write	Database A...
DIV	Read / Write	Device Inve...
FS_ACCESS	Read / Write	Fault Summa...
IC	Read / Write	InfoCenter: ...
IC_ADMIN	Read / Write	InfoCenter: ...
IPSM_ACCESS	Read / Write	Access IP Se...
NPT_ACCESS	Read / Write	Network Pat...
OM_CONF_...	Read / Write	OmniView: C...
OM_CONF_T...	Read / Write	OmniView: C...
OM_READ_S...	Read / Write	OmniView: R...
OM_SNMP_S...	Read / Write	OmniView: S...
SE_READ_S...	Read / Write	SuperEV: Re...
SE_SNMP_S...	Read / Write	SuperEV: SN...
TDC_READ_...	Read / Write	TD Continuit...
TDC_SNMP_...	Read / Write	TD Continuit...
TOPUI_ACC...	Read / Write	Auto Topolo...

Token Name	Permission	Description

For detailed information about the Attach Permission Group dialog box, click Help in the dialog box.

3 Select a group in the All Available Groups list.

4 Click the >>> button to move the tokens for the selected group to the Attached tokens list.

The Tokens For This Group pane lists all available tokens and their current permission settings. The Attached Tokens pane lists the tokens currently attached to the selected permission group.

5 If necessary, customize the permission group.

See “Changing permission groups” on page 41 for more information.

6 Click OK.

Changing permission groups

After you create a permission group and attach its tokens, you can modify the permission group by:

- Attaching or detaching additional tokens

  See “Attaching and detaching permissions” on page 36 for more information.

- Changing the permission level of one or more tokens

  See “Changing permission settings” on page 36 for more information.

Note: Only users with read/write permission to the ACCESS_CONTROL token can configure permission groups.

Assigning view domains to Enterprise NMS users

Enterprise NMS administrators can assign specific view domains to specific Enterprise NMS users. Users can use Enterprise NMS to view and manage only those network elements within their view domains. See *Using Nortel Enterprise NMS* (part number 207569-G) for more information about creating and changing view domains.

➡ **Note:** In order to assign view domains to Enterprise NMS users:

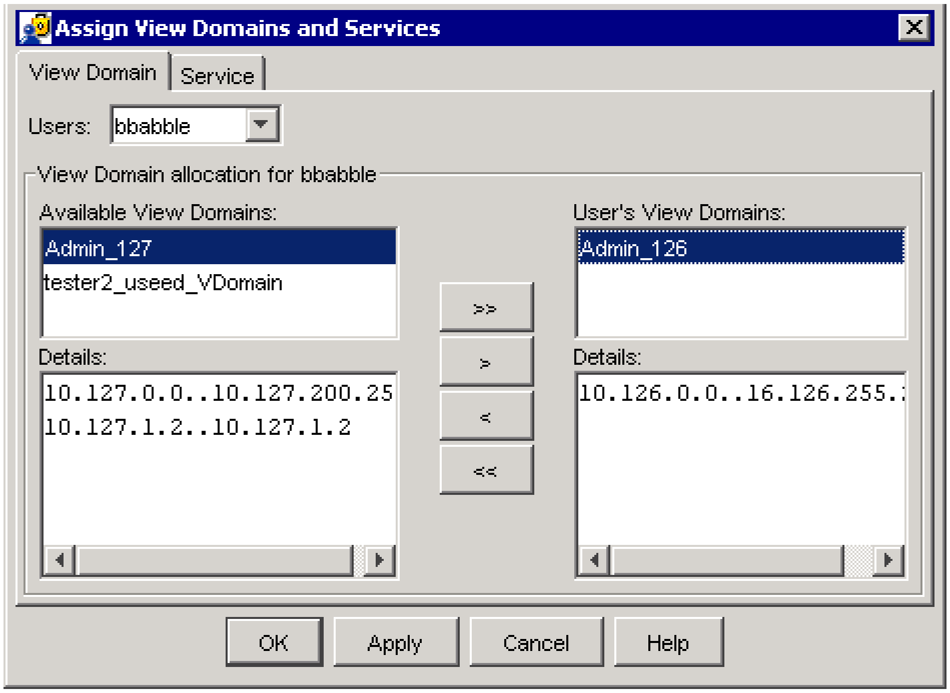
- Access Control must be enabled. See “Enabling and disabling access control” on page 32 for more information.
- You must have read/write permission to the VIEW_DOMAIN_MGMT token to assign view domains. See “Access permission tokens” on page 24 for more information.

To assign view domains to Enterprise NMS users:

1 In Access Control Administrator, choose Actions > Assign view domain.

The Assign View Domains and Services dialog box opens with the View Domain tab forward (Figure 7).

Figure 7 Assign View Domains and Services dialog box (View domain tab shown)



Assign View Domains and Services

Users: bbabble

View Domain allocation for bbabble

Available View Domains:

Admin_127
tester2_useed_VDomain

Details:

```
10.127.0.0..10.127.200.25
10.127.1.2..10.127.1.2
```

User's View Domains:

Admin_126

Details:

```
10.126.0.0..16.126.255.:
```

2 From the Users menu, choose the user to whom you want to assign the view domain.

3 In the Available View Domains list, choose one or more view domains by clicking or with Shift+Click and Ctrl+Click.

4 Use the >> and > buttons to move the selected view domains from the Available View Domains list to the User's View Domains list.

5 Click OK to apply your changes and close the dialog box, or click Apply to apply your changes but leave the dialog box open.

The view domains are automatically added to the user views. Users who are connected to InfoCenter see the changes without having to log-off from InfoCenter.

Assigning services to Enterprise NMS users

Note: In order to assign view domains to Enterprise NMS users:

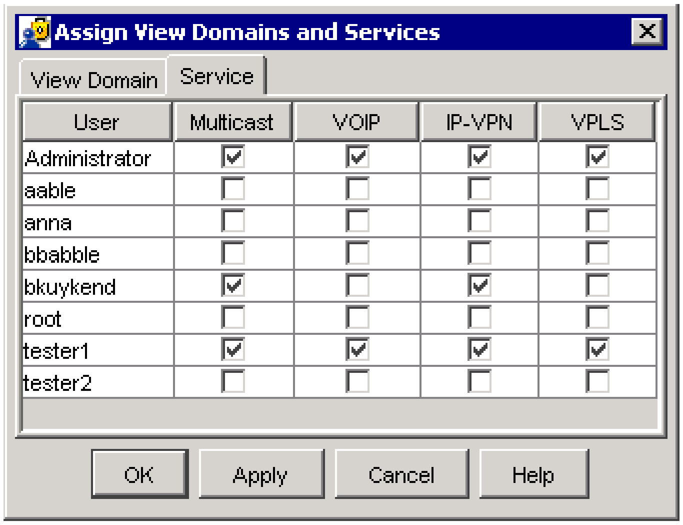
- Access Control must be enabled. See "Enabling and disabling access control" on page 32 for more information.
- You must have read/write permission to the SERVICE_ASSIGN token to assign view domains. See "Access permission tokens" on page 24 for more information.

To assign services to Enterprise NMS users:

1 In Access Control Administrator, choose Actions > Assign service.

The Assign View Domains and Services dialog box opens with the Service tab forward (Figure 8).

Figure 8 Assign View Domains and Services dialog box (Service tab shown)



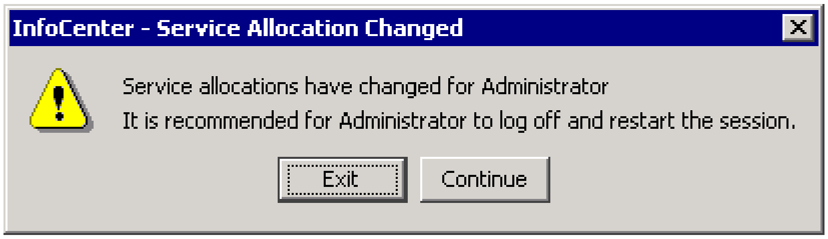
User	Multicast	VOIP	IP-VPN	VPLS
Administrator	☑	☑	☑	☑
aable	□	□	□	□
anna	□	□	□	□
bbabble	□	□	□	□
bkuykend	☑	□	☑	□
root	□	□	□	□
tester1	☑	☑	☑	☑
tester2	□	□	□	□

2 Use the check boxes in the Service tab table to assign services to Enterprise NMS users.

3 Click OK to apply your changes and close the dialog box, or click Apply to apply your changes but leave the dialog box open.

When you change service allocations for any Enterprise NMS users that are using InfoCenter, the Service Allocation Changed dialog box (Figure 9) opens to alert them to the change. They must exit and restart InfoCenter in order to view or manage the new services.

Figure 9 Service Allocation Changed dialog box



InfoCenter - Service Allocation Changed

Service allocations have changed for Administrator
It is recommended for Administrator to log off and restart the session.

Changing the look and feel of the window

Access Control Administration lets you change the look and feel of the Access Control Administration window to best match the operating system under which it is running.

To change the look and feel of the Access Control Administration window:

1 From the Access Control Administration menu bar, choose View > Look and feel.

The Look and Feel shortcut opens.

2 Choose the selection that best matches your computing environment.

Troubleshooting Access Control Administration

The following sections describe how to troubleshoot Access Control Administration problems:

- "Resolving problems," next
- "Error messages" on page 46

Resolving problems

Table 6 suggests techniques for resolving problems or interpreting unexpected results.

Table 6 Access Control Administration problems and resolutions

Problem	Resolution
An Enterprise user cannot launch InfoCenter.	Enterprise users require access to launch InfoCenter. Log in as an Enterprise Administrator to add InfoCenter to the user's list of access tokens.
An Enterprise user cannot open InfoCenter Administration menus.	Log in as an Enterprise Administrator to add IC_ADMIN to the user's list of access tokens.
The Access Control Administration window opens empty, without default permission tokens or access administrator users in the User and Permission panes.	The application control database was not properly set up during postinstallation. Contact the Technical Support Center. Access Control Administration requires the following items to operate properly: • Db/AppControlDB.db/access.schema • registration/webpotsrvr/access_admin.reg
The toolbar buttons have the wrong background color.	When you drag the Access Control Administration toolbar to a different location and then change the Look and Feel setting, the toolbar buttons sometimes retain the color of the previous setting. The toolbar button background color has no effect on the operation of the application.

Error messages

Table 7 describes the error messages you might encounter while using the Access Control Administration window.

Table 7 Common Access Control Administration error messages

Error message	Description
`Access Admin. cannot remove this user.`	You cannot remove root or Administrator users.
`You may not change any of the superuser permissions.`	You cannot remove or change the permission setting for any root or Administrator tokens.

Table 7 Common Access Control Administration error messages (continued)

Error message	Description
`Login name starting with blanks or trailing blanks. Extra blanks are removed.`	You cannot use spaces when specifying an Enterprise username.
`Login name must be less than 50 characters. Try again.`	When you add an Enterprise user, you cannot use more than 50 characters to specify the user name.
`Permission group name must be less than 50 characters. Try again.`	When you add a permission group, you cannot use more than 50 characters to specify the group name.

Chapter 4
Specifying access to devices with the Community Strings Editor

This chapter is divided into the following major sections:

- "Community Strings Editor overview," next
- "Getting started with the Community Strings Editor" on page 50
- "Working with the Community Strings Editor" on page 64
- "Troubleshooting the Community Strings Editor" on page 87

Community Strings Editor overview

The Community Strings Editor lets you add, delete, modify, or rearrange non-default SNMP read and read/write community strings that control access to your network devices. Use the Community Strings Editor to manage non-default community strings, so that Enterprise NMS applications can discover and access devices that use those community strings.

You can also use the Community Strings Editor to import and export community strings to and from files. This feature lets you easily exchange lists of community strings with other Enterprise NMS server, or with HP OpenView platforms. For more information, see "Importing a community strings file" on page 79 and "Exporting a community strings file" on page 82.

The Community Strings Editor also supports the SNMPv3 user security model (USM) that lets you administer user security to accommodate your network requirements. The USM lets you specify authentication and privacy security features for:

- Each user
- Multiple users for a specific IP or a range of IP addresses
- A single Enterprise user for trap registration

The Community Strings Editor stores information about community strings and security in the Enterprise NMS topology database.

Getting started with the Community Strings Editor

The following sections introduce the Community Strings Editor and tell how to get started using it:

- "About community strings," next
- "Default community strings" on page 52
- "About user security" on page 54
- "Starting the Community Strings Editor" on page 56
- "Access permissions for Community Strings Editor" on page 57
- "Community Strings Editor window" on page 58
- "IP address syntax" on page 52
- "Understanding wildcards" on page 53

About community strings

In an SNMP network, SNMP community strings control management access to network devices.

An SNMP community is a logical relationship between SNMP agent software running on network devices and one or more SNMP management stations. Each device agent limits access to its management information base (MIB) by defining read only and read/write communities with specific ASCII text strings as passwords—the SNMP community strings.

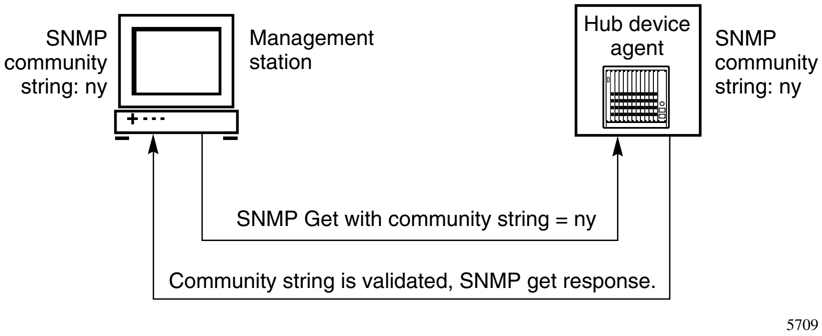
- Read-only community members can view configuration and performance information in the MIB.
- Read/write community members can view and change configuration and performance data.

Communication between an SNMP management station and managed devices works as follows:

- When an application needs information from a managed device, it reads the management station community strings database, finds a match for the device IP address, and retrieves the community string.
- The management station sends an SNMP message to the device that includes the community string.
- The device agent verifies that the management station is using the correct read-only or read/write password (community string).
- If the password is correct, the agent allows the management station read or write access to the device management information base (MIB). Otherwise, it denies access.

Figure 10 shows this process.

Figure 10 Community strings and SNMP


SNMP community string: ny
Management station
Hub device agent
SNMP community string: ny
SNMP Get with community string = ny
Community string is validated, SNMP get response.
5709

Default community strings

Many network devices are configured with default community strings:

- The default read community string is Public.

  When a device read community string is set to Public, every management station has read access to the device MIB.
- The default write community string is Private.

  When a device read/write community string is set to Private, the device denies write access to all management stations.

To configure the Enterprise NMS server with write access to a particular device MIB, you must change the default Write community string. First change the community string for the device agent, then add or change the Enterprise NMS server community string for that device.

After you initially set the SNMP community strings for your network, you may want to change them periodically for enhanced security.

IP address syntax

Each 32-bit IP address contains four octet values that together specify the network address ID and the host ID for a device.

Use the following format to specify IP addresses in the community strings table or in the IP Range Table:

<*value*>.<*value*>.<*value*>.<*value*>

where each <*value*> is one of the following:

- An integer 0 to 255.
- A range of valid integer values. For example, 120-127.
  The dash (-) is the only valid character to indicate a range.
- An asterisk (*) wildcard to match the range 0-255.
  The asterisk (*) is the only valid wildcard character.

IPv6 addresses are also supported, though wildcards are not.

Understanding wildcards

When you configure a community string, you can specify a wildcard as one or more octet in the device IP address. For example, use wildcards to specify a group of network or host IDs that use the same community string.

To communicate with a managed device, Enterprise NMS reads the community strings table to find a match for the IP address. A wildcard matches all values for a particular octet. You can specify 1 to 4 wildcards in an IP address. The wildcard character is the asterisk (*).

How you order IP addresses within the IP Range Table affects the way Enterprise matches address entries to hosts in the network. Address matching begins with the first entry in the table. Make sure that IP addresses that contain wildcards do not overlap or exclude other IP address entries in the table.

Table 8 shows some examples of how IP address matching works with and without wildcards.

Table 8 Community string matching examples

IP address	Description
134.177.125.31	Matches only the specified IP address.
134.177.125.1-31	Matches all addresses in the range 134.177.125.1 to 134.177.125.31.
134.177.125.*	Matches all addresses in the range 134.177.125.1 to 134.177.125.255.
134.177.125-128.*	Matches all addresses in the range 134.177.125.* to 134.177.128.*
..*.*	Matches all addresses. This is usually the last entry in the community strings table, used to specify default community strings for devices without specific entries in the table.

About user security

The Community Strings Editor implements the SNMPv3 USM defined in RFC 2574, and supports three important USM security services: authentication, privacy, and access control. To deliver these services in a flexible and efficient manner, the USM introduces the concept of a principal, which is the entity on whose behalf services are provided or processing takes place.

A principal can be any of the following:

- An individual acting in a particular role
- A set of individuals, with each acting in a particular role
- An application or set of applications, or a combination thereof

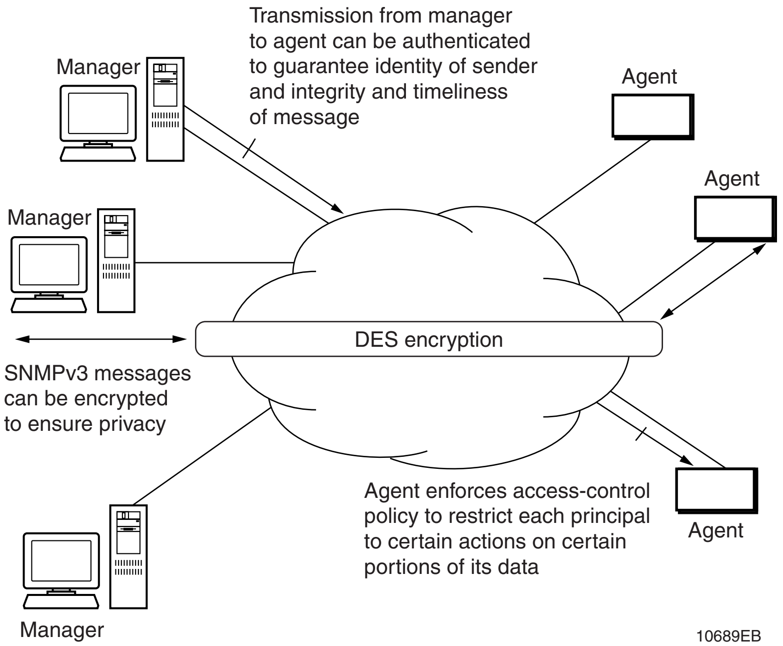
In essence, a principal operates from a management station and issues SNMP commands to agent systems. The identity of the principal and the target agent together determine the security features that are invoked, including:

- Authentication
- Privacy
- Access control

The use of principals allows security policies to be tailored to the specific principal, agent, and information exchange (Figure 11), and gives security managers considerable flexibility in assigning network authorization to users.

The principal in the USM is represented by a user, who is identified by user name.

Figure 11 SNMPv3 security features


Manager
Transmission from manager to agent can be authenticated to guarantee identity of sender and integrity and timeliness of message
Agent
Agent
Manager
DES encryption
SNMPv3 messages can be encrypted to ensure privacy
Agent enforces access-control policy to restrict each principal to certain actions on certain portions of its data
Agent
Manager
10689EB

Understanding user security services

The Community Strings Editor lets you administer authentication and privacy security services to protect your network against the following threats:

- Modification of Information—An entity could alter an in-transit message generated by an authorized entity in such a way as to effect unauthorized management operations, including the setting of object values.
- Masquerade—Unauthorized management operations attempted by an entity masquerading as an authorized entity
- Message Stream Modification—SNMP is designed to operate over a connectionless transport protocol. There is a threat that SNMP messages could be reordered, delayed, or replayed (duplicated) to effect unauthorized management operations.
- Disclosure—An entity could observe exchanges between a manager and an agent and thereby learn the values of managed objects and learn of trap events.

Community strings security does not provide protection against the threats listed above.

Starting the Community Strings Editor

To start the Community Strings Editor:

1 Take one of the actions shown in Table 9.

Table 9 Starting Community Strings Editor

To start Community Strings Editor from:	**Do this:**
InfoCenter	Choose Admin > Community Strings **Note:** If the Community Strings Editor menu command is disabled, it means you do not have the proper access permissions to use Community Strings Editor.
Windows Start menu	Choose Start > Programs > Enterprise > CommunityString

Windows command prompt	**`cd %lnmshome%\bin`**
	`comstrings`

UNIX command prompt	**`cd $LNMSHOME/bin`**
	`comstrings`

Web browser	Point your Web browser to: **`http://`***`[IP or hostname of Enterprise NMS server]`* Click the Community Strings Editor icon on the Enterprise Web page. **Note:** You can use your Web browser's Bookmark or Favorites feature to bookmark the Community Strings Editor application. Doing so saves the URL for Community Strings Editor.

If you are not starting Community Strings Editor from InfoCenter, the Connect to Enterprise Server dialog box opens.

2 If prompted, enter your login information and click OK.

The Community Strings Editor window opens.

Access permissions for Community Strings Editor

When access control is enabled on the Enterprise NMS server, the Community Strings Editor requires the following permission tokens:

- IC
- IC_ADMIN
- COMMUNITY_STRINGS

Table 10 shows the level of access a user has with read-only, read/write, or no access to the three required permission tokens.

Table 10 Access permissions

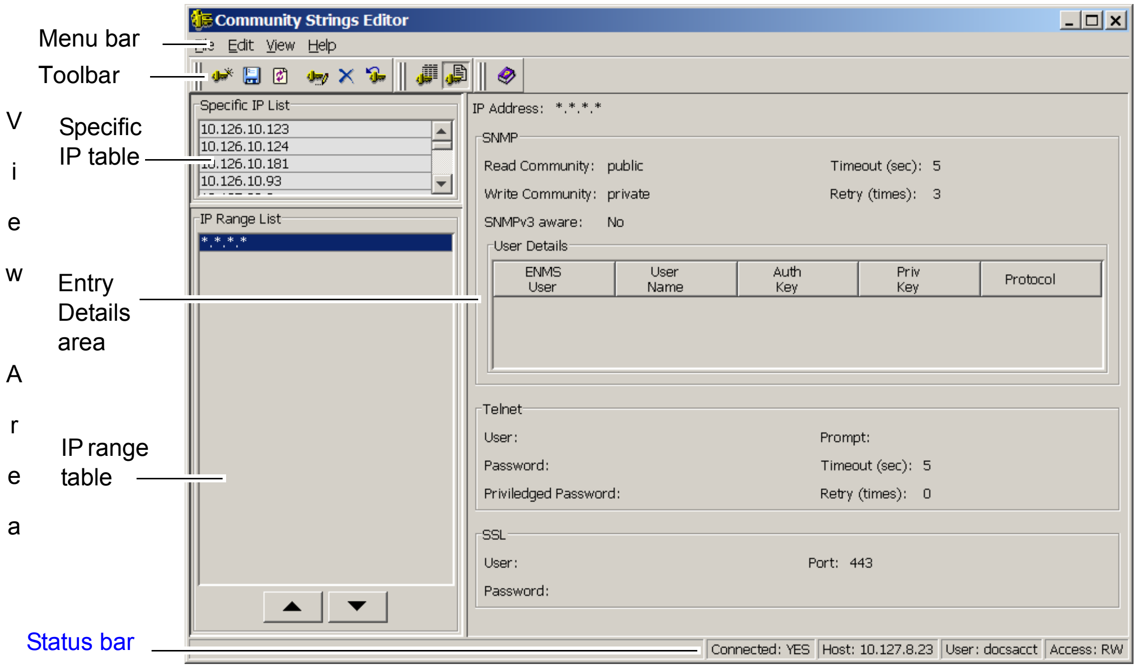
Permission	Access
None	No access. The Community String Editor window does not open.
Read only	User can view the Community strings table, but cannot add, delete, modify, or change the order of entries. Import, export, and save commands are also disabled.
Read/write	User has full access to all features of the Community Strings Editor.

Community Strings Editor window

The Community Strings Editor window has two views: Individual view and Table view.

Figure 12 shows the Individual view.

Figure 12 Community Strings Editor—Individual view



10.126.10.123
10.126.10.124
10.126.10.181
10.126.10.93

..*.*

IP Address: *.*.*.*

SNMP

Read Community: public
Timeout (sec): 5
Write Community: private
Retry (times): 3
SNMPv3 aware: No

User Details

ENMS User	User Name	Auth Key	Priv Key	Protocol

Telnet

User:
Prompt:
Password:
Timeout (sec): 5
Priviledged Password:
Retry (times): 0

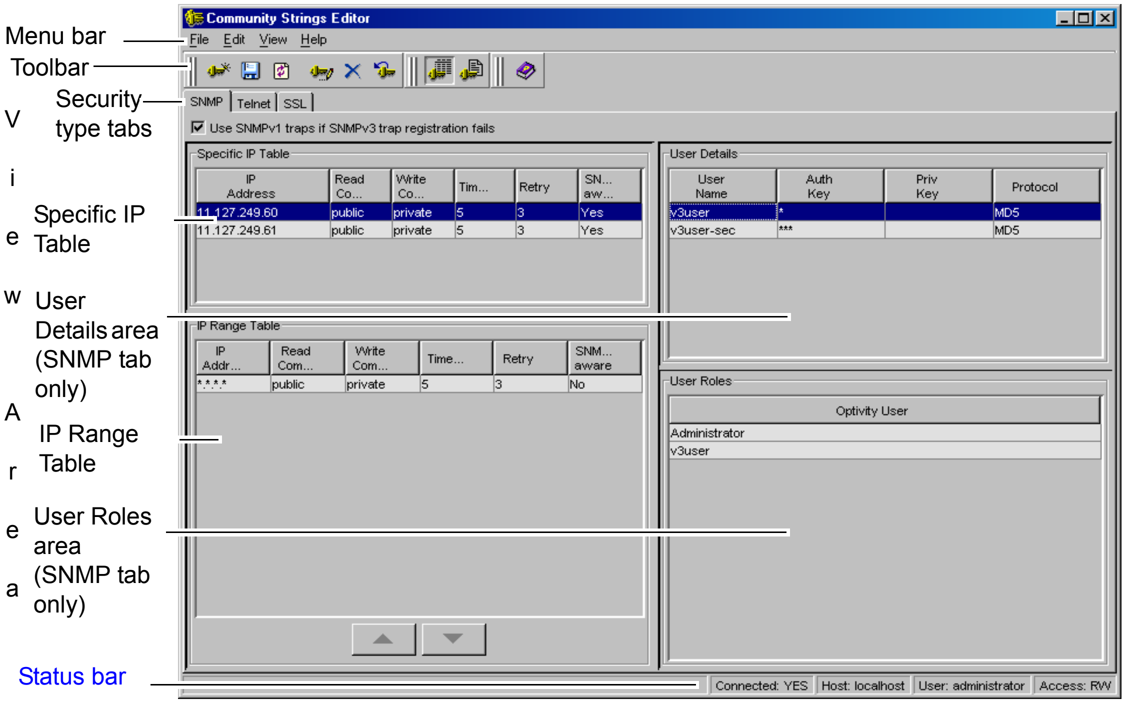
SSL

User:
Port: 443
Password:

Connected: YES | Host: 10.127.8.23 | User: docsacct | Access: RW

Figure 14 shows the Table view.

Figure 13 Community Strings Editor window—Table view



☑ Use SNMPv1 traps if SNMPv3 trap registration fails

Specific IP Table

IP Address	Read Co...	Write Co...	Tim...	Retry	SN... aw...
11.127.249.60	public	private	5	3	Yes
11.127.249.61	public	private	5	3	Yes

IP Range Table

IP Addr...	Read Com...	Write Com...	Time...	Retry	SNM... aware
..*.*	public	private	5	3	No

User Details

User Name	Auth Key	Priv Key	Protocol
v3user	*		MD5
v3user-sec	***		MD5

User Roles

Optivity User
Administrator
v3user

Connected: YES | Host: localhost | User: administrator | Access: RW

Table 11 describes the parts of the Community Strings Editor window.

Table 11 Parts of the Community Strings Editor window

Part	Description
Menu bar	Provides access to all available Community Strings Editor commands. See "Menu bar and toolbar" on page 60 for more information.
Toolbar	Provides quick access to commonly used Community Strings Editor commands. See "Menu bar and toolbar" on page 60 for more information.

Table 11 Parts of the Community Strings Editor window (continued)

Part	Description
View area	Shows you the community string entries in either the Individual view or the Table view. See “Table view” on page 62 and “Individual view” on page 63 for more information.
Status bar	Displays information about the selected menu bar command, the server hostname, user name and access privileges. See “Status bar” on page 64 for more information.

Menu bar and toolbar

The Community Strings Editor menu bar and toolbar contain commands that let you add and manipulate SNMP non-default community strings that are stored in the Enterprise application control database.

Table 12 shows the menu names, command names, toolbar buttons, and command descriptions.

Table 12 Menu bar commands and toolbar buttons

Menu	Command	Toolbar button	Description
	Menu	📋	Opens the Community Strings Editor menu in a Web browser.
File	Import Data		Imports a new community strings file, overwriting any existing community strings configured for the Enterprise NMS server. You can import community strings files in both Enterprise and HP OpenView* .CSV file format. See “Importing a community strings file” on page 79 for more information.
	Export Data		Exports the existing community strings information in the Enterprise database to a file to the server file system. You can export community strings files in both Enterprise and HP OpenView.CSV file format. See “Exporting a community strings file” on page 82 for more information.
	Save	💾	Saves all community string entry changes that you have made in the Community Strings Editor window to the Enterprise application control database. See “Saving changes” on page 72 for more information.
	Exit		Closes the Community Strings Editor window.

Table 12 Menu bar commands and toolbar buttons (continued)

Menu	Command	Toolbar button	Description
Edit	New		Opens the Configure Community Strings Entry dialog box to let you create a new community strings entry. See "Adding a new community string entry" on page 65 for more information.
	Edit		Opens the selected entry in a Configure Community Strings Entry dialog box to let you edit the entry. See "Modifying a community string entry" on page 68 for more information.
	Delete	✕	Deletes the selected community strings entry. See "Deleting a community string entry" on page 69 for more information.
	Reset		Discards all of the changes you have made since the last save. See "Resetting changes" on page 71 for more information.
	Refresh		Refreshes the Community Strings Editor display with current information from the Enterprise NMS database. Also discards all of the changes you have made since the last save. See "Refreshing the display" on page 71 for more information.
View	Display Toolbar		Shows or hides the toolbar.
	Display Status Bar		Shows or hides the status bar.
	View Type		Opens a submenu that lets you choose either of two view types: • Table • Individual
	Look and Feel		Changes the appearance of the Community Strings Editor window. A submenu opens—Metal, CDE/Motif, and Windows—for you to select the appearance command that you want. The default option is Windows.
Help	Community Strings Editor Help		Opens the Community Strings Editor online Help.
	Using Help		Opens online Help about how to use the Community Strings Editor online Help.
	About Community Strings Editor		Displays the software version and copyright information for the Community Strings Editor application.

View Area

The following sections describe the two types of view shown in the view area of the Community Strings Editor:

- “Table view,” next
- “Individual view” on page 63

While using either view, you can easily modify any community strings entry by double-clicking the entry. Doing so opens the entry in a Configure Community Strings Entry dialog box. You can also add, modify, or delete entries using the Edit menu or the shortcut menu that opens when you right-click an entry. See “Working with community strings entries” on page 65 for more information.

Table view

The table view shows all community string entries. This view has one tab for each security type. Each tab shows you all community string entries and their settings for the security type.

For every tab, the table view shows a Specific IP table and an IP range table. The columns of the table show the settings for the security type. The following table describes the parts of the SNMP tab in the table view.

Table 13 describes the parts of the table view.

Table 13 Parts of the table view

Part	Description
SNMP tab	• Shows whether Enterprise NMS uses SNMPv1 traps if SNMPv3 trap registration fails. See "Selecting SNMPv1 traps if SNMPv3 trap registration fails" on page 76 for more information. • Shows for each entry: — IP address or IP range for the entry — SNMP read and write community strings (for SNMPv1 authentication) — Timeout interval and retry number — Whether the device or range is SNMPv3 aware See "Working with community strings entries" on page 65 and "Working with SNMPv3 users" on page 72 for more information.
Telnet tab	Shows for each entry: • Telnet user name, password, and privileged password • Telnet Timeout interval, retry number, and prompt See "Working with Telnet and SSL settings" on page 77 for more information.
SSL tab	Shows for each entry the SSL user name, password, and port See "Working with Telnet and SSL settings" on page 77 for more information.

Individual view

The individual view shows all of the SNMP, Telnet, and SSL settings for a selected community string entry.

Table 14 describes the parts of the individual view.

Table 14 Parts of the individual view

Part	Description
Specific IP list	Lists all of the community strings entries for specific devices

Table 14 Parts of the individual view (continued)

Part	Description
IP range list	Lists all of the community strings entries for ranges of devices
Details area	This area on the right side of the view shows the following settings for the selected entry in the Specific IP list or the IP range list: • IP address or IP range for the entry • SNMP read and write community strings • Timeout interval and retry number • Whether the device or range is SNMPv3 aware • Details for all SNMPv3 users • Telnet user name, password, and privileged password • Telnet Timeout interval, retry number, and prompt • SSL user name, password, and port See "Working with community strings entries" on page 65 for more information about modifying the settings for the entry or for adding new entries.

Status bar

The status bar in the Community Strings Editor window displays the following information:

- Toolbar and menu command descriptions
- Error and information messages.
- Whether you are currently connected to the Enterprise NMS server
- Current user name.
- Your Access Control privileges.

Working with the Community Strings Editor

The Community Strings Editor lets you set up SNMP configuration options to support your network arrangement. The following sections describe how to configure community strings and user details:

- "Working with community strings entries," next
- "Working with SNMPv3 users" on page 72

- "Working with Telnet and SSL settings" on page 77
- "Importing and exporting community strings" on page 79

Working with community strings entries

The following sections describe how to perform basic operations with community strings entries:

- "Adding a new community string entry," next
- "Modifying a community string entry" on page 68
- "Deleting a community string entry" on page 69
- "Changing the order of community string entries" on page 69
- "Resetting changes" on page 71
- "Refreshing the display" on page 71
- "Saving changes" on page 72

Adding a new community string entry

Add community string entries or devices or ranges of devices in your network that use non-default SNMP community strings. If devices on your network use default community strings, you do not need to add entries for them.

At a minimum, you must configure basic SNMP settings for every entry. Additionally, you can configure SNMPv3 users, Telnet settings, and SSL settings for entries.

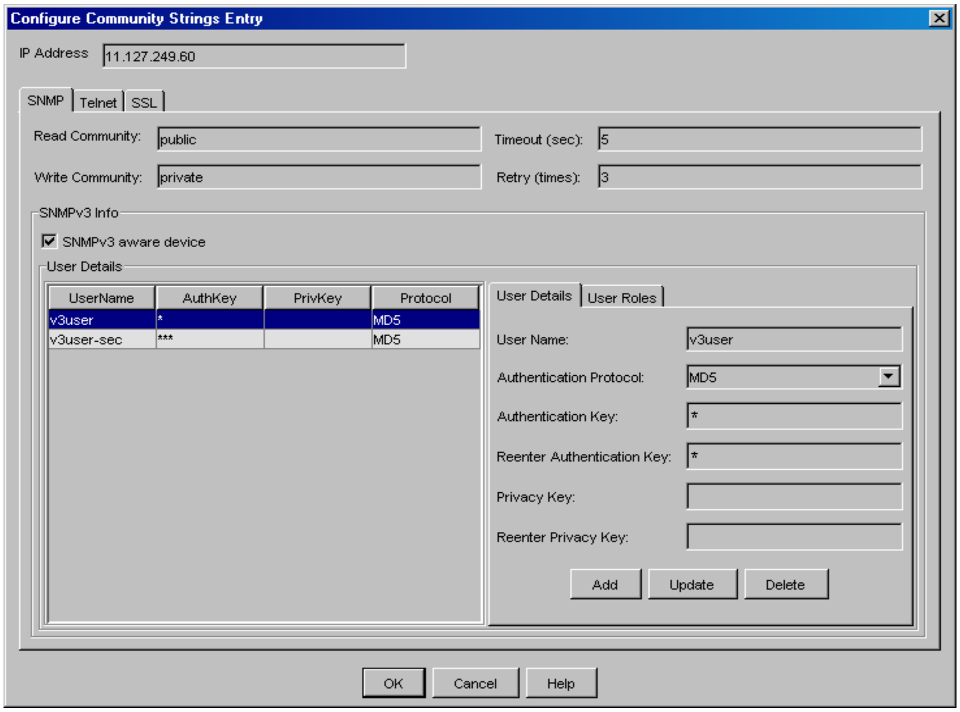
To add a new community string entry:

1 Do one of the following:

- On the toolbar, click Create New Entry
- On the menu bar, choose Edit > New

The Configure Community Strings Entry dialog box opens (Figure 14).

Figure 14 Configure Community Strings Entry dialog box



Configure Community Strings Entry

IP Address 11.127.249.60

Read Community: public

Timeout (sec): 5

Write Community: private

Retry (times): 3

SNMPv3 Info

☑ SNMPv3 aware device

User Details

UserName	AuthKey	PrivKey	Protocol
v3user	*		MD5
v3user-sec	***		MD5

User Name: v3user

Authentication Protocol: MD5

Authentication Key: *

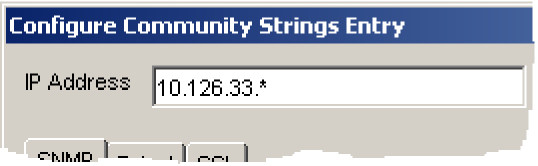
Reenter Authentication Key: *

Privacy Key:

Reenter Privacy Key:

2 In the IP Address text box, type a valid IP address (Figure 15).

Figure 15 IP address text box



Configure Community Strings Entry

IP Address 10.126.33.*

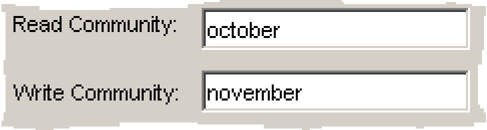
The Community Strings Editor checks the IP address for correct syntax.

See "IP address syntax" on page 52 and "Understanding wildcards" on page 53 for more information.

Note: Community string matching begins with the first entry in the table. When you add a new community string, place entries with wildcards carefully.

3 Enter the read and read/write community strings for the device (Figure 16).

Figure 16 Read and write community strings text boxes



Read Community: october

Write Community: november

The strings must be 50 characters or less.

4 Type a timeout interval between 1 and 99 seconds to specify the amount of time the management application waits for a response before attempting to retry the SNMP request.

The value must be an integer.

5 Type a retry value between 1 and 99 to specify the maximum number of retries the management application attempts before designating the device as unreachable.

The value must be an integer.

6 (Optional) Configure SNMPv3, Telnet, and SSL settings for the entry. For more information, see:

- "Adding SNMPv3 users to an entry" on page 73
- "Configuring Telnet settings for an entry" on page 78
- "Configuring SSL settings for an entry" on page 78

7 Click OK.

Community Strings Editor closes the Configure Community Strings Entry dialog box and adds the entry to either the Specific IP Table or the IP Range Table as appropriate.

8 Do one of the following:

- From the menu bar, choose File > Save.
- On the toolbar, click Save.

Community Strings Editor applies your changes to the Enterprise NMS database.

Modifying a community string entry

You can change any value in a non-default SNMP community string entry in the community strings table. When you click the Change button, the change is added to the community strings table.

To modify a community string entry:

1. In any Community strings table, chose the community string entry you want to change.

   You can choose an entry from any of the following locations:

   - Specific IP list (individual view)
   - IP range list (individual view)
   - Specific IP list (any tab of the table view)
   - IP range list (any tab of the table view)

2. Do one of the following:

   - Double-click the entry
   - Right-click the entry and choose Edit from the shortcut menu.
   - Click the entry and click Edit selected entry on the toolbar.
   - Click the entry and choose Edit > Edit on the menu bar.

   The entry opens in a Configure Community Strings Entry dialog box.

3. Enter your changes in the dialog box. For more information, see “Modifying an SNMPv3 user” on page 75, “Configuring Telnet settings for an entry” on page 78, and “Configuring SSL settings for an entry” on page 78.

4. Click OK.

   Community Strings Editor closes the Configure Community Strings Entry dialog box and modifies the entry on the Specific IP Table or the IP Range Table.

5 Do one of the following:

- From the menu bar, choose File > Save.
- On the toolbar, click Save.

Community Strings Editor applies your changes to the Enterprise NMS database.

Deleting a community string entry

You can delete any non-default SNMP community strings entry in either the Specific IP Table or the IP Range Table.

To delete a community string:

1 In either the either the Specific IP Table or the IP Range Table, click a row.

The row is highlighted.

2 Click Delete.

The table row entry is deleted.

3 Do one of the following:

- From the menu bar, choose File > Save.
- On the toolbar, click Save.

Community Strings Editor applies your changes to the Enterprise NMS database.

Note: You cannot delete the default entry (*.*.*.*).

Changing the order of community string entries

You can change the order of nondefault community strings entries in the community strings table with wildcard IP addresses.

Enterprise Autotopology searches for non-default SNMP community string entries with exact IP addresses first, then searches for community string entries with wildcard IP addresses. Higher entries in the table are evaluated before lower entries.

Table 15 shows examples of how Enterprise NMS responds to the order of IP addresses.

Table 15 Community string order example

IP address	Read community	Result
134.177.123.* 134.177.*.*	public1 public2	For a community string fetch for 134.177.123.122, public1 is selected.
134.177.*.* 134.177.123.*	public2 public1	For a community string fetch for 134.177.123.122, public2 is selected

See "Understanding wildcards" on page 53 for more information.

To change the order of community string entries in the community strings table:

1 In any IP range list or table, select the community string entry or entries you want to move.

You can choose an entry from any of the following locations:

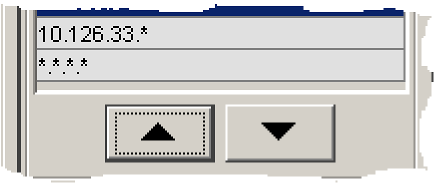
- IP range list (individual view)
- IP range table (any tab of the table view)

You can choose more than one entry at a time using Ctrl+click and Shift+click.

When you select entries in the IP range list or table, the Community Strings Editor enables the Up and Down arrow buttons.

2 Click Up or Down to move the entry or entries to the desired position (Figure 17).

Figure 17 Up and Down buttons below IP Range list or table



Each click moves the entry or entries one position in the table.

3 Do one of the following:

- From the menu bar, choose File > Save.
- On the toolbar, click Save.

Community Strings Editor applies your changes to the Enterprise NMS database.

Resetting changes

Changes that you make in the community strings table are temporarily stored in memory.

To discard all changes and reset the table to the last saved set of community strings:

➔ Click Reset.

➡ **Note:** Once you reset the table, all changes since the last save are lost. To keep your changes, you must use the toolbar or menu bar Save command before you exit the Community Strings Editor window.

Refreshing the display

Use the refresh feature to reload the Community Strings Editor display with the latest community strings information from the Enterprise NMS database. This feature is useful if changes have been made to the database since the Community Strings Editor was last opened or refreshed. However, refreshing the display discards any changes you have made since the last save. So you may want to save the current changes before you refresh the display.

To discard all changes and refresh the Community Strings Editor display from the Enterprise NMS database:

➔ Click Reset.

➡ **Note:** Once you refresh the display, all changes since the last save are lost. To keep your changes, you must use the toolbar or menu bar Save command before you exit the Community Strings Editor window.

Saving changes

Changes that you make in the community strings table are temporarily stored in memory.

To save non-default SNMP community strings information to the Enterprise Topology database:

➔ Do one of the following:

- From the menu bar, choose File > Save.
- On the toolbar, click Save.

Community Strings Editor applies your changes to the Enterprise NMS database.

Working with SNMPv3 users

The following sections describe how to manage SNMPv3 users for community strings entries:

- "Adding SNMPv3 users to an entry," next
- "Modifying an SNMPv3 user" on page 75
- "Deleting an SNMPv3 user" on page 75
- "Selecting SNMPv1 traps if SNMPv3 trap registration fails" on page 76

Adding SNMPv3 users to an entry

You use the Configure Community Strings Entry dialog box to add SNMPv3 usernames and to associate these with Enterprise NMS users.

Note: Enterprise NMS applications – AutoTopology Manager, Expanded View, Fault Summary, and OmniView – use the Enterprise NMS root user (UNIX systems) or Administrator user (Windows systems) to access devices. Hence, an association between the root / Administrator user and an SNMPv3 user is required for Enterprise NMS operations.

Caution: If a user attempts to access an SNMPv3 aware device and the log in fails, SNMPv1 read/write community strings take effect. For this reason, Nortel recommends that you establish complex SNMPv1 community strings.

This procedure assumes you are adding an SNMPv3 user to an existing community string. See "Adding a new community string entry" on page 65 or "Modifying a community string entry" on page 68 for more information.

To add an SNMPv3 user:

1 If you haven't already done so, open a Configure Community Strings Entry dialog box for the entry for which you want to configure the SNMPv3 settings.

2 On the Configure Community Strings Entry dialog box, click the SNMP tab to bring it to the front.

3 Mark the SNMPv3 aware device check box to enable SNMPv3 features.

The SNMPv3 User Details table, User Details tab, and User Roles tab become active. See "SNMP tab" on page 83 for detailed information on the table and tab elements.

You must enter at least one SNMPv3 user name, for association with the Enterprise NMS root / Administrator user.

4 Select the User Details tab.

5 Enter a User Name. This is the SNMPv3 username.

6 Type an authentication key (optional) in the Authentication Key text box.

You must re-enter the authentication key.

7 Re-enter the authentication key.

The Privacy Key text box is enabled.

8 Type a privacy key (optional) in the Privacy Key text box.

You must re-enter the privacy key.

9 Re-enter the privacy key.

10 Click the Add button.

The SNMPv3 username is added to the User Details table.

11 Select the UserName in the User Details table.

12 Select the User Roles tab.

13 From the Users column, select the Enterprise NMS user(s) to be associated with the SNMPv3 username.
Use the Control key to select more than one Enterprise NMS user.

14 Use the >> button to move the selected Enterprise NMS user(s) to the Mapped Users column.

Use the >>> button to move all Enterprise NMS users to the Mapped Users column.

The Enterprise NMS users in the Mapped Users column are now associated with the SNMPv3 username and can access the IP Address specified by the community string.

15 On the Configure Community Strings Entry dialog box, click OK.

16 Do one of the following:

- From the menu bar, choose File > Save.
- On the toolbar, click Save.

The Community Strings Editor applies the changes to the Enterprise NMS database.

Modifying an SNMPv3 user

To modify SNMPv3 user settings:

1. If you haven't already done so, open a Configure Community Strings Entry dialog box for the entry for which you want to change the SNMPv3 user settings. See "Adding a new community string entry" on page 65 or "Modifying a community string entry" on page 68 for more information.
2. On the Configure Community Strings Entry dialog box, click the SNMP tab to bring it to the front.
3. On the User Details table, click the row for the SNMPv3 UserName you want to modify.
4. Click the User Details tab and modify the SNMPv3 properties as required.
5. Click the User Roles tab and modify the Enterprise NMS roles as required.
6. Click Update.

   The Community Strings Editor incorporates the changes.
7. Click OK.

   The Community Strings Editor closes the Configure Community Strings Entry dialog box.
8. Do one of the following:
   - From the menu bar, choose File > Save.
   - On the toolbar, click Save.

   The Community Strings Editor applies the changes to the Enterprise NMS database.

Deleting an SNMPv3 user

If you delete the SNMPv3 User Name to which the Enterprise NMS root (UNIX) or Administrator (Windows) has been mapped, Enterprise NMS application are not able to access the device(s) for the respective IP address(es). In this case, the system displays a message informing you that you will not receive SNMPv3 traps. You are prompted to continue or stop the deletion process.

To delete an SNMPv3 user:

1 If you haven't already done so, open a Configure Community Strings Entry dialog box for the entry for which you want to delete an SNMPv3 user. See "Adding a new community string entry" on page 65 or "Modifying a community string entry" on page 68 for more information.

2 On the Configure Community Strings Entry dialog box, click the SNMP tab to bring it to the front.

3 On the User Details table, click the row for the SNMPv3 UserName you want to delete.

4 Click Delete.

➡ **Note:** If you delete the SNMPv3 user that is mapped to the root / Administrator Enterprise NMS user, you must designate another user as the Enterprise user. Otherwise, Enterprise NMS applications do not function properly.

5 Click Update.

The Community Strings Editor incorporates the changes.

6 Click OK.

The Community Strings Editor closes the Configure Community Strings Entry dialog box.

7 Do one of the following:

- From the menu bar, choose File > Save.
- On the toolbar, click Save.

The Community Strings Editor applies the changes to the Enterprise NMS database.

Selecting SNMPv1 traps if SNMPv3 trap registration fails

The Community Strings Editor lets you configure a global preference that causes the system to default to the community strings authorization if SNMPv3 trap registration fails.

Some possible reasons for SNMPv3 trap registration to fail are:

- The authentication key is rejected
- The privacy key is rejected
- The user does not have permissions set in Access Control

If the option "Use SNMPv1 traps if SNMPv3 trap registration fails" is selected, the system will receive SNMPv1 traps. If the option is not marked, no traps are received by the system.

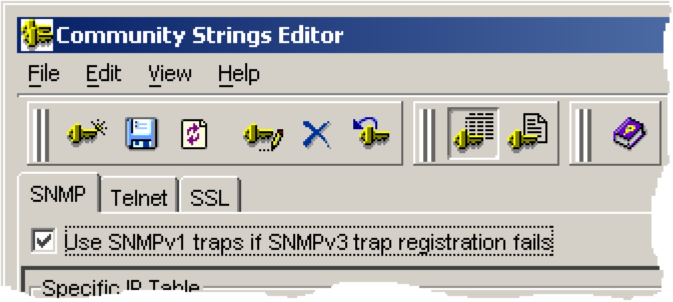
To enable the Enterprise NMS server to receive SNMPv1 traps:

1 On the toolbar, Click show data as table to switch to the table view.

2 If necessary, in the view area click the SNMP tab to bring it to the front.

3 Mark the check box for Use SNMPv1 traps if SNMPv3 trap registration fails.

Figure 18 Marking the check box for Use SNMPv1 traps if SNMPv3 trap registration.



Community Strings Editor

File Edit View Help

SNMP | Telnet | SSL

☑ Use SNMPv1 traps if SNMPv3 trap registration fails

Specific IP Table

4 On the toolbar, click Save to apply the change to the Enterprise NMS database.

Working with Telnet and SSL settings

The following sections describe how to configure Telnet and SSL security settings for community strings entries:

- "Configuring Telnet settings for an entry," next
- "Configuring SSL settings for an entry" on page 78

Configuring Telnet settings for an entry

To configure telnet settings for either an existing entry or a new entry:

1 If you haven't already done so, open a Configure Community Strings Entry dialog box for the entry for which you want to configure the telnet settings. See "Adding a new community string entry" on page 65 or "Modifying a community string entry" on page 68 for more information.

2 On the Configure Community Strings Entry dialog box, click the Telnet tab to bring it to the front.

3 On the Telnet tab, enter the necessary telnet login information.

You must enter at least the IP address and telnet user name. You will probably need to also enter and confirm the telnet password. Depending on your device configurations, you may also need to enter the privileged password, prompt, timeout value, and retry valueSee "Telnet tab" on page 85 for more information about telnet tab elements.

4 If you are done configuring the community strings entry, click OK. Otherwise, click either the SNMP tab or the SSL tab to configure the settings on that tab.

Configuring SSL settings for an entry

➡ **Note:** SSL settings apply to IP telephony and VoIP systems only (for examples: Communication Server 1000, Business Communications Manager, Meridian 1 PBX, MCS 5100 Multimedia Communications System). SSL information is not used by any other type of device.

To configure SSL settings for either an existing entry or a new entry:

1 If you haven't already done so, open a Configure Community Strings Entry dialog box for the entry for which you want to configure the telnet settings.

See "Adding a new community string entry" on page 65 or "Modifying a community string entry" on page 68 for more information.

2 On the Configure Community Strings Entry dialog box, click the SSL tab to bring it to the front.

3 On the SSL tab, enter the necessary login information.

You must enter at least the IP address and SSL user name. You will probably need to also enter and confirm the SSL password.See "SSL tab" on page 86 for more information about SSL tab elements.

4 If you are done configuring the community strings entry, click OK. Otherwise, click either the SNMP tab or the Telnet tab to configure the settings on that tab.

Importing and exporting community strings

The following sections describe how to import community string entries from files, and also how to export entries to files. You can use these features to transfer and coordinate community strings between Enterprise NMS and other network management applications and platforms:

- "Importing a community strings file," next
- "Understanding Timeout value conversion" on page 81
- "Exporting a community strings file" on page 82

Importing a community strings file

You can import a community strings file into the Enterprise database using the Community Strings Editor. Use this feature when you:

- Migrate from one operating system platform to another
- Transfer from one Enterprise NMS server to another server

Note: Nortel recommends that you not modify community strings files manually.

A community strings file can contain from one to many community strings and properties. When you save an imported community strings file, it completely overwrites the existing community strings and properties that exist in the local Enterprise NMS database.

An imported HP OpenView community strings file does not support the Telnet login password and SNMPv3. Therefore, Telnet and SNMPv3 information is not imported.

When you import a community strings file in HP OpenView format, the Community Strings Editor automatically converts the timeout values.

See "Understanding Timeout value conversion" on page 81 for more information.

Note: You cannot import community string files using the Community Strings Editor Web browser interface.

To import a new community strings file:

1. Save the community strings file that you want to import.
2. From the Community Strings Editor menu bar, choose either File > Import Data >Enterprise format or File > Import Data >HP-OV format.

   Use the command that matches the file type you are importing.

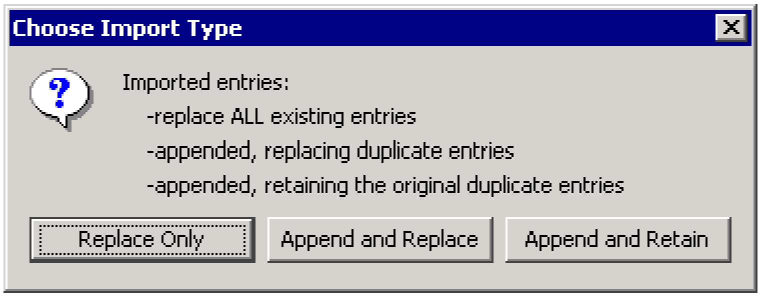
   The Import Community Strings dialog box opens.

3. Locate and select the community strings file that you want to import.

   The file must be in comma separated value or in HP OpenView format.

4. Click OK.
5. The Choose Import Type dialog box opens to prompt you how to import the entries in the file (Figure 19).

Figure 19 Choose Import Type dialog box



Choose Import Type

Imported entries:
-replace ALL existing entries
-appended, replacing duplicate entries
-appended, retaining the original duplicate entries

6 Click one of the choices described in Table 16.

Table 16 Community Strings Editor file import types

Click this...	To do this...
Replace only	Delete all existing community strings entries in the Enterprise NMS database and replace them with the community strings from the file.
Append and Replace	Add the entries in the file to the Enterprise NMS database. Entries in the database that duplicate entries in the file are replaced by entries in the file. All non-duplicate entries in the file are appended to the database.
Append and retain	Append all entries in the file to the database. Duplicate entries are retained.

7 Do one of the following:

- From the menu bar, choose File > Save.
- On the toolbar, click Save.

Understanding Timeout value conversion

The Community Strings Editor automatically converts the Timeout parameter when you import a file in HP OpenView format. The HP OpenView Timeout is a real number in 1/10 of a second. Enterprise NMS Timeout is an integer between 1 and 99. The Community Strings Editor rounds the Timeout value to the nearest non-zero integer.

Table 17 shows examples of the value conversions.

Table 17 Timeout value conversion examples

HP OpenView timeout value (seconds)	Converted Enterprise NMS timeout value (seconds)
5.2	5
5.6	6
1.23	1
2.88	3
0.80	1
0.30	1

Exporting a community strings file

Using Community Strings Editor, you can export the community strings information in the Enterprise NMS database to a file. Community Strings Editor lets you export a community strings file in comma-separated value or HP OpenView file format. You can use the community strings file as a backup while you make changes to existing community strings, or to import new community strings to another Enterprise NMS server system.

For security when you export, Telnet password and SNMPv3 information is not readable. Additionally, the Telnet login, password, and SNMPv3 information is ignored for HP OpenView file format.

When you export an Enterprise NMS community strings file in HP OpenView format, the Enterprise NMS time out value information is automatically converted to the HP OpenView values.

➡ **Note:** Nortel strongly recommends that you not edit a community strings file.

To export the current community strings data:

1 From the Community Strings Editor menu bar, choose File > Export data.

The Export Community Strings dialog box opens.

2 Go to the location on the Enterprise NMS server file system where you want to save the exported file.

3 Type a name for the file and choose the file format for the file.

4 Click OK.

Understanding the Community Strings Editor interface

The following topics describe the dialog boxes you encounter while using Community Strings Editor:

- “Configure Community Strings Entry dialog box” on page 83

Configure Community Strings Entry dialog box

Use the Configure Community Strings Entry dialog box to add a new entry or modify an existing entry. See "Working with community strings entries" on page 65 for more information.

The following table describes the parts of the Configure Community Strings Entry dialog box.

Table 18 Parts of the Configure Community Strings Entry dialog box

Part	**Description**
IP Address	The IP address or range to which the entry applies. When adding a new entry, enter the IP address or range. You can use * wildcards to indicate ranges. When editing an existing entry, the IP address is read-only.
SNMP tab	Lets you configure SNMP parameters for the entry. See "SNMP tab," next for more information.
Telnet tab	Lets you configure Telnet parameters for the entry. See "Telnet tab" on page 85 for more information.
SSL tab	Lets you configure SSL parameters for the entry. See "SSL tab" on page 86 for more information.
OK	Applies your changes and closes the dialog box.
Cancel	Discards your changes and closes the dialog box.
Help	Opens online Help for the dialog box.

SNMP tab

Use the SNMP tab of the Configure Community Strings Entry dialog box to configure SNMP parameters for a community strings entry. See "Working with community strings entries" on page 65, and "Working with SNMPv3 users" on page 72 for more information.

The following table describes the parts of the SNMP tab.

Table 19 Parts of the SNMP tab

<table>
<tr><th>Part</th><th colspan="2">Description</th></tr>
<tr><td>Read Community</td><td colspan="2">The SNMP read community string for the entry.</td></tr>
<tr><td>Write Community</td><td colspan="2">The SNMP write community string for the entry.</td></tr>
<tr><td>Timeout</td><td colspan="2">The number of seconds that Enterprise NMS allows to elapse before attempting to retry the SNMP request.</td></tr>
<tr><td>Retry</td><td colspan="2">The number of times that Enterprise NMS attempts to contact the device before designating it as unreachable.</td></tr>
<tr><td>SNMPv3 aware device</td><td colspan="2">Indicates that the device or range of devices use SNMPv3 features. The elements in the SNMPv3 area are enabled only when SNMPv3 aware device is marked.</td></tr>
<tr><td rowspan="11">User Details</td><td colspan="2">Lets you view and manage a list of SNMPv3 users configured for the selected device or range. See "Working with SNMPv3 users" on page 72 for more information.</td></tr>
<tr><td><b>Part</b></td><td><b>Description</b></td></tr>
<tr><td>User Details table</td><td>Shows you a list of SNMPv3 users and their settings</td></tr>
<tr><td>User Details tab</td><td>Provides a summary of the SNMPv3 UserName selected in the User Details table.
Allows you to add a new SMMPv3 username, or update or delete an existing username.</td></tr>
<tr><td></td><td>User Name: The SNMPv3 username.</td></tr>
<tr><td></td><td>Authentication Protocol:
Currently, the MD5 protocol is supported.</td></tr>
<tr><td></td><td>Authentication Key:
Enter the authentication key. For security, the key is displayed as asterisks.</td></tr>
<tr><td></td><td>Reenter Authentication Key:
Reenter the authentication key. For security, the key is displayed as asterisks.</td></tr>
<tr><td></td><td>Privacy Key:
Enter the privacy key. For security, the key is displayed as asterisks.</td></tr>
<tr><td></td><td>Reenter Privacy Key:
Reenter the privacy key. For security, the key is displayed as asterisks.</td></tr>
<tr><td></td><td>Add:
Adds the entry to the User Details table.</td></tr>
</table>

Table 19 Parts of the SNMP tab (continued)

Part	Description	
		Update: Updates the selected entry with new settings.
		Delete: Deletes the selected entry.
	User Roles table	Users: List of all Enterprise NMS users, as defined through Access Control Administration.
		Mapped Users: Enterprise NMS users that are mapped to the SNMPv3 username selected in the User Details table.
		>>, >>>, <<, <<<<: When one or more users is selected, the >> and << buttons map or unmap the selected user(s), respectively. Use the Control key to select several users. Use the >>> and <<< buttons map or unmap all users, respectively.
OK	Applies the selected SNMP settings to the device or range entry and closes the dialog box.	
Cancel	Discards the settings to the device or range entry and closes the dialog box.	
Help	Opens online Help for the dialog box.	

Telnet tab

Use the Telnet tab of the Configure Community Strings Entry dialog box to configure Telnet parameters for a community strings entry. See "Configuring Telnet settings for an entry" on page 78 for more information.

The following table describes the parts of the Telnet tab.

Table 20 Parts of the Telnet tab

Part	Description
User	Enter a valid Telnet user name.
Password	Enter the Telnet user password. For security, the password is displayed as asterisks.

Table 20 Parts of the Telnet tab

Part	**Description**
Reenter Password	Reenter the password to confirm it. For security, the password is displayed as asterisks.
Prompt	Enter the Telnet prompt.
Timeout	The number of seconds that Enterprise NMS allows to elapse before attempting to retry the Telnet connection.
Retry	The number of times that Enterprise NMS attempts to contact the device before designating it as unreachable.
Privileged Password	Enter the Telnet privileged password. For security, the password is displayed as asterisks.
Reenter Privileged Password	Reenter the privileged password to confirm it. For security, the password is displayed as asterisks.

SSL tab

Use the SSL tab of the Configure Community Strings Entry dialog box to configure SSL security parameters for a community strings entry. See "Configuring SSL settings for an entry" on page 78 for more information.

The following table describes the parts of the SSL tab.

Table 21 Parts of the SSL tab

Part	**Description**
User	Enter a valid SSL user name.
Password	Enter the SSL user password. For security, the password is displayed as asterisks.
Reenter Password	Reenter the password to confirm it. For security, the password is displayed as asterisks.
Port	Enter the SSL port.

Troubleshooting the Community Strings Editor

Table 22 suggests techniques for resolving problems or interpreting unexpected results.

Table 22 Common Community Strings Editor problems

Problem	**Resolution**
The Community Strings Editor does not start.	Verify that: - The *cstrings.reg* file is in the directory *weboptsrvr/registration* beneath the Enterprise NMS home directory. - The *cstrings.schema* file is in the directories *db/AppControlDB.db* and *schemas/AppControlDB* beneath the Enterprise NMS home directory. Also be sure that the Enterprise user has access permission to the IC, IC_ADMIN, and COMMUNITY_STRINGS permission tokens in the Access Control Administration window. See “Specifying access to applications with Access Control Administration” on page 21 for more information.
You see the following message: `Community Strings Editor has determined that the community strings are managed by another platform other than Enterprise. Enterprise applications will not use the Enterprise database for getting the Community Strings in this case. Do you want to use the Enterprise database?`	This is the expected behavior, not a problem. The Community Strings Editor is not applicable when a network management system such as HP OpenView or Tivoli NetView is installed on the Enterprise NMS server station. If you want Enterprise NMS to manage community strings, do the following: 1. Uninstall the other network management software. 2. Uninstall Enterprise NMS. 3. Reinstall Enterprise NMS.
You cannot add a community string entry.	Verify that you have fewer than 500 community strings configured. You can add a maximum of 500 community strings.
You cannot add, delete, change the order of, reset, save, import, or export entries in the IP (community strings) table.	Verify that you have read/write access to the COMMUNITY_STRINGS permission token in the InfoCenter Access Control Administration window.

Table 22 Common Community Strings Editor problems (continued)

Problem	**Resolution**
The values in the IP (community strings) table are not what you expected after clicking the Reset button.	Perform a Save on the table. A reset restores the IP (community strings) table values to the last SAVE performed.
You receive an error while trying to import a new community strings file.	If one or more line of the *.csv file you are trying to import does not match the expected format, the error message provides the line number of each incorrect entry. Contact Nortel Customer Support with this information.

Index