



Net-Net® EMS
User Guide
Release Version 6.4 4000

Acme Packet, Inc.
100 Crosby Drive
Bedford, MA 01730
t 781-328-4400
f 781-275-8800
www.acmepacket.com

Notices

©2002—2010 Acme Packet®, Inc., Bedford, Massachusetts. All rights reserved. Acme Packet®, Session Aware Networking®, Net-Net®, and related marks are registered trademarks of Acme Packet, Inc. All other brand names are trademarks, registered trademarks, or service marks of their respective companies or organizations.

Patents Pending, Acme Packet, Inc.

The Acme Packet Documentation Set and the Net-Net systems described therein are the property of Acme Packet, Inc. This documentation is provided for informational use only, and the information contained within the documentation is subject to change without notice.

Acme Packet, Inc. shall not be liable for any loss of profits, loss of use, loss of data, interruption of business, nor for indirect, special, incidental, consequential, or exemplary damages of any kind, arising in any way in connection with the Acme Packet software or hardware, third party software or hardware, or the documentation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above exclusions may not apply. These limitations are independent from all other provisions and shall apply notwithstanding the failure of any remedy provided herein.

Copying or reproducing the information contained within this documentation without the express written permission of Acme Packet, Inc., 100 Crosby Drive, Bedford, MA 01730, USA is prohibited. No part may be reproduced or retransmitted.

Acme Packet Net-Net products are protected by one or more of the following patents: United States: 7072303, 7028092, 7002973, 7133923, 7031311, 7142532, 7151781. France: 1342348, 1289225, 1280297, 1341345, 1347621. Germany: 1342348, 1289225, 1280297, 1341345, 1347621. United Kingdom: 1342348, 1289225, 1280297, 1341345, 1347621. Other patents are pending.

Contents

| | |
|---|-------------|
| About this Guide | xvii |
| Who is Acme Packet?..... | xvii |
| Customer Questions, Comments, or Suggestions..... | xvii |
| Contact Us..... | xvii |
| | |
| 1 Getting Started | 19 |
| Overview | 19 |
| Before You Start..... | 19 |
| Net-Net EMS and Net-Net 4000 SBC Compatibility..... | 19 |
| Minimum Net-Net SBC Configuration..... | 20 |
| Boot Parameters | 20 |
| System Configuration Element..... | 21 |
| SNMP Community Element..... | 22 |
| Trap Receiver Element | 22 |
| Instructions Based on Mozilla Firefox 1.06 | 22 |
| | |
| 2 Using Net-Net EMS..... | 23 |
| Introduction | 23 |
| About the Relationship with ACI..... | 23 |
| Basic Workflow | 23 |
| Accessing the Net-Net EMS GUI..... | 24 |
| HTTP Login | 24 |
| HTTPS Login Using Microsoft Internet Explorer 6.0 | 24 |
| HTTPS Login Using Mozilla Firefox 1.0..... | 26 |
| After You Login | 28 |
| Overview of Net-Net EMS GUI..... | 29 |
| Menu Bar | 29 |
| Toolbar | 31 |
| Navigation Tree | 31 |

| | |
|--|-----------|
| Net-Net EMS Standalone Net-Net SBC and HA Pair Icons | 32 |
| Alarm Count by Severity Table | 34 |
| Changing the Alarm Table Presentation | 34 |
| Display Pane | 36 |
| Status Bar | 36 |
| Right-Click Mouse Functions | 36 |
| Active Configuration Category | 36 |
| Active Domain | 36 |
| Active Net-Net SBC Configuration | 37 |
| Active SD HA Pair | 37 |
| Inactive Configuration Category | 37 |
| Inactive Domain | 38 |
| Inactive Configuration Node | 38 |
| Inactive Net-Net SBC Configuration | 38 |
| Inactive SD HA Pair | 39 |
| Viewing Net-Net EMS License Information | 40 |
| About the License Data | 40 |
| Sending Broadcast Messages | 42 |
| Connecting Using Telnet | 43 |
| Offline Configuration | 44 |
| Copying a Configuration | 44 |
| Creating an Original Configuration | 45 |
| Replicating Selected Configuration Elements | 47 |
| Record Validation | 47 |
| Replicating Data | 47 |
| Reboot Notices | 51 |
| Configuring External Trap Receivers | 52 |
| About Net-Net EMS Traps | 52 |
| Notification Objects | 53 |
| Configuring External Trap Receivers | 53 |
| Using Net-Net EMS Client Logs | 55 |
| Enabling the Java Console | 55 |
| Starting the Java Console | 57 |
| Configuring the Client Log Levels | 58 |
| Viewing Log Data Online | 59 |
| Viewing the Java Console Log File | 60 |
| 3 Discovering Net-Net SBCs | 61 |
| Overview | 61 |

| | |
|---|-----------|
| Types of Discovery | 61 |
| SSH Username | 61 |
| Disabling File-Based Discovery | 61 |
| Minimum Net-Net SBC Configuration | 62 |
| Boot Parameters | 62 |
| System Configuration Element | 62 |
| SNMP Community Element | 62 |
| Trap Receiver Element | 63 |
| About Configuring the Discovery | 63 |
| Creating a New Domain | 63 |
| Accessing the Discovery Window | 64 |
| About the Discovery Table | 65 |
| About the Save Log | 65 |
| Configuring the Discovery | 66 |
| Entering the Net-Net SBC Addresses | 66 |
| Standalone Net-Net SBC | 66 |
| Net-Net SBC HA Pair | 66 |
| Multiple Net-Net SBCs | 67 |
| Completing the Configuration | 68 |
| Moving the Discovered Net-Net SBC | 72 |
| Rediscovering Net-Net SBCs | 73 |
| Display Configuration Version | 76 |
| Discovery Process Sequences | 77 |
| Use-Case Scenarios | 77 |
| Viewing the Configuration Version | 78 |
| Active Configuration | 78 |
| Inactive Configuration | 79 |
| Copying the Net-Net SBC | 80 |
| Renaming the Net-Net SBC Configuration Copy | 81 |
| 4 Configuring Net-Net SBCs | 83 |
| Introduction | 83 |
| About Net-Net 4000 SBCs | 83 |
| Configuration Overview | 83 |
| Tool Tips | 83 |
| Using Net-Net EMS to Configure the Net-Net SBC | 84 |
| Storing Configurations | 84 |
| Relationship Between ACLI/EMS | 84 |
| Discovery | 84 |
| Copy-for-Edit | 85 |

| | |
|---|------------|
| Net-Net EMS Save Methods | 86 |
| Save Method..... | 86 |
| Full Save Method..... | 88 |
| EMS Activate..... | 89 |
| Error Paths | 90 |
| Error during Discovery..... | 90 |
| Error during Copy | 90 |
| Error during Save: Phases 1, 2, or 3..... | 90 |
| Error during Activate | 91 |
| Save and Activtate EMS Commands..... | 91 |
| Saving Configurations..... | 92 |
| Save Method | 92 |
| Early Contention Detection | 92 |
| Example of Save Process | 93 |
| Configuration Operations Lockout..... | 94 |
| Full Save Method..... | 94 |
| Performing Save and Full Save | 94 |
| Performing a Save Operation..... | 95 |
| Performing a Save and Activate Operation | 95 |
| Performing a Full Save Operation | 96 |
| Performing a Full Save and Activate Operation | 97 |
| Accessing the Configuration Changes Table..... | 98 |
| Locking Your Configuration | 99 |
| Lock Privileges | 99 |
| Locking and Unlocking an Inactive Configuration | 99 |
| Locking and Unlocking an Active Configuration | 101 |
| Configuration Search | 103 |
| Caveats..... | 103 |
| Searching for Configuration Objects..... | 103 |
| 5 Work Order Administration..... | 111 |
| Introduction | 111 |
| About Work Order Administration | 111 |
| Predefined Work Flows | 111 |
| Software Upgrade..... | 112 |
| Global Parameter Changes..... | 112 |
| Combined Upgrade and Parameter Changes | 112 |
| Work Order Phases | 112 |
| Before You Start | 115 |
| User Permissions | 115 |

| | |
|--|------------|
| High Availability Requirements | 115 |
| Software Image Archive Management | 115 |
| Specifying the Software Image Directory | 116 |
| Software Image Archive Management Data | 117 |
| Software Image Archive Management Actions | 117 |
| Software Version Requirements | 117 |
| Software Downgrade Capability | 117 |
| Work Order Administration Graphical User Interface | 118 |
| Work Orders Tab | 118 |
| Work Order Actions | 120 |
| Work Order Table Data | 121 |
| About Device Tasks | 123 |
| Device Task Data | 123 |
| Software Image Archive Management Tab | 124 |
| Edit Work Order Window | 125 |
| Universal Work Order Parameters | 126 |
| About Targeted Devices | 126 |
| Targeted Devices Data | 127 |
| About Work Flow | 128 |
| Software Upgrade Tab | 128 |
| Global Parameter Changes Tab | 129 |
| Configuration Table Data | 129 |
| Configuration Table Actions | 130 |
| About Attribute Modification | 131 |
| Attribute Modification Data | 131 |
| Universal and Work-Order Specific Procedures | 132 |
| Performing a Software Upgrade | 132 |
| Creating a Software Upgrade Work Order | 132 |
| Configuring Target Software Image for Software Upgrades | 134 |
| Configuring Optional Software Upgrade Parameters | 134 |
| Configuring Optional Pause and Unlock After Loading Software Image | 134 |
| Configuring Optional Break Points | 135 |
| Configuring Optional Call Shedding | 135 |
| Configuring a Health Score for HA Pairs Only | 136 |
| Applying Changes | 136 |
| Executing Work Order | 136 |
| Committing Work Order | 136 |
| Configuring Universal Parameters | 138 |
| Scheduling Work Order Start Date and Time | 138 |
| Configuring the Error Policy | 139 |
| Configuring the Behavior | 139 |

| | |
|--|------------|
| Enabling Auto Commit | 140 |
| Adding Targeted Devices..... | 140 |
| Procedural Steps for Work Orders | 142 |
| Software Upgrade for a Standalone Device..... | 142 |
| Software Upgrade for an HA Pair | 142 |
| Global Parameter Changes for a Standalone Device or an HA Pair | 143 |
| Software Upgrade and Global Parameter Changes for a Standalone Device..... | 143 |
| Software Upgrade and Global Parameter Changes for an HA Pair | 143 |
| Software Rollback for a Standalone Device | 144 |
| Software Rollback for an HA Pair | 144 |
| Global Parameter Changes Rollback for a Standalone Device or an HA Pair..... | 145 |
| Global Parameter Changes and Software Rollback for a Standalone Device | 145 |
| Global Parameter Changes and Software Rollback for an HA Pair..... | 145 |
| Universal Procedure for Executing a Work Order on Demand | 146 |
| Work Order Execution..... | 146 |
| Active Device Tasks Within a Running Work Order | 146 |
| Executing a Work Order on Demand..... | 146 |
| Universal Procedure for Committing a Work Order..... | 148 |
| Manually Committing a Work Order | 148 |
| Performing Global Parameter Changes | 149 |
| Creating a Global Configuration Group..... | 149 |
| Creating a Global Configuration | 150 |
| Creating a Global Configuration from an Existing Net-Net SBC | 150 |
| Creating a Global Configuration Using Net-Net SBC Default Values | 151 |
| Modifying your Global Configuration..... | 153 |
| Creating a Session Agent Example | 153 |
| Creating a Global Parameter Changes Work Order..... | 154 |
| Configuring Universal Parameters..... | 155 |
| Modifying Global Configuration | 156 |
| Assigning the Global Configuration to the Work Order | 156 |
| Setting Criteria for Element Instances in Work Orders | 157 |
| Viewing Set Criteria Details | 159 |
| Apply Configuration Changes | 160 |
| Executing Work Order | 160 |
| Committing Work Order | 160 |
| Performing a Software Upgrade and Global Parameter Changes | 162 |
| Creating Global Configuration Group | 162 |
| Creating Global Configuration | 162 |
| From an Existing Net-Net SBC | 162 |
| Using Net-Net SBC Default Values..... | 162 |
| Creating the Work Order | 162 |

| | |
|--|------------|
| Configuring Universal Parameters | 162 |
| Configuring Software Upgrade Portion | 162 |
| Configuring Target Software Image | 162 |
| Configuring Optional Upgrade Parameters | 163 |
| Configuring Global Parameter Changes Portion | 163 |
| Assigning Global Configuration to the Work Order..... | 163 |
| Modifying Global Configuration | 163 |
| Setting Criteria for Element Instances | 163 |
| Viewing Criteria Details | 163 |
| Applying Configuration Changes | 163 |
| Resuming the Work Order After the Software Upgrade | 164 |
| Executing your Work Order | 164 |
| Committing your Work Order | 164 |
| Universal Pausing, Copying, and Editing Copies of Work Orders | 165 |
| About Pausing a Work Order | 165 |
| Resuming a Paused Work Order..... | 165 |
| Creating a Copy of an Existing Work Order | 166 |
| Editing a Copy of a Work Order..... | 166 |
| Global Configuration Modification Report | 168 |
| About the Global Configuration Modification Data..... | 169 |
| Device Table | 169 |
| Parameters Table..... | 169 |
| Elements Table | 169 |
| Work Order Processing States and User Actions Matrices | 171 |
| Matrix for Work Order States and Actions | 171 |
| Matrix for Device Task States and Actions | 172 |
| Work Order Logs | 173 |
| 6 Viewing the Audit Log | 177 |
| Overview | 177 |
| About the Information Logged | 177 |
| About the Audit Trail Information | 177 |
| Viewing Audit Logs | 178 |
| Accessing Audit Logs..... | 178 |
| Displaying Audit Trails by User Name..... | 179 |
| Displaying Audit Trails by Date-Time Range | 179 |
| Display Audit Trails by User Name and Date-Time Range | 181 |
| About the Audit Trail Data | 182 |
| Refreshing Audit Trail Data | 182 |
| Deleting Audit Trails | 182 |

| | |
|--|------------|
| Saving Data | 183 |
| 7 Generating HDR Reports | 185 |
| Introduction | 185 |
| Configuring Net-Net EMS for HDR Collection | 185 |
| Group Record Types | 186 |
| Configuring HDR Reporting Operations | 190 |
| Accessing HDR Operations | 190 |
| Starting Data Collection | 190 |
| Stopping Data Collection | 191 |
| Restarting Collection | 192 |
| Checking Collection Status | 193 |
| Generating Reports | 194 |
| Accessing the Report Generation Operation | 194 |
| Choosing Reporting Criteria | 194 |
| Choose an Interface Instance | 197 |
| Examples of Report Styles | 198 |
| Line Chart | 198 |
| Area Chart | 198 |
| Time Chart | 199 |
| Table Chart | 199 |
| 8 Inventory Management | 201 |
| Introduction | 201 |
| Inventory Data Collected | 201 |
| Accessing Inventory Information | 202 |
| Accessing Inventory Data | 202 |
| Accessing Data for a Specific Net-Net SBC | 202 |
| No Available Data | 203 |
| Accessing Data for All Discovered Net-Net SBCs | 204 |
| Viewing Standalone Data | 204 |
| No Data is Available | 205 |
| Viewing HA Data | 206 |
| No Data is Available | 207 |
| Saving Data | 207 |
| Net-Net SBC Configuration Integrity | 208 |
| Configuration Record Counting | 208 |
| Discovery | 208 |
| Save | 208 |

| | |
|--|------------|
| Accessing the Configuration Record Count | 208 |
| Saving Record Counts..... | 210 |
| Viewing Hardware Information | 211 |
| Accessing Hardware Data..... | 211 |
| Viewing the Details..... | 213 |
| Viewing Software Information | 214 |
| Accessing Software Data | 214 |
| About the Configuration Versions | 214 |
| About the Boot Table Data | 214 |
| Viewing Boot Table Details | 216 |
| Viewing Backup Information | 216 |
| Viewing Details..... | 217 |
| Viewing License Information | 218 |
| Accessing License Data | 218 |
| About the Total Capacity | 218 |
| About the License Data..... | 218 |
| Viewing Details..... | 220 |
| 9 Fault Management | 221 |
| Overview | 221 |
| About the Relationship of Traps to Events and Alarms | 221 |
| Verifying Net-Net SBC Configuration..... | 221 |
| Accessing Fault Management Information | 222 |
| Viewing Event Information | 222 |
| Event Severity..... | 222 |
| Accessing Event Information | 223 |
| Changing Number of Events on the Page..... | 223 |
| Navigating Pages..... | 223 |
| Sorting Events..... | 224 |
| Viewing Event Details | 225 |
| Viewing Alarm Information | 226 |
| About Alarms | 226 |
| Alarm Categories | 226 |
| Alarm Severities | 228 |
| Default Alarm Severity Color Codes | 229 |
| Remapping Alarm Severities | 229 |
| Alarm Count by Severity Table | 231 |
| Viewing Alarms by Severity for a Specific Category..... | 232 |
| Viewing All Alarms by Severity..... | 232 |
| Viewing Alarms by Category | 233 |

| | |
|--|------------|
| Displaying the Alarm View | 234 |
| Changing Number of Alarms on the Page | 235 |
| Navigating Pages | 235 |
| Sorting Alarms | 235 |
| Viewing Alarm Details | 236 |
| Acknowledging Alarms | 237 |
| Clearing Alarms | 237 |
| Deleting Alarms | 237 |
| Configuring Alarm Email List | 237 |
| Using the Audible Alarm System | 238 |
| About the Audible Alarm System | 238 |
| How the Audible Alarm System Works | 238 |
| About the Audio Files | 238 |
| Substituting WAV Files | 238 |
| Using the Audible Alarm Console | 239 |
| Accessing the Audible Alarm Console | 239 |
| Configuring Audible Alarms | 240 |
| Viewing Alarm Information | 240 |
| Clearing the Audible Alarm | 241 |
| Alarm Handling | 241 |
| Configuring Flashing Alarms | 242 |
| Stopping Alarms from Flashing | 243 |
| Using the Alarm Flashing Console | 243 |
| Acknowledging Alarms | 243 |
| Saving and Deleting Selected Alarms | 243 |
| Configuring Alarm Selection | 243 |
| Saving Alarms | 245 |
| Deleting Alarms | 245 |
| Synchronizing Alarms | 246 |
| Configuring Global Automatic Synchronization | 246 |
| Synchronizing Alarms Using the Console | 247 |
| Accessing the Console | 247 |
| Single Net-Net SBC | 249 |
| All Net-Net SBCs | 249 |
| Manually Synchronize Alarms | 250 |
| Viewing Syslog Information | 251 |
| Syslog Message Example | 251 |
| Hardware Monitor Failure Trap Example | 251 |
| Displaying Syslog Messages | 252 |
| Viewing Details | 254 |
| Stopping Syslog Message Display | 256 |

| | |
|--|------------|
| Starting Syslog Message Display | 256 |
| Sorting Syslog Messages | 257 |
| Filtering Syslog Messages | 257 |
| Accessing the Syslog Filter Dialog Box | 257 |
| Adding New Syslog Filters | 258 |
| Editing Syslog Filters | 263 |
| Deleting Filters | 263 |
| Viewing Registration Cache Information..... | 264 |
| How It Works | 264 |
| Accessing the Registration Cache..... | 264 |
| Working with SIP Registration Caches | 264 |
| IP Address | 265 |
| Users | 266 |
| Realm | 267 |
| Registrar | 268 |
| Route | 269 |
| Command Status | 269 |
| Viewing Registration Cache Details..... | 270 |
| Clearing the SIP Registration Cache..... | 271 |
| Auditing the SIP Registration Cache | 271 |
| Working with the H.323 Registration Cache | 271 |
| Displaying the H.323 Registration Cache..... | 271 |
| Viewing Registration Cache Details..... | 273 |
| Clearing the H.323 Registration Cache..... | 274 |
| Auditing the H.323 Registration Cache | 274 |
| Working with MGCP Registration Caches..... | 274 |
| Displaying the MGCP Registration Cache | 274 |
| Command Status | 275 |
| Viewing Registration Cache Details..... | 276 |
| Clearing the MGCP Registration Cache | 277 |
| Auditing the MGCP Registration Cache | 277 |
| Configuring Severity Color-Coding | 278 |
| Choosing a New Color | 279 |
| Editing HSB Values | 280 |
| Editing RGB Values | 281 |
| 10 Performance Management..... | 283 |
| Introduction | 283 |
| Accessing Performance Management Information..... | 284 |
| Refreshing Data | 285 |
| Saving Data..... | 285 |

| | |
|---|------------|
| Viewing System Information | 286 |
| Accessing System Data | 286 |
| General | 286 |
| Identification | 287 |
| Viewing SNMP Information..... | 288 |
| Accessing SNMP Data..... | 288 |
| Viewing IP Information..... | 291 |
| Accessing IP Data | 291 |
| General | 291 |
| Addresses | 293 |
| Interfaces | 294 |
| Extended Interfaces | 297 |
| ICMP | 299 |
| TCP..... | 300 |
| UDP | 303 |
| Viewing Environmental Information..... | 304 |
| Accessing Environmental Data | 304 |
| Voltage | 304 |
| Temperature | 306 |
| Fans | 307 |
| Power Supplies..... | 308 |
| Cards..... | 309 |
| Viewing Session Information | 310 |
| Displaying Session Data | 310 |
| Specifying the Number of Records to Display..... | 310 |
| Displaying All Records | 310 |
| Refreshing Records | 310 |
| Saving Records..... | 310 |
| Accessing Session Data | 311 |
| SIP Session Agents..... | 311 |
| Realm | 315 |
| H.323 Session Agents | 319 |
| Combined Session Agents | 323 |
| Viewing NSEP Information | 326 |
| Accessing NSEP Data | 326 |
| Viewing LDAP Server Information | 327 |
| Accessing LDAP Server Data | 327 |
| Viewing Number of Cached Contacts | 328 |
| Accessing Number of Cached Contacts..... | 328 |
| Viewing Trap Table Summary Information | 329 |

| | |
|--|------------|
| Displaying Trap Table Data | 329 |
| Specifying the Number of Records to Display | 329 |
| Displaying All Records | 329 |
| Refreshing Records | 329 |
| Saving Records | 329 |
| Accessing Trap Table Summary Data | 330 |
| Viewing Storage Utilization Information | 331 |
| Accessing Storage Utilization Data | 331 |
| Viewing IDS Information. | 332 |
| Accessing IDS Data | 332 |
| Viewing Network Management Controls Information | 333 |
| Accessing NM Control Data | 333 |
| Viewing ENUM Server Information | 334 |
| Accessing ENUM Server Data | 334 |

About this Guide

The *Net-Net® EMS 6.4 Work Order Administration Guide* provides the information you need to use Work Order Administration for Acme Packet's Net-Net session border controller.

Who is Acme Packet?

Acme Packet enables service providers to deliver trusted, first class interactive communications—voice, video and multimedia sessions—across IP network borders. Our Net-Net family of session border controllers satisfy critical security, service assurance and regulatory requirements in wireline, cable and wireless networks. Our deployments support multiple applications—from VoIP trunking to hosted enterprise and residential services; multiple protocols—SIP, H.323, MGCP/NCS and H.248; and multiple border points—interconnect, access network and data center.

Established in August 2000 by networking industry veterans, Acme Packet is a public company trading on the NASDAQ and headquartered in Bedford, Massachusetts.

Customer Questions, Comments, or Suggestions

Acme Packet is committed to providing our customers with reliable documentation. If you have any questions, comments, or suggestions regarding our documentation, please contact your Acme Packet customer support representative directly or email support@acmepacket.com.

Contact Us

Acme Packet
100 Crosby Drive
Bedford, MA 01730 USA
t 781 328 4400
f 781 275 8800
www.acmepacket.com

Overview

This chapter contains information you should review before you get started using Net-Net EMS.

Before You Start

This section contains the information you should review before you start the installation process.

Net-Net EMS and Net-Net 4000 SBC Compatibility

You should ensure that the version of Net-Net EMS you are using is compatible with the version of software on the Net-Net 4000 SBCs you plan to manage. The following table lists the released versions of Net-Net 4000 SBC software and indicates compatibility with the Net-Net EMS releases.

| Net-Net SBC | Net-Net EMS | | | | | | | | | | | | |
|-------------|-------------|-------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|---|
| | 4.0 | 4.0.1 | 4.1 | 4.2 | 4.3 | 5.0 | 5.1 | 6.0 | 6.1 | 6.2 | 6.3 | 6.4 | |
| 4.0 | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| 4.0.1 | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| 4.1 | N | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| 4.1.1 | N | N | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| 4.1.4 | N | N | N | N | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| 5.0 | N | N | N | N | N | Y | Y | Y | Y | Y | Y | Y | Y |
| 5.1 | N | N | N | N | N | N | Y | Y | Y | Y | Y | Y | Y |
| 5.1.1 | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | Y |
| 6.0 | N | N | N | N | N | N | N | Y* | Y | Y | Y | Y | Y |
| CX6.0 | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y |
| C6.0M1 | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y |
| SC6.1 | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y |
| SCX6.1 | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y |
| SCX61M2 | N | N | N | N | N | N | N | N | N | N | Y | Y | Y |
| C6.0M2 | N | N | N | N | N | N | N | N | N | N | Y | Y | Y |
| C6.0M3 | N | N | N | N | N | N | N | N | N | N | Y | Y | Y |
| SC6.1M2 | N | N | N | N | N | N | N | N | N | N | Y | Y | Y |
| SC6.2 | N | N | N | N | N | N | N | N | N | N | Y | Y | Y |

| | Net-Net EMS | | | | | | | | | | | | |
|-------------|-------------|-------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|--|
| Net-Net SBC | 4.0 | 4.0.1 | 4.1 | 4.2 | 4.3 | 5.0 | 5.1 | 6.0 | 6.1 | 6.2 | 6.3 | 6.4 | |
| SCX6.1M2 | N | N | N | N | N | N | N | N | N | N | Y | Y | |
| MC1.0 | N | N | N | N | N | N | N | N | N | N | Y | Y | |
| C6.0M4 | N | N | N | N | N | N | N | N | N | N | N | Y | |
| SCX6.1M1 | N | N | N | N | N | N | N | N | N | N | N | Y | |
| SCX6.1M3 | N | N | N | N | N | N | N | N | N | N | N | Y | |
| SCX6.1M4 | N | N | N | N | N | N | N | N | N | N | N | Y | |
| SC6.1M3 | N | N | N | N | N | N | N | N | N | N | N | Y | |
| SC6.1M4 | N | N | N | N | N | N | N | N | N | N | N | Y | |
| SC6.2M1 | N | N | N | N | N | N | N | N | N | N | N | Y | |
| SC6.2M2 | N | N | N | N | N | N | N | N | N | N | N | Y | |
| CX6.0M1 | N | N | N | N | N | N | N | N | N | N | N | Y | |
| CX6.0M2 | N | N | N | N | N | N | N | N | N | N | N | Y | |
| CX6.0M3 | N | N | N | N | N | N | N | N | N | N | N | Y | |
| CX6.0M4 | N | N | N | N | N | N | N | N | N | N | N | Y | |

* Net-Net EMS 6.0 can manage Net-Net SBC 4000 version 6.0 but does not support all features.

Contact your Acme Packet representative if you have questions about compatibility between Net-Net EMS and Net-Net 4000 SBCs.

Minimum Net-Net SBC Configuration

The Net-Net SBCs you plan to manage using Net-Net EMS must have the following information configured in order to be discovered. To verify the minimum configuration for Net-Net SBCs you plan to manage, see the following documentation:

- *Net-Net EMS 4000 Configuration Guide* for details about configuring a Net-Net SBC using the Acme Command Line Interface (ACLI)
- *Net-Net ACLI Reference Guide* to refer to all ACLI commands.

Boot Parameters

Boot parameters specify the information your Net-Net SBC system uses at boot time when it prepares to run applications. The Net-Net SBC system's boot parameters include the Net-Net SBC system's IP address for the management interface (wancom0) and the target name.

Net-Net EMS uses the target name to uniquely identify a Net-Net SBC from among the list of Net-Net SBCs in its Active configuration area. You need to ensure that all Net-Net SBCs you plan to manage, thus discover, with Net-Net EMS have unique target names. Otherwise, a list of Net-Net SBCs, all with the default name acmesystem would appear in the list.

Ensure the following boot parameters have been configured:

- wancom0 IP address and mask

- target name is set to a unique name (do not use the default name acmesystem)

System Configuration Element

You need to ensure the **system-config** element has been configured. This element establishes general system information and settings, for example:

- Contact information for this Net-Net SBC system for SNMP purposes
- Identification of the Net-Net SBC system for SNMP purposes
- Physical location of the Net-Net SBC system for SNMP purposes
- Whether SNMP is enabled on the system
- Whether traps are enabled
- default gateway

For complete details about system configuration, see the *Net-Net 4000 Configuration Guide* and the *Net-Net ACLI Reference Guide*.

SNMP Community Element

You need to ensure the **snmp-community** element is configured. This element defines the NMSes from which the Net-Net SBC system will accept SNMP requests. Specifically, you need to ensure:

- IP address list contains the address of the host upon which EMS server is running. IP address(es) for SNMP communities for authentication purposes.
- Access mode is read-only

Note: Discovery will fail if SNMP is not configured properly.

Trap Receiver Element

You need to ensure the **trap-receiver** element is configured. This element defines the NMSes to which the Net-Net SBC system sends SNMP traps for event reporting. Specifically, you need to ensure the following:

- IP address is that of the Net-Net EMS server
- Filter level is set to All
- Community name matches the name in the SNMP community element

Instructions Based on Mozilla Firefox 1.06

The instructions in this document are based on Mozilla Firefox 1.06. The instructions are the same for Internet Explorer, except where noted. For example, when connecting to the Net-Net EMS server using the secure login, additional security messages appear.

All screen examples are those from Mozilla Firefox 1.06.

Introduction

This chapter explains how to use the Net-Net EMS Graphical User Interface (GUI). It explains how to logon to Net-Net EMS, the relationship between Net-Net EMS and the Acme Command Line Interface (ACLI), and contains descriptions of the GUI itself.

About the Relationship with ACLI

The Net-Net EMS provides a GUI-based approach to managing Net-Net SBCs. It provides the ability to configure and monitor standalone Net-Net SBCs and HA pairs. The ACLI is an administrative interface that communicates with other components of the Net-Net system. The ACLI is a single DOS-like, line-by-line entry interface that you can use to configure and monitor your Net-Net family of products.

You can use the Net-Net EMS to perform almost all the same configuration and monitoring functions that can be performed using the ACLI. (See the *Net-Net ACLI Reference Guide* for more information about using the ACLI.) You can use both interfaces to work with Net-Net SBCs; even switching from Net-Net EMS to login to a Net-Net SBC and use the ACLI.

Basic Workflow

The basic provisioning cycle includes the following:

- Discover a Net-Net SBC configuration.
- Copy the discovered Net-Net SBC configuration to the Inactive configurations area to edit it.
- Edit the inactive copy of the Net-Net SBC configuration.
- Save the edited Net-Net SBC configuration and activate it.

Accessing the Net-Net EMS GUI

You can access the Net-Net EMS GUI by HTTP or HTTPS login, using the following address formats:

`http://<EMS server IP address>:9090`

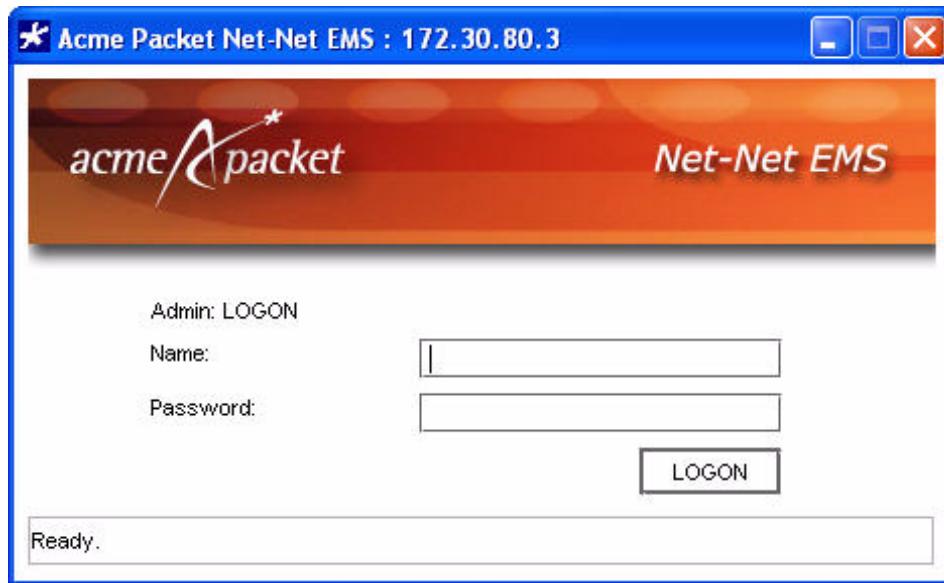
`https://<EMS server IP address>:8443`

Note: If you want to connect to EMS servers over a SSL connection, you must have administrator privileges on the client system.

HTTP Login

To access the Net-Net EMS GUI:

1. Open a Web browser.
2. Connect to the Net-Net EMS server using one of the following address formats:
`http://<EMS server IP address>:9090`
The Login screen appears.



3. Enter your user name and password and click LOGON. (The default username is **admin**, with a default password of **admin**.)

Go to the *After You Login* section to continue.

HTTPS Login Using Microsoft Internet Explorer 6.0

The process for a secure login using Microsoft Internet Explorer 6.0 includes first accepting or rejecting the security certificate.

To login using Microsoft Internet Explorer 6.0:

1. Open Microsoft Internet Explorer 6.0.
2. Connect to the Net-Net EMS server using the following address format:
`https://<EMS server IP address>:8443`

A Security Alert screen appears:



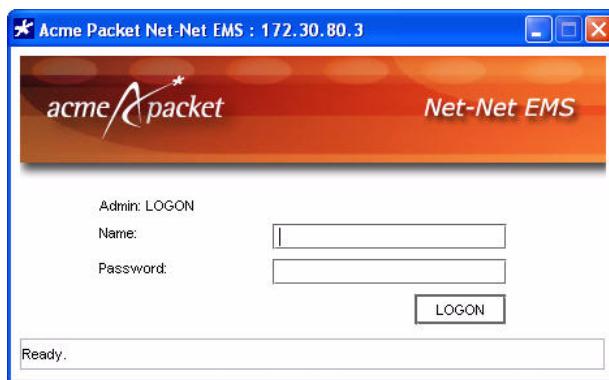
3. Click **Yes** to continue. The Warning - Security screen appears:



4. Click one of the following:

- **Yes** to accept the security certificate for this session only and to access the Login screen.
- **No** if you want to reject the security certificate and discontinue the login process.
- **Always** to permanently accept the security certificate, prevent this screen from appearing, and access the Login screen.
- **More Details** for more information.

If you choose **Yes** or **Always**, the Login screen appears.



5. Enter your user name and password and click **LOGON**. (The default username is **admin**, with a default password of **admin**.)

Go to the *After You Login* section to continue.

HTTPS Login Using Mozilla Firefox 1.0

The process for a secure login using Mozilla Firefox 1.0 includes first accepting or rejecting the security certificate.

To login using Mozilla Firefox 1.0:

1. Open Mozilla Firefox 1.0.
2. Connect to the Net-Net EMS server using the following address format:

https://<EMS server IP address>.8443

A Website Certified by an Unknown Authority screen appears:



3. Click one of the following options and click **OK**:
 - Accept the certificate permanently
 - Accept the certificate temporarily for the session (this window will appear each time you connect to the Net-Net EMS server)
 - Do not accept the certificate and do not connect to the web site

If you choose to accept the certificate permanently or temporarily, the Security Warning appears:



4. Ensure the checkbox is marked if you want this warning to appear each time you view an encrypted page. If you deselect the checkbox, this warning will not appear again.
5. Click **OK** to clear the Security Warning. The Opening WebNMS.jnlp window appears:

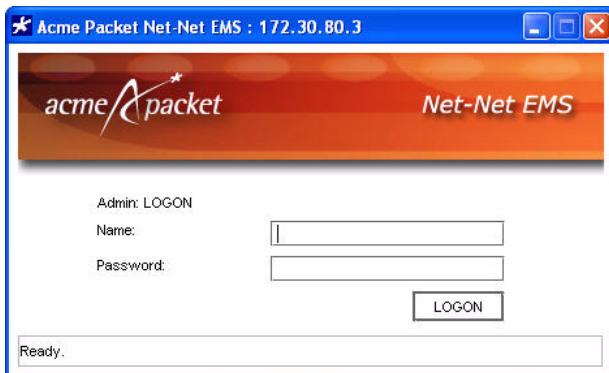


6. Click open it with the default application (JNLPFile) and Always perform this action when handling files of this type. This popup will not appear next time you connect.
7. Click OK. The Warning - Security screen appears:



8. Click one of the following:
 - Yes to accept the security certificate for this session only and to access the Login screen.
 - No if you want to reject the security certificate and discontinue the login process.
 - Always to permanently accept the security certificate, prevent this screen from appearing, and access the Login screen.
 - More Details for more information.

If you choose Yes or Always, the Login screen appears.

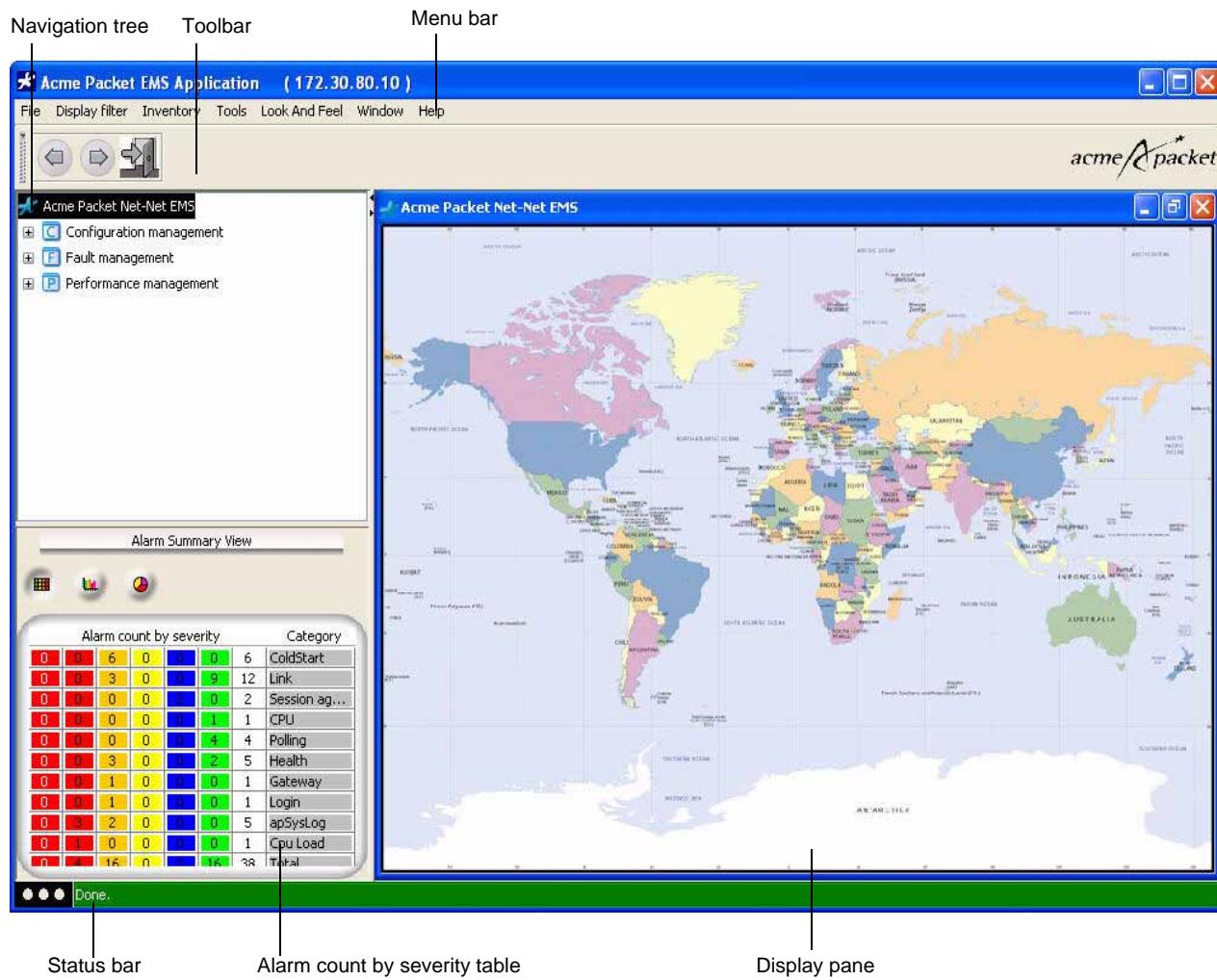


9. Enter your user name and password and click LOGON. (The default username is admin, with a default password of admin.)

Go to the *After You Login* section to continue.

After You Login

The Acme Packet splash screen appears displaying a progress bar while contacting Net-Net EMS. Next, the top-level Net-Net EMS screen appears:



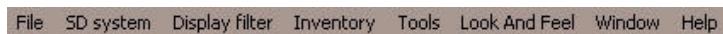
Overview of Net-Net EMS GUI

The top-level screen is divided into the following areas:

- Menu bar across the top of the window
- Toolbar located under the menu bar
- Navigation tree in the upper left pane
- Alarm count by severity table in the lower left pane
- Display pane on the right side of the window
- Status bar across the bottom of the screen

Menu Bar

The menu bar across the top of the screen contains sets of functions you can perform organized into different categories (menus). You click a menu to access a list of options, from which you then select the function you want to perform. (Many of these functions are also available when you right-click objects in the Navigation tree.)



The menu bar differs from screen to screen based on the functions being performed and on your privileges as a user. For example, the Active configurations module has the additional menu item called Add domain. Other menu items remain constant, such as File, Tools, Look And Feel, Window, and Help.

The following table lists the menus and their options; including a brief description

| Menu | Menu Item | Description |
|---|-------------------------------|--|
| File | Broadcast message | Send messages to clients connected to the server |
| | Logout | Exit Net-Net EMS |
| Save all (Inactive configurations) | Save All | Not currently supported |
| SD system | Save configuration | Saves the current configuration to the Net-Net system's last-saved configuration, stored in flash memory |
| | Activate config | Activates the current configuration on the Net-Net SBC to make it the running configuration |
| | Save and Activate config | Saves and then activates the configuration |
| | Display configuration changes | Displays the currently-staged configuration changes |
| | Copy for Edit | Copies an active configuration to the Inactive configuration area for editing purposes |
| | Create offline configuration | Copy an existing active or inactive configuration and modify the existing parameters offline |

| Menu | Menu Item | Description |
|----------------|--------------------------------|---|
| | Replicate | Replicates selected configuration data from one inactive Net-Net SBC configuration copy to another. Data includes: <ul style="list-style-type: none">• account configuration• authentication• capture receiver• SIP manipulation• SNMP community• NTP configuration• session agents• session agent groups• routes• trap receiver |
| | Search configuration | Allows you to search for, view, and edit top-level objects |
| | Configuration inventory | Lists the total number of configuration elements for each type configured on the Net-Net SBC |
| Display filter | Syslog filter | View existing syslog filters and create new filters to apply to the syslog view |
| Inventory | Inventory details | Access the Inventory window from which you can choose the different standalone Net-Net SBCs or Net-Net SBC pairs for which you want to review inventory data. |
| Tools | View license | Monitor the number of Net-Net SBCs and the total number of concurrent sessions under management by the Net-Net EMS server |
| | Runtime administration | Currently not supported by Net-Net EMS |
| | Security administration | Access the Security Administration tool. Users who have administration privileges can control the different security levels of Net-Net EMS. |
| | Password Notification Interval | Set the password notification interval (in days). The default is 3 days. This means you will be notified 3 days prior to your password expiring. |
| | Alarm Synchronization | Displays: Alarm synchronization console, which lists: <ul style="list-style-type: none">• IP Address• Start Time• Submit Time• Status You can refresh alarms or synchronize alarms. You can enable Alarm Synchronization in two ways: <ul style="list-style-type: none">• upon device discovery• upon device reconnection |
| | External trap receivers | Configure IP addresses to receive SNMP traps or edit existing external trap receivers. |
| | Audit logs | View the audit log. The audit log provides information about the changes made to the copies of Net-Net SBCs while using the Net-Net EMS. |
| | Client log level | Configure the client log levels. See <i>Configuring External Trap Receivers</i> for details about configuring logs. |
| | Change password | Change the password used to login to Net-Net EMS. Net-Net EMS uses Java's Password Based Encryption (PBE) to encrypt passwords on the EMS server. |

| Menu | Menu Item | Description |
|----------------------|---------------------------|--|
| | Login Banner | Add text to the login screen as a banner that is displayed when you login to Net-Net EMS |
| | Task Administration | Access the task administration console |
| | Operation Administration | Access the operation administration console |
| | Work Order Administration | Launches the work order administration tool |
| | EMS HA SFTP Settings | Set HA SFTP user name and password |
| Look and Feel | Metal | Apply Metal look to GUI appearance |
| | CDE/Motif | Apply CDE/Motif look to GUI appearance |
| | Windows | Apply Windows look to GUI appearance |
| | Windows Classic | Apply Windows Classic look to GUI appearance |
| Window | Show toolbar | Display or hide the toolbar |
| Help | Help Topics | Access the Net-Net EMS online help |
| | About Acme Packet EMS | Access Acme Packet version and contact information |

Toolbar

The toolbar displays a collection of actions, commands, or control functions. It is placed below the menu bar and consists of various tools for different nodes. A tool tip indicates the operation performed by each tool.

Scroll backward and forward through Navigation tree choices.



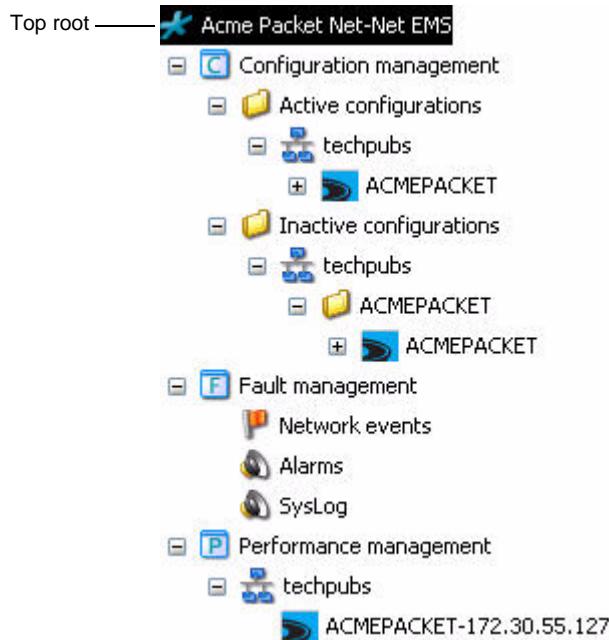
Click to hide/display toolbar.

Note: The Show toolbar option located on the Windows menu is not currently supported by Net-Net EMS.

Navigation Tree

The upper section of the left pane is called the Navigation tree. The Navigation tree is divided into three categories under the top node or root (Acme Packet Net-Net EMS). Each category contains objects called nodes, each of which represents a Net-Net SBC data item. Those nodes in turn can contain additional data items.

The following example shows a Navigation tree with all categories fully expanded to display all the nodes:



The Navigation tree contains the following three functions:

- **Configuration management:** where you discover and configure a Net-Net SBC. The Active configurations area contains a list of all discovered Net-Net SBCs and reflects the current configuration each of them. You cannot modify these configuration values. You need to make a copy of the Net-Net SBC in this area, which is placed in the Inactive configurations area, in order to make configuration changes.
- **Fault management:** where you monitor alarms, events, and syslog.
- **Performance management:** which displays real-time, on-demand performance statistics for monitoring performance and utilization. For example, system, session agent-, and realm-based session information. You can export this information to .CSV format.

Net-Net EMS Standalone Net- Net SBC and HA Pair Icons

The following chart displays the Net-Net EMS icons for standalone Net-Net SBCs.

| | Net-Net 4000 | Net-Net 9000 | Net-Net 4500 | Net-Net 3800 |
|-----------------------------|--------------|--------------|--------------|--------------|
| Standalone | | | | |
| Discovery | | | | |
| Rediscovery | | | | |
| Configuration Change | | | | |
| Save | | | | |

| | Net-Net 4000 | Net-Net 9000 | Net-Net 4500 | Net-Net 3800 |
|---|--------------|--------------|--------------|--------------|
| Save and Activate | | | | |
| Full Save | | | | |
| Full Save and Activate | | | | |
| Lock | | | | |
| Delete | | | | |
| Configuration Operations Lockout | | | | |

The following chart displays the Net-Net EMS icons for HA pairs of Net-Net SBCs.

| HA Pairs | Net-Net 4000 | Net-Net 4500 | Net-Net 3800 |
|---|--------------|--------------|--------------|
| Standalone | | | |
| Discovery | | | |
| Configuration Change | | | |
| Save | | | |
| Save and Activate | | | |
| Full Save | | | |
| Full Save and Activate | | | |
| Lock | | | |
| Delete | | | |
| Configuration Operations Lockout | | | |

Alarm Count by Severity Table

The lower left pane displays the Alarm count by severity table:

| Alarm count by severity | | | | | | | Category |
|-------------------------|---|----|---|---|----|----|---------------|
| 0 | 0 | 6 | 0 | 0 | 0 | 6 | ColdStart |
| 0 | 0 | 3 | 0 | 0 | 9 | 12 | Link |
| 0 | 0 | 0 | 0 | 2 | 0 | 2 | Session ag... |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | CPU |
| 0 | 0 | 0 | 0 | 0 | 4 | 4 | Polling |
| 0 | 0 | 3 | 0 | 0 | 2 | 5 | Health |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | Gateway |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | Login |
| 0 | 3 | 2 | 0 | 0 | 0 | 5 | apSysLog |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | Cpu Load |
| 0 | 4 | 16 | 0 | 2 | 16 | 38 | Total |

The Alarm count by severity table displays a summary of all alarms generated, by alarm severity and by category. The summary displays the number of alarms that are generated under various categories and severity levels. This table is automatically refreshed when alarms arrive at the Net-Net EMS server.

Each row in the Alarm count by severity table corresponds to a specific category of alarms. The number of rows correspond to the number of alarm categories. The last row provides the total number of alarms for each severity level.

See *Viewing Alarm Information* in the *Fault Management* chapter for details.

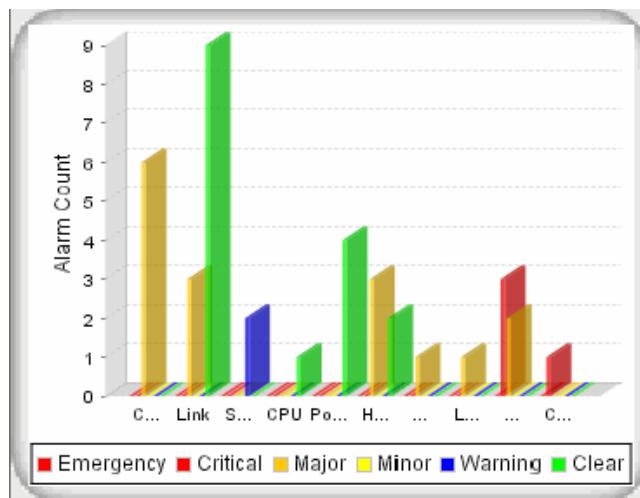
Changing the Alarm Table Presentation

You can change the presentation of the alarm summary information by clicking the following buttons.

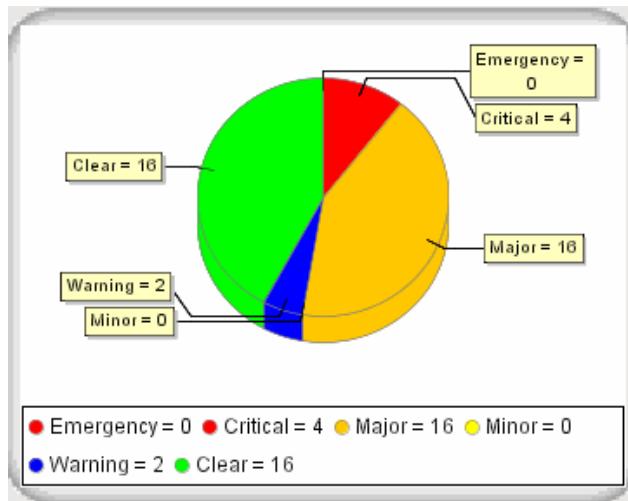


- displays the alarm information by severity and category in the table

-  displays the alarm information by severity and category in a stack chart



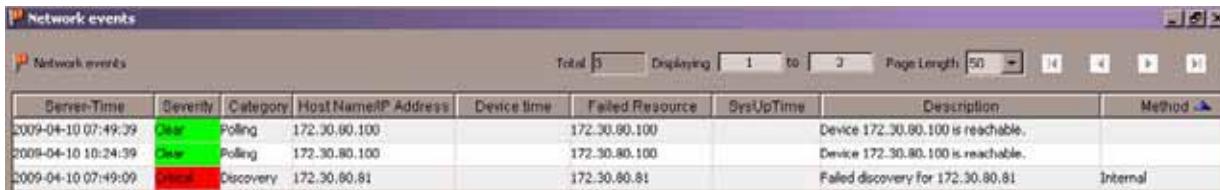
-  displays the alarm information by severity in a pie chart



Display Pane

The Display pane is displayed on the right side of the Net-Net EMS GUI and contains a map of the world when you first access Net-Net EMS. When you select an option from the Navigation tree, the result of the choice appears in the Display pane.

For example, if you choose Network events from the Fault management category, a list of network events appears in the Display pane:



| Network events | | | | | | | | |
|---|-----------|-----------|-----------------------|-------------|-----------------|-----------|------------------------------------|----------|
| Total [3] Deploying [1 to 3] Page Length [50] [First] [Previous] [Next] [Last] | | | | | | | | |
| Server-Time | Servertiy | Category | Host Name/ IP Address | Device time | Failed Resource | SysUpTime | Description | Method |
| 2009-04-10 07:49:39 | Clear | Polling | 172.30.80.100 | | 172.30.80.100 | | Device 172.30.80.100 is reachable. | |
| 2009-04-10 10:24:39 | Clear | Polling | 172.30.80.100 | | 172.30.80.100 | | Device 172.30.80.100 is reachable. | |
| 2009-04-10 07:49:09 | critical | Discovery | 172.30.80.81 | | 172.30.80.81 | | Failed discovery for 172.30.80.81 | Internal |

Status Bar

The Status Bar is located at the bottom of the screen.



It indicates the status of the current discovery or rediscovery process by displaying text and changing from green to blue. When the process completes, the final status of indicating whether the process is successful is displayed.

For example, if rediscovery has been initiated the message appears and the background color of the status bar changes from green to blue.



When rediscovery has completed successfully, a message appears. For example:



Right-Click Mouse Functions

You can right-click in both the Active and Inactive configuration areas to access pop-up lists of functions. To choose a function, click the function name.

Active Configuration Category

Right-click the Active configuration category to access the following function.

| Function | Description |
|---------------|---------------------|
| Create domain | Create a new domain |

Active Domain

Right-click a domain in the Active configuration area to access the following functions:

| Function | Description |
|----------|----------------------------|
| Rename | Rename the selected domain |
| Delete | Delete the selected domain |

Active Net-Net SBC Configuration

Right-click a Net-Net SBC configuration in the Active configuration area to access the following functions:

| Function | Description |
|------------------------------|--|
| Rediscovery | Rediscover this Net-Net SBC |
| Reboot | Reboot this Net-Net SBC |
| Set offline | Take this Net-Net SBC offline |
| Move | Move this Net-Net SBC configuration to another domain |
| Copy for edit | Copy this Net-Net SBC configuration to the Inactive configuration area |
| Create offline configuration | Create an offline configuration based on the selected Net-Net SBC configuration. You can then edit the offline configuration's parameters. |
| Delete | Delete this Net-Net SBC configuration from the Net-Net EMS navigation tree |
| Inventory Details | Access details about the hardware, software, and licenses associated with this Net-Net SBC |
| Telnet to SD System | Open a Telnet session to this Net-Net SBC |
| SSH to device | Open a Secure Shell session to this Net-Net SBC. You need a username and password for SSH authentication |
| HDR operations | Access HDR reporting operations |
| Registration Cache | Access Registration cache details for this active configuration |
| Lock | Lock the configuration node to prevent other users from performing any configurations on the same node |
| Unlock | Unlock the configuration node |
| Search configuration | Allows you to search for, view, and edit top-level objects |
| Configuration inventory | Access configuration inventory details for this active configuration. |
| Synchronize Alarms | Allows you to synchronize alarms for this Net-Net SBC |

Active SD HA Pair

Right-click an HA pair to access the following functions in addition to those in the active Net-Net SBC configuration table:

| Function | Description |
|----------------|---|
| Switch HA Role | Switch the role of the active node to standby. The standby node becomes the active one. |
| Reboot Active | Reboot the active Net-Net SBC |
| Reboot Standby | Reboot the standby Net-Net SBC |

Inactive Configuration Category

Right-click the Inactive configuration category to access the following functions:

| Function | Description |
|----------|-------------------------|
| Save all | Not currently supported |

Inactive Domain

Right-click the Inactive domain to access the following functions:

| Function | Description |
|------------------------------------|---|
| Create offline SD configuration | Create a new offline standalone Net-Net SBC configuration associated with this domain |
| Create offline SD HA configuration | Create a new offline Net-Net SBC HA configuration associated with this domain |
| Save all | Not currently supported |

Offline configuration lets you create configurations for devices that are not currently available. Using offline configuration lets you create a Net-Net SBC node that is not associated with a specific Net-Net SBC until you save the configuration to one.

Inactive Configuration Node

Right-click an inactive configuration node to access the following functions:

| Function | Description |
|----------|---|
| Rename | Rename the configuration node |
| Delete | Delete the configuration node |
| Lock | Lock the configuration node to prevent other users from performing any configurations on the copy of the node configuration |
| Unlock | Unlock the configuration node |

Inactive Net-Net SBC Configuration

Right-click a Net-Net SBC configuration in the Inactive configuration areas to access the following functions:

| Function | Description |
|-------------------------------|---|
| Save config | Saves the current configuration to the Net-Net system's last-saved configuration, stored in flash memory |
| Activate config | Activates the current configuration on the Net-Net SBC to make it the running configuration |
| Save and Activate config | Saves and then activates the configuration |
| Display configuration changes | Displays a session log detailing configuration changes for this inactive configuration |
| Copy for edit | Copy an inactive configuration for edit |
| Create offline configuration | Copy an existing active or inactive configuration and modify the existing parameters offline |
| Create SD HA node | Create an HA node with two Net-Net SBC configurations |
| Replicate | Replicates selected configuration data from one inactive Net-Net SBC configuration copy to another. Data includes: <ul style="list-style-type: none"> • session agents • session agent groups • routes |
| Search configuration | Allows you to search for, view, and edit top-level objects |
| Configuration inventory | Access configuration inventory details for this inactive configuration |

Inactive SD HA Pair

Right-click an HA pair to access the following functions:

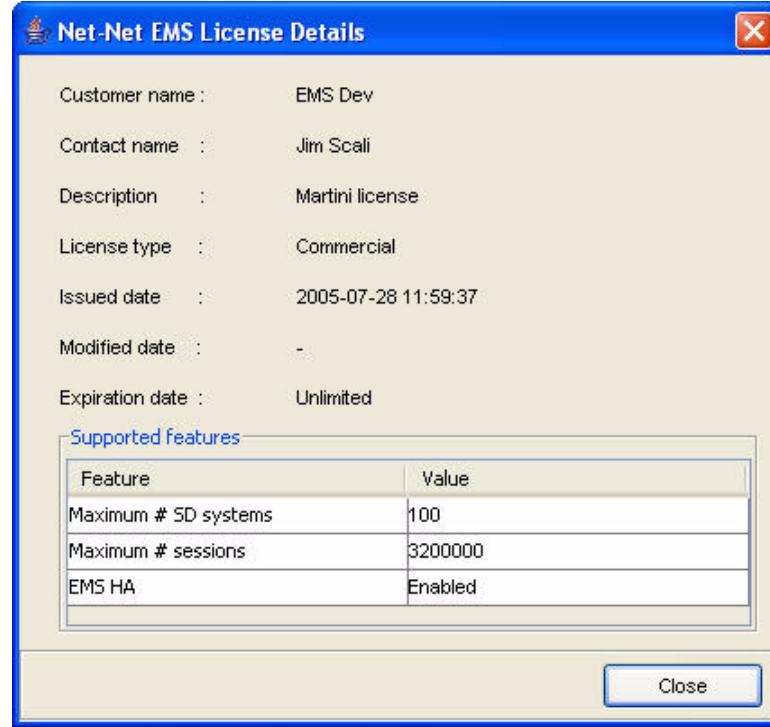
| Function | Description |
|------------------------------|--|
| Save and Activate Config | Saves the current configuration to the Net-Net system's last-saved configuration, stored in flash memory and activates it to make it the running configuration |
| Create offline configuration | Copy an existing active or inactive configuration and modify the existing parameters offline |
| Rename | Rename the configuration node |

Viewing Net-Net EMS License Information

This section explains how to view the Net-Net EMS license information.

To view license information:

- From the Tools menu, choose **view license**. The Net-Net EMS License Details window appears:



About the License Data

The following table defines the data displayed by Net-Net EMS for a standalone Net-Net SBC or for the Net-Net SBCs that belong to an HA pair:

| Data | Description |
|---------------|--|
| Customer name | Name of customer licensed to use Net-Net EMS |
| Contact name | Name of the contact person |
| Description | Descriptive text that describes the license |
| License type | Type of license issued: <ul style="list-style-type: none"> • Commercial: indicates Net-Net EMS is licensed for commercial use • Evaluation: indicates Net-Net EMS is licensed for evaluation purposes and beta deployments |
| Issued date | Date the Net-Net EMS license was issued in the format: yyyy-mm-dd hh:mm:ss |
| Modified date | Date modifications were made to the license in the format: yyyy-mm-dd hh:mm:ss |

| Data | Description |
|---------------------------|--|
| Expiration date | Date the Net-Net EMS license expires. Values are: <ul style="list-style-type: none"> • Unlimited for a Commercial license only • Specific date in the format: yyyy-mm-dd hh:mm:ss |
| Supported features | |
| Maximum # SD systems | Maximum number of Net-Net SBCs allowed in the Active configurations area. (The number in the Inactive configurations area does not count.) When the maximum number is exceeded, you cannot discover additional systems, apply offline configuration, or save to an offline Net-Net SBC. You must delete the excess number of Net-Net SBCs to proceed. Note: Net-Net SBC HA pair is considered a single system. |
| Maximum # sessions | Informational only |
| EMS HA | Whether EMS HA functionality is enabled |

Sending Broadcast Messages

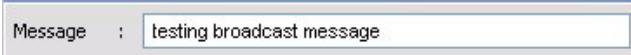
This section explains how to send (broadcast) messages to all the clients connected to the server.

To broadcast a message:

- From the File menu, choose **Broadcast Message**. The Broadcast Message dialog box appears:



- Message**—Type the message to be broadcast in the Message field. For example:



- Select the delivery option:

- Send to my FE client only**: The message is sent to all the clients connected to that specific Net-Net EMS server.
- Send to all clients**: The message is sent to all the clients connected to different Net-Net EMS servers.

- Click **Broadcast**.

The message is delivered to intended clients that are connected to the Web NMS Server and is displayed on the status bar.

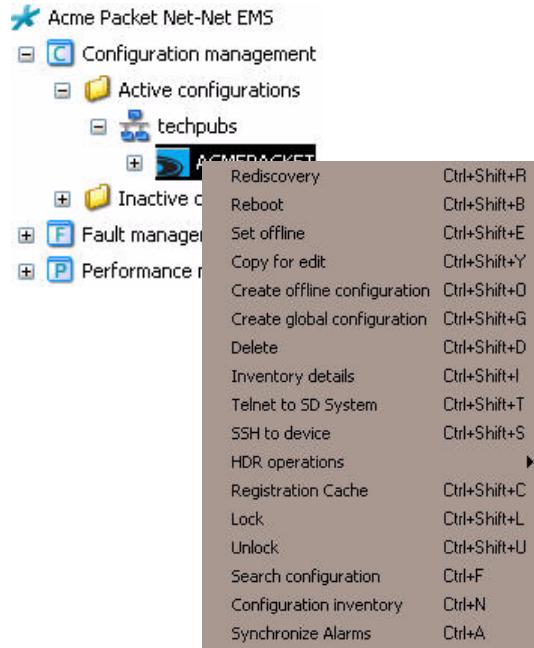


Connecting Using Telnet

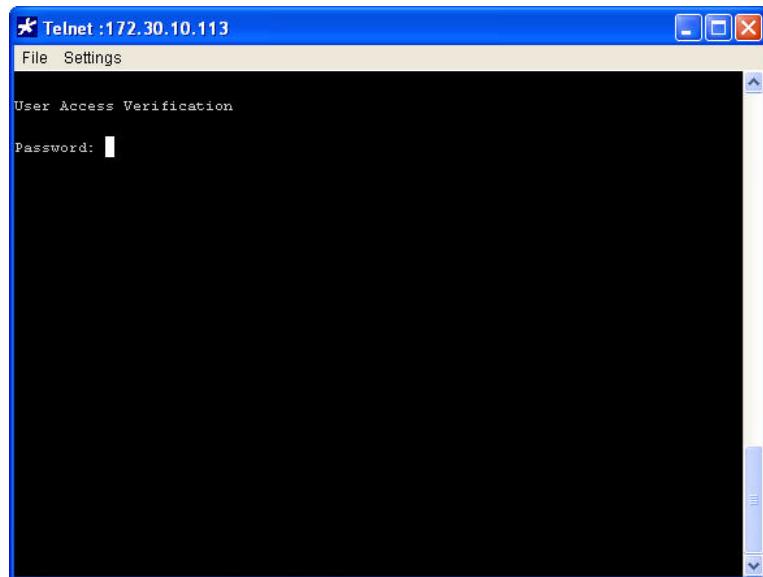
If you want to switch from configuring Net-Net SBCs in the Net-Net EMS to using the ACLI, you can connect through Telnet to the Net-Net SBC. You can then login in to continue working using the ACLI.

To connect using Telnet:

1. In the **Active configurations** area, right click the name of the Net-Net SBC. A list of options appears:



2. Click **Telnet to SD system**. The Telnet window appears:



3. Login to the Net-Net SBC. See the *Net-Net ACLI Reference Guide* for details about logging in and using the ACLI. See the *Net-Net EMS Configuration Guide* for details about configuring a Net-Net SBC using the ACLI.
4. Save the configuration to the Net-Net SBC to activate it.

Offline Configuration

Offline configuration lets you create configurations for devices that are not currently available. Using offline configuration lets you create a Net-Net SBC node that is not associated with a specific Net-Net SBC until you save the configuration to one.

Note: See the *Net-Net EMS Configuration Guide* for details about creating offline configurations.

You can create an offline configuration using one of the following methods:

- Copy an existing active or inactive configuration and modify the existing parameters
- Create an original configuration

Copying a Configuration

To copy an existing configuration:

1. In the **Active configurations** or **Inactive configurations** area, right-click the Net-Net SBC to access the popup menu. (You can also select an existing offline configuration.)
2. Click **create offline configuration**. The Create offline configuration dialog box appears:

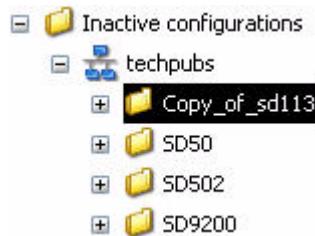


3. **Configuration name**—Edit the name of the copy if you do not want to retain the default.
4. Click **OK**. A status message appears indicating the request has been sent to the server.

When the process completes, the following message appears:



The copy appears under the Inactive configurations category of the Net-Net EMS navigation tree.

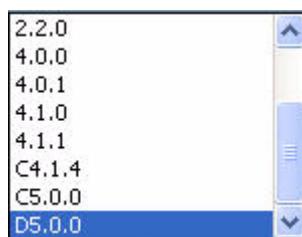


Refer to the *Net-Net EMS Configuration Guide* for details about configuring a Net-Net SBC.

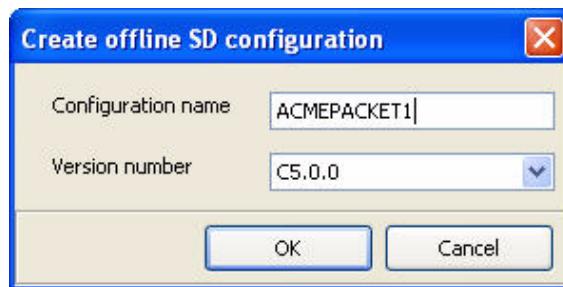
Creating an Original Configuration

To create an original configuration:

1. Click the domain to which you want to associate the new configuration under Inactive configurations.
2. Right-click the domain name to access the pop-up menu.
3. Click one of the following options:
 - Standalone Net-Net SBC: **Create offline SD configuration**
The Add offline SD configuration dialog box appears:
 - HA Net-Net SBC pair: **Create offline SD HA configuration**
The Add offline SDHA configuration dialog box appears:
4. **Configuration name**—In either dialog box, enter a name for this configuration.
5. Click the down arrow to access a drop-down list of versions.

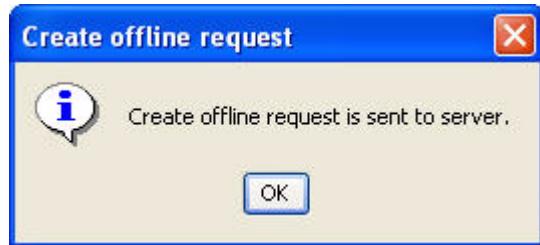


6. **Version number**—Click the version number to select it. For example:



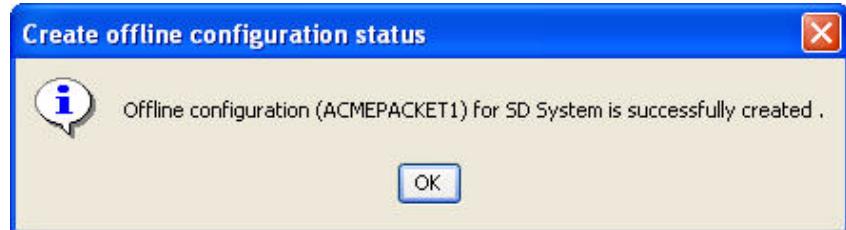
7. Click **OK**.

A message appears indicating the request has been sent to the server:



8. Click **OK** to clear the message.

When the process completes, the following message appears:



Refer to the *Net-Net EMS Configuration Guide* for details about configuring a Net-Net SBC.

Replicating Selected Configuration Elements

If you have the privilege to configure an SBC, you can replicate configuration information for the following elements from one inactive configuration copy to another:

- account configuration
- authentication
- capture receiver
- NTP configuration
- session agents
- session agent groups
- routes
- SIP manipulation
- translation rules
- translation profiles
- SNMP communities
- trap receivers

You need to ensure that all the configuration records referenced by the elements you are replicating have corresponding counterparts in the target configuration.

The target you choose for the data you are replicating must have a matching platform, a matching configuration (standalone or HA), and a matching version of Net-Net SBC software (6.0, 6.1).

Note: The existing configuration information on the target will be deleted and replaced by the replicated configuration data.

Record Validation

Net-Net EMS validates that all records referenced by the data being replicated in the source configuration have corresponding records in the destination copy. For example, all realm IDs that appear as source realm values in routes being copied must already exist with the same realm ID in the destination configuration.

Replicating Data

To replicate data:

1. In the Inactive configurations area, right click the Net-Net SBC from which you want to replicate data. A pop-up menu appears.

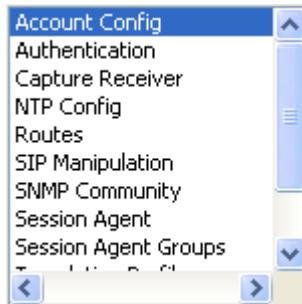
2. Click **Replicate**. The Selective Configuration Replication console appears.



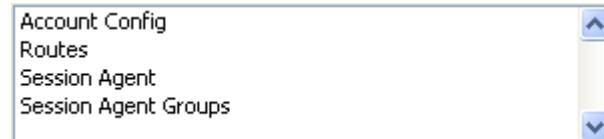
3. **Target Configuration**—Select the target configuration from the drop-down list.



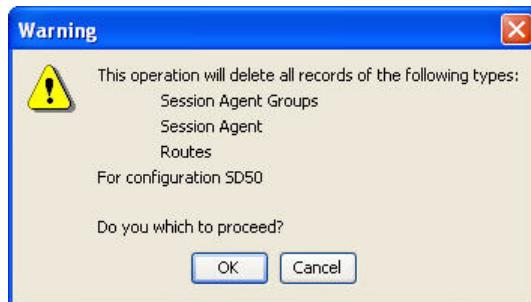
4. **Targeted groups**—Click **Add**. The Selective Configuration Replication selector window appears.
5. Click a group name in the Available Groups list to select it.



6. Click **< >** to move the group name to the Selected Groups list.
 - You can select multiple non-contiguous group names by holding down the CTRL key and clicking the different group names. Click **>** to move the multiple group names to the Selected Groups list.
 - You can move all groups from the Available Groups list to the Selected Groups list by clicking **>>**.
7. Click **OK** to save your selections and close the Selective Configuration Replication selector window. The group names you chose appear in the Targeted groups list.



8. Click **Start** to begin the replication. A warning message appears about existing data in the target configuration being deleted.



9. Click **OK** to proceed. The icon at the top of the window changes to indicate replication is in progress.

Net-Net EMS validates all records in the source configuration that are associated with the set of data being copied have corresponding records in the destination copy. For example, all realm IDs that appear as source realm values in routes being copied must already exist with the same realm ID in the destination configuration.

| 06/27/2007 10:58:01 : Request for replication submitted. | | | |
|--|--------|----------------------|-------------|
| ----- | | | |
| 06/27/2007 10:58:01 : Started replication processing for thread : Thread-594 | | | |
| ----- | | | |
| 06/27/2007 10:58:01 : Replication started from source : SD50 to target :SD50 | | | |
| ----- | | | |
| Operation | Status | Element Name | Object Name |
| Validation | true | SessionAgentGroup | N/A |
| Validation | false | SessionAgent | h323-sa |
| Validation | false | SessionAgent | sip-sa |
| Validation | false | SessionAgentCarriers | hong-carr1 |
| Validation | false | SessionAgentCarriers | hong-carr3 |
| ----- | ----- | ----- | ----- |

Validations for all elements are listed in the Replication log area. If validation fails, you can see which records were invalid, as well as the specific parameters within those records that cause the failure. Replication is cancelled and the target configuration is restored to its original state.

If validation fails, a message appears in the Replication log area.

| | | | |
|--|-------|--------------------------|-------------|
| Validation | false | SessionAgent | N/A |
| Validation | false | LocalPolicySourceRealm | access1 |
| Validation | false | LocalPolicySourceRealm | access3 |
| Validation | false | LocalPolicyAttribute | RPS |
| Validation | false | LocalPolicyAttribute | RPI |
| Validation | false | LocalPolicyMediaProfiles | hong1-media |
| Validation | false | LocalPolicyMediaProfiles | hong3-media |
| Validation | false | LocalPolicy | N/A |
| ----- | ----- | ----- | ----- |
| 06/27/2007 10:58:01 : Validation failed for target : SD502 | | | |
| 06/27/2007 10:58:01 : Exception thrown for thread : Thread-5945. Reason : Ab | | | |
| 06/27/2007 10:58:01 : Replication aborted for thread Thread-5945. | | | |
| 06/27/2007 10:58:01 : Replication process completed for thread Thread-5945. | | | |

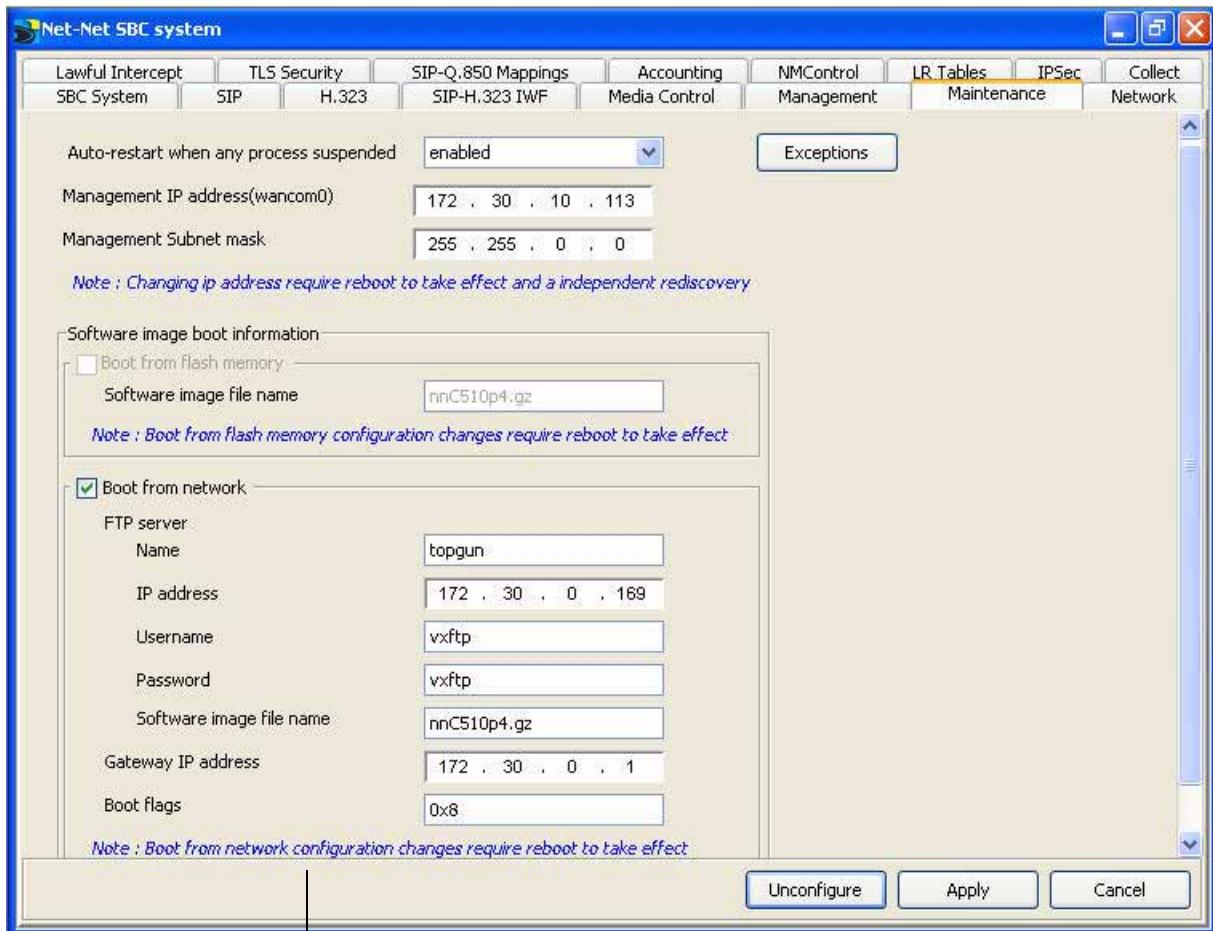
If validation is successful, all session agent, route, and route policy records are deleted from the target configuration and replaced with duplicates of the source configuration records. A message appears indicating replication was successful.

| | | | |
|--|--------|----------|---------|
| Replicate | routes | Route 8 | Success |
| Replicate | routes | Route 9 | Success |
| Replicate | routes | Route 10 | Success |
| <hr/> | | | |
| Commit Transaction @ 06/01/2007 14:35:05 | | | |
| Transaction completed successfully @ 06/01/2007 14:45:05 | | | |
| <hr/> | | | |
| Replication completed successfully @ 06/01/2007 14:45:40 | | | |
| <hr/> | | | |

10. Click **Export** if you want to save the replication log information to a file.
11. Click **Close** to exit the Selective Configuration Replication console.

Reboot Notices

Some Net-Net SBC configuration parameters require a reboot of the system if the values are changed. On-screen notifications about the need to reboot the Net-Net SBC are included where required. For example if managing Net-Net 4000:



Notice indicates that you need to reboot after editing these values.

Configuring External Trap Receivers

This section describes the Net-Net EMS traps contained in the Acme Packet EMS MIB and the configuration of the external trap receivers. Net-Net EMS generates traps when it detects the following:

- Failure to discover or rediscover a Net-Net SBC configuration
- Failure to save a Net-Net SBC configuration
- Failure to activate a Net-Net SBC configuration
- Missing components when validating a Net-Net SBC configuration
- Node status change from reachable to unreachable

You need to configure an external server as the receiver for these traps.

About Net-Net EMS Traps

Net-Net EMS generates the following traps.

| Trap | Description |
|---|--|
| apEMSDiscoveryFailure | Generated when Net-Net EMS fails to discover or rediscover a Net-Net SBC configuration. The trap is generated from any discovery or rediscovery failure initiated by the SOAP XML API, Net-Net EMS, or system processing. The trap contains the Net-Net SBC's node ID, the start and end time of the discovery or rediscovery operation, and the user who initiated the operation. |
| apEMSSaveFailNotification | Generated when Net-Net EMS fails to save a configuration. The trap is generated by a save failure whether initiated by the SOAP XML API or Net-Net EMS GUI for the save/activate, save, or offline save operations. The trap contains the Net-Net SBC node ID, the start and stop time of the save configuration attempt, and the user initiating the save operation. |
| apEMSActivateFailNotification | Generated when Net-Net EMS fails to activate a configuration, whether initiated from the SOAP XML API or the Net-Net EMS GUI for the save/activate or activate operations |
| apEMSIInvalidConfigDiscoveredNotification | Generated when Net-Net EMS validates a discovered Net-Net SBC's configuration (for example, confirms each referenced realm is configured) and detects missing components. The trap contains the time and the Net-Net SBC node ID. |
| apEMSNNodeUnreachableNotification | Generated when a node's status changes from reachable to unreachable. The trap contains the Net-Net SBC's node ID and the time of the event. |
| apEMSNNodeUnreachableClearNotification | Clearing condition trap. Generated when a node's status changes from unreachable to reachable. The trap contains the Net-Net SBC's node ID and the time of the event. |

Notification Objects

The Acme Packet EMS MIB also lists the following notification objects, the information for which is contained in the generated traps.

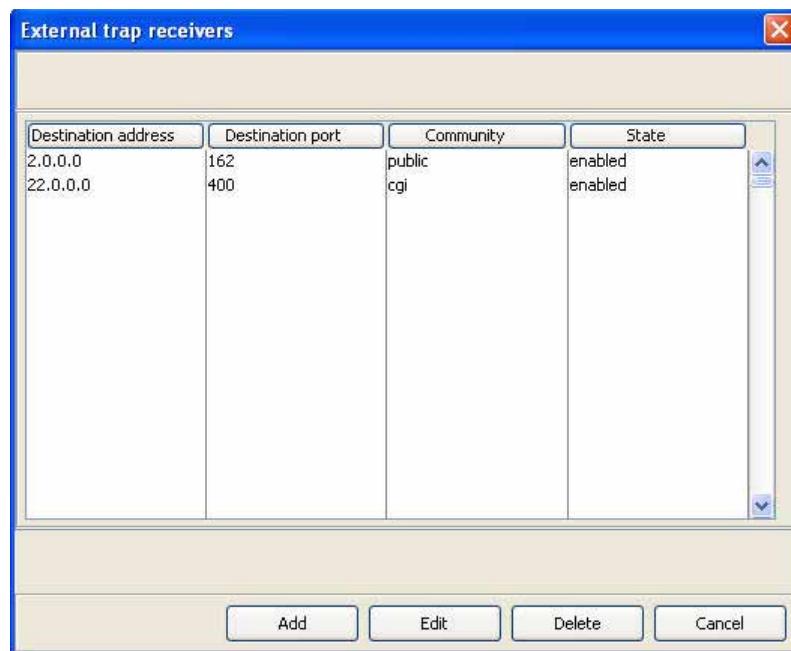
| Notification Objects | Description |
|----------------------|--|
| apEMSDiscoveryMode | Discovery mode values: unknown(0) discovery(1) reDiscovery(2) |
| apEMSNodeID | Identifier for a Net-Net EMS node that appears on the navigation tree in the Active configuration area on the Discovery table in the Host Name/IP Address column |
| apEMSStartTime | Time as configured on the EMS server when an event occurs |
| apEMSDateTime | Time as configured on the EMS server when an event completes |
| apEMSUser | User initiating the function. If the function was automatically initiated by the Net-Net EMS application, the user is system. |
| apEMDeviceAddress | Address for a device being managed |

Configuring External Trap Receivers

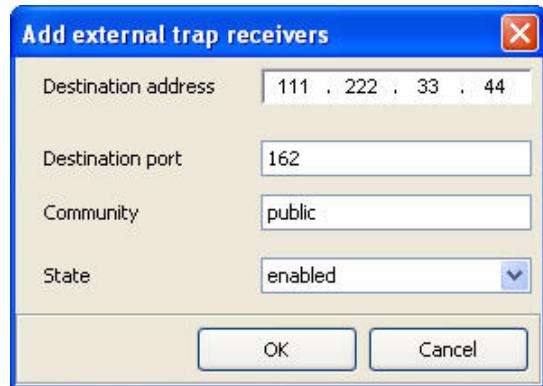
An external trap receiver is a server that you use as the trap destination, instead of the server where Net-Net EMS is installed. When you configure the external trap receiver, you enter its address and port. The combination of IP address and port must be unique for each configured trap receiver.

To configure external trap receivers:

1. Login to Net-Net EMS.
2. From the Tool menu, choose **External trap receiver**. The External trap receivers table appears:



3. Click **Add**. The Add external trap receivers dialog box appears.
4. **Destination address**—Enter the IP address of the server receiving the traps.
5. **Destination port**—Enter the port number for the server receiving the traps or retain the default value of 162.
6. **Community**—Enter the name of the SNMP community to which the server receiving traps belongs or retain the default value **public**.
7. **State**—Retain the default value **enabled**.



8. Click **OK**.

A validation is performed on the destination address and port. If either or both cannot be validated the following message appears.



A validation is also performed on the community name. If left blank, the following message appears.



9. If necessary, click **OK** to clear the error message.

The new trap receiver appears in the External trap receivers table.

You can edit an existing trap receiver to change its SNMP community name and state; you cannot edit the destination address and port.

Using Net-Net EMS Client Logs

This section explains how to use Net-Net EMS client logs. Client logs contain messages about the following Net-Net EMS client-side processes:

- Discovery
- Configuration
- Fault
- Miscellaneous (all other processes that do not fall under the first three categories)

To view the messages, you need to enable the Java console and set the client log levels. Messages are then written to the Java console and you can review them online, save them to a file, or both.

Enabling the Java Console

You enable the Java console by configuring the Java Web Start application.

To enable the Java console:

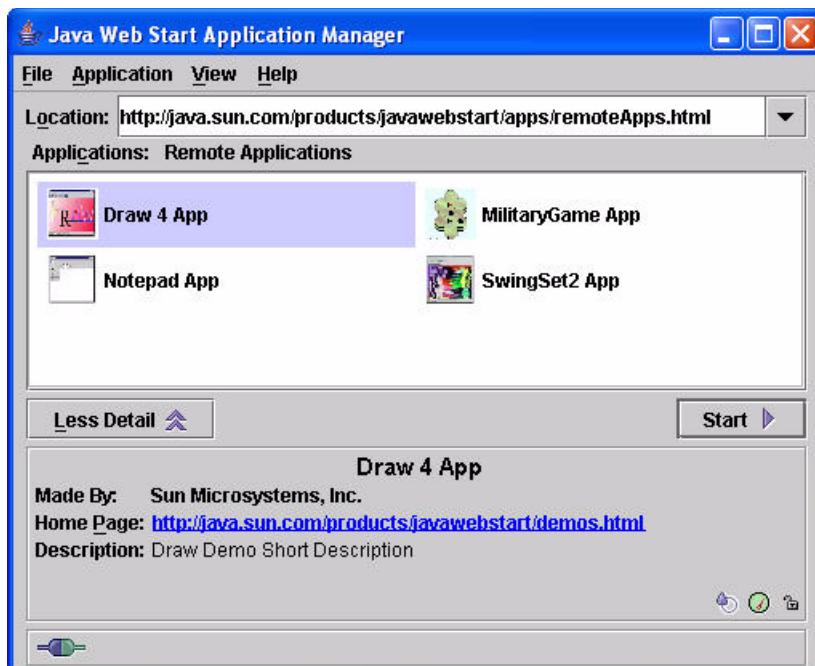
1. Click **Start**, then **All Programs**, and choose **Java Web Start** from the list.

or

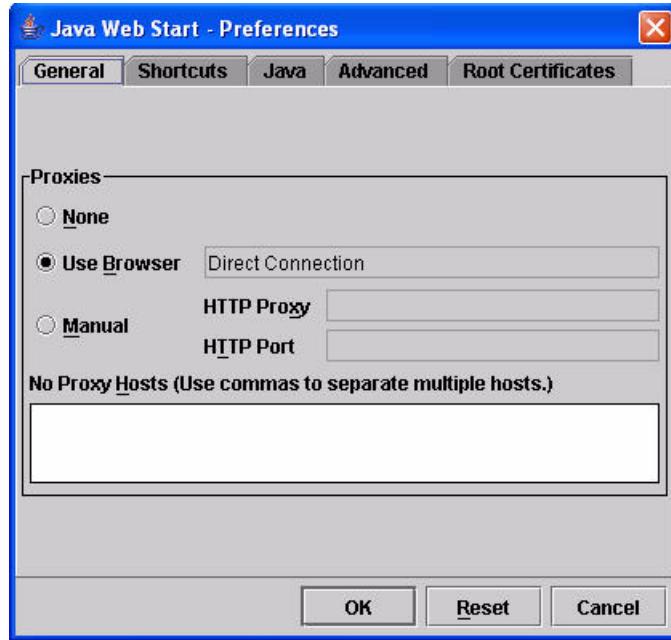


Double-click **Java Web Start** on your desktop (if present).

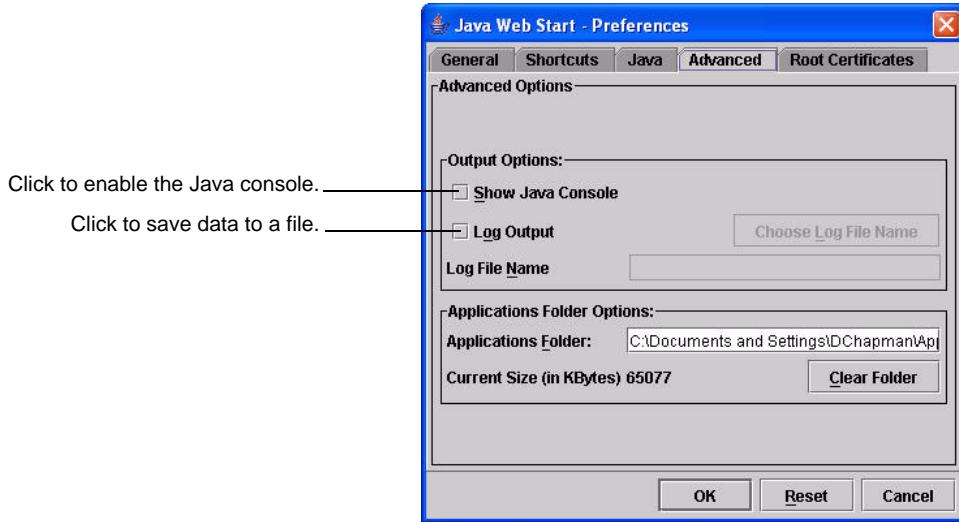
The Java Web Start Application Manager appears:



- Choose Preferences from the File menu. The Java Web Start Preferences window appears:



- Click the Advanced tab. The Advanced Options appear:



Note: You can choose to view the data online, save the data to a file, or do both.

- To view the data online, click **Show Java Console** to enable the display of the Java console. The Java console will start after you connect to the Net-Net EMS. It appears along with the Login screen.
If you want to review the Java console logs online, go to step 7. If you want to save the data to a file, continue to the next step.

5. **Log Output**—To save the Java console logs to a file, click **Log output** to activate the **Log File Name** textbox:



6. **Log File Name**—Enter a name for the file (for example, emsclientlog.txt) or click **choose Log File Name** to browse to file you want to use.

Data is written to the file you name when the Java console starts. If you have also chosen to enable the Java console display, the same data appears in the Java console.

7. Click **OK** to return to the Java Web Start Application Manager window.
8. Exit the Java Web Start Application Manager.

Starting the Java Console

To start the Java console:

1. Ensure you have enabled the Java console display in the Java Web Start application.
2. Connect to the Net-Net EMS server using the following address format:

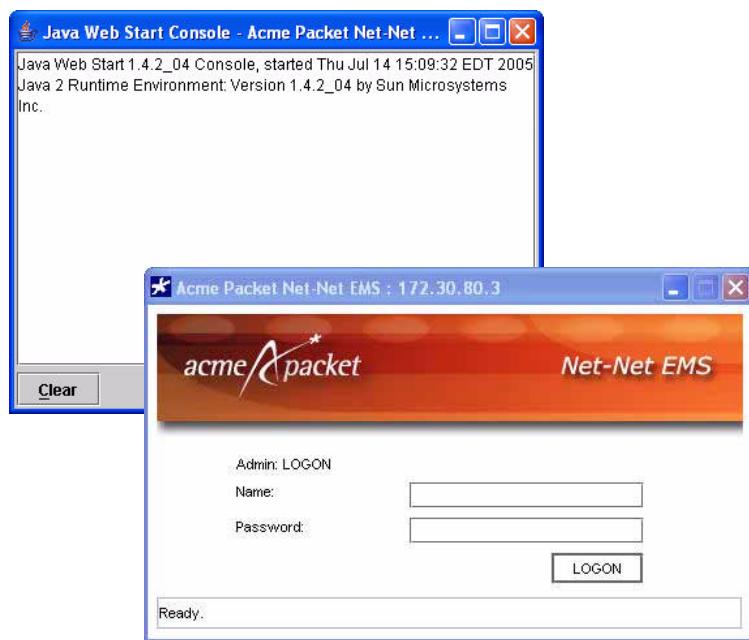
http://<EMS server IP address>:9090

Note: If your system has been configured for HTTPS login, you need to use the following address format to connect:

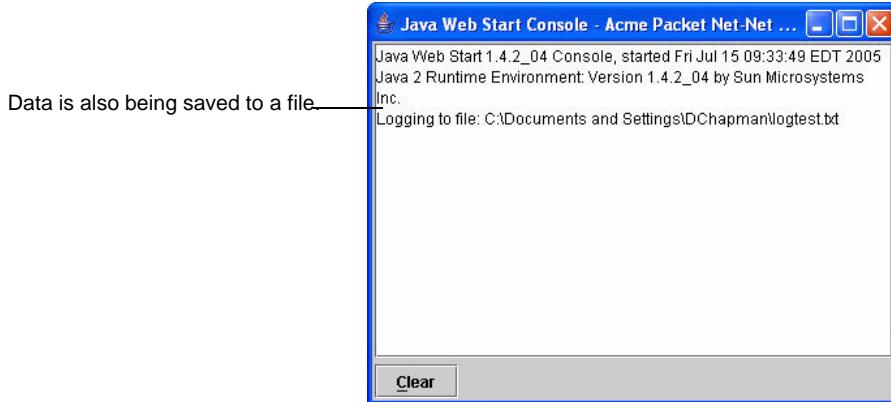
https://<EMS server IP address>:8443

See *HTTPS Login Using Microsoft Internet Explorer 6.0* or *HTTPS Login Using Mozilla Firefox 1.0* for details about the security windows that appear when you connect using HTTPS.

Because you have enabled the Java console, it appears along with the Login screen:



If you also chose to save data to a file, the Java console displays the complete path and filename:



You can minimize the Java console and continue with the Net-Net EMS login. See *Accessing the Net-Net EMS GUI* for details. After you login to Net-Net EMS, you can configure the client log levels for the current session.

Configuring the Client Log Levels

When you configure the client log levels, you are configuring them for the current session. If you logout and login again, you have started a new session and the log levels have reverted to the default values.

To configure the client log levels for the current session:

1. Login to Net-Net EMS.
2. From the Tool menu, choose `Client log level`. The Configure client log levels window appears:



Note: Acme Packet recommends you use either NONE or DEBUG for log levels. Set the client log levels to NONE if you do not need to log information for the current session. Retain the DEBUG level if you need to log error information for diagnostic purposes.

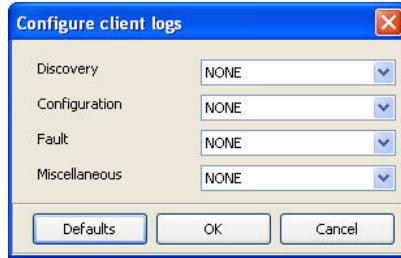
For example, if an Acme Packet representative asks you to provide a log of client process information, you set the level to DEBUG and enable the Java console to save the data to a file. See "Enabling the Java Console" on page 55 for details.

Although there are several other log levels available, INTERMEDIATE_DETAIL, SUMMARY, and VERBOSE, NONE and DEBUG should provide the information you need.

3. Retain the default value DEBUG for each category for which you want to log the current session's error information. All error information is logged.

or

Click **Defaults** to set all categories to the log level **NONE** if you do not plan to log messages for the current session.



Note: When you set the log level to **NONE**, you might find some error information is still logged.

4. Click **OK** to apply your changes and close the Configure client logs window.
You can now maximize the Java console and view log data.

Viewing Log Data Online

To view Java console logs online:

1. Start or maximize the active Java console.
2. Perform the process for which you want to view data, if you have set the log level for a specific process. For example if you have set the log level for the Discovery process, perform a discovery and view the data online in the Java console.

Information is written to the screen in real-time:

 A screenshot of the 'Java Web Start Console - Acme Packet Net-Net EMS' window. The window title bar includes the application name and standard window controls. The main area displays a continuous stream of log messages in a monospaced font. The messages are primarily in Java code, showing various component names like 'ConnectionManager', 'ClientUtil', and 'DiscoverSystem' along with their corresponding methods and parameters. The scroll bar on the right indicates the text is scrollable.


```
#:172.30.80.3/ConnectionManager, and is
com.acme.ems.server.app.cli.CLIClnectionManagerImpl_Stub[RemoteStub [ref:
[endpoint:[172.30.80.3:43945](remote),objID:[a613f8:104edf727a7-8000, 54]]]]
ClientUtil: checkRemoteObjects: got RemoteObject for rmi://172.30.80.3/DBBackupPolicyManager,
and is com.velankani.ems.server.app.policy.backuppolicy.DBBackupPolicyManagerImpl_Stub[RemoteStub [ref:
[endpoint:[172.30.80.3:43945](remote),objID:[a613f8:104edf727a7-8000, 55]]]]
ClientUtil: checkRemoteObjects: got RemoteObject for rmi://172.30.80.3/OperationStateManager,
and is com.acme.ems.server.utility.OperationStateManagerImpl_Stub[RemoteStub [ref:
[endpoint:[172.30.80.3:43945](remote),objID:[a613f8:104edf727a7-8000, 56]]]]
ClientUtil: checkRemoteObjects: got RemoteObject for rmi://172.30.80.3/ObjectStatusUpdate, and is
com.acme.ems.server.app.main.ObjectStatusUpdateImpl_Stub[RemoteStub [ref:
[endpoint:[172.30.80.3:43945](remote),objID:[a613f8:104edf727a7-8000, 58]]]]
ClientUtil: checkRemoteObjects: got RemoteObject for rmi://172.30.80.3/Command, and is
com.acme.ems.server.app.main.CommandImpl_Stub[RemoteStub [ref:
[endpoint:[172.30.80.3:43945](remote),objID:[a613f8:104edf727a7-8000, 59]]]]
ClientUtil: checkRemoteObjects: got RemoteObject for rmi://172.30.80.3/Inventory, and is
com.acme.ems.server.app.inventory.InventoryDetailsImpl_Stub[RemoteStub [ref:
[endpoint:[172.30.80.3:43945](remote),objID:[a613f8:104edf727a7-8000, 61]]]]
ClientUtil: checkRemoteObjects: got RemoteObject for rmi://172.30.80.3/Performance, and is
com.acme.ems.server.app.performance.PerformanceCollectionImpl_Stub[RemoteStub [ref:
[endpoint:[172.30.80.3:43945](remote),objID:[a613f8:104edf727a7-8000, 52]]]]
ClientUtil: checkRemoteObjects: got RemoteObject for rmi://172.30.80.3/SyslogManager, and is
com.acme.ems.server.app.syslog.SyslogManagerImpl_Stub[RemoteStub [ref:
[endpoint:[172.30.80.3:43945](remote),objID:[a613f8:104edf727a7-8000, 60]]]]
Registering for responses BROADCAST_FROM_CLIENT
Registering for responses CatchBroadcastMessage
DiscoverSystem: setPollingStatus: setPollingStatus() sdProps: (primaryKey=,
```

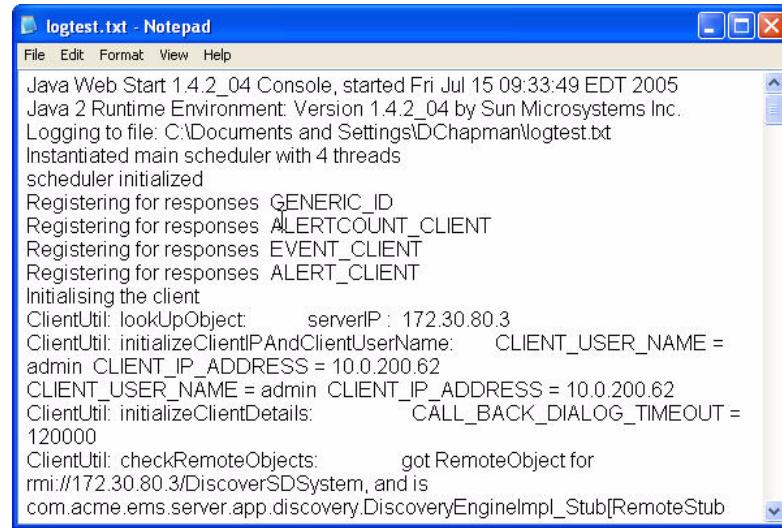
3. Click **Clear** to clear the data from the screen.

Viewing the Java Console Log File

If you chose to write the log messages to a file, you can access that file to view the data.

To view the log file:

1. Open the log file that you named in the Java Web Start application. The logged data appears. For example:



```
logtest.txt - Notepad
File Edit Format View Help
Java Web Start 1.4.2_04 Console, started Fri Jul 15 09:33:49 EDT 2005
Java 2 Runtime Environment: Version 1.4.2_04 by Sun Microsystems Inc.
Logging to file: C:\Documents and Settings\DC Chapman\logtest.txt
Instantiated main scheduler with 4 threads
scheduler initialized
Registering for responses GENERIC_ID
Registering for responses ALERTCOUNT_CLIENT
Registering for responses EVENT_CLIENT
Registering for responses ALERT_CLIENT
Initialising the client
ClientUtil: lookUpObject: serverIP: 172.30.80.3
ClientUtil: initializeClientIPAndClientUserName: CLIENT_USER_NAME =
admin CLIENT_IP_ADDRESS = 10.0.200.62
CLIENT_USER_NAME = admin CLIENT_IP_ADDRESS = 10.0.200.62
ClientUtil: initializeClientDetails: CALL_BACK_DIALOG_TIMEOUT =
120000
ClientUtil: checkRemoteObjects: got RemoteObject for
rmi://172.30.80.3/DiscoverSDSSystem, and is
com.acme.ems.server.app.discovery.DiscoveryEngineImpl_Stub[RemoteStub]
```

Overview

This chapter explains how to discover the Net-Net SBCs you want to manage using Net-Net EMS. You can discover a single Net-Net SBC, a single Net-Net SBC high availability (HA) pair, or multiple single and HA pair systems.

Discovery is the process of identifying Net-Net SBCs in the network using the IP address and collecting inventory data about the devices to store in the Net-Net EMS database. Discovery discovers devices in the network and gathers resource information about the devices for use with data collection, report generation, and queries.

Discovery establishes a connection with the Net-Net SBC or HA pair, checks the state of an HA pair, obtains the system's details, and adds the Net-Net SBC or HA pair to the Net-Net EMS navigation tree.

There is also a rediscovery process that occurs when a Net-Net SBC's configuration has been updated, after the reboot of the system. The reboot causes the rediscovery to occur automatically.

Types of Discovery

As of release 6.2, Net-Net EMS can perform two types of discovery, depending on the version of Net-Net SBCs being managed.

- record-by-record: used when discovering Net-Net SBCs prior to version C6.0M1. The record-by-record discovery uses the Acme Control Protocol (ACP) to obtain the configuration object-by-object from the Net-Net SBC being discovered.
- file-based: used when discovering Net-Net SBCs running version C6.0M1 and later, and when the use of an SSH password is disabled on the Net-Net SBC. File-based discovery uses the Secure File Transfer Protocol (SFTP) to obtain the saved configuration from the Net-Net SBC being discovered.

Note: If Net-Net EMS cannot perform a file-based discovery, it will revert to the record-by record discovery process. You can verify the type of discovery used by reviewing the Discovery log.

SSH Username

If you have a SSH/SFTP username defined in addition to the standard usernames `user` and `admin` and you want to use file-based discovery when managing Net-Net SBCs that support it, you need to remove that additional user name. If the additional username is retained, the file-based discovery fails and Net-Net EMS automatically retries using the record-by-record discovery method.

Disabling File-Based Discovery

If you have system administrator privileges, you can disable file-based discovery in order to use the record-by-record process instead. Refer to the the *Net-Net System Administration Guide* for details.

Minimum Net-Net SBC Configuration

The Net-Net SBCs you plan to manage using Net-Net EMS must have the following information configured in order to be discovered. To verify the minimum configuration for Net-Net SBCs you plan to manage, see the following documentation:

- *Net-Net EMS 4000 Configuration Guide* for details about configuring a Net-Net SBC using the Acme Command Line Interface (ACLI)
- *Net-Net ACLI Reference Guide* to refer to all ACLI commands.

Boot Parameters

Boot parameters specify the information your Net-Net system uses at boot time when it prepares to run applications. The Net-Net system's boot parameters include the Net-Net system's IPv4 address for the management interface (wancom0) and the target name of the Net-Net SBC.

Net-Net EMS uses the target name to uniquely identify a Net-Net SBC from among the list of Net-Net SBCs in its Active configuration area. You need to ensure that all Net-Net SBCs you plan to manage, thus discover, with Net-Net EMS have unique target names. Otherwise a list of Net-Net SBCs, all with the default name `acmesystem`, would appear in the list.

Ensure the following boot parameters have been configured:

- wancom0 IP address and mask
- target name is set to a unique name (do not use the default name `acmesystem`)

System Configuration Element

You need to ensure the `system-config` element has been configured. This element establishes general system information and settings, for example:

- Contact information for this Net-Net system for SNMP purposes
- Identification of the Net-Net system for SNMP purposes
- Physical location of the Net-Net system for SNMP purposes
- Whether SNMP is enabled on the system
- Whether traps are enabled

For complete details about system configuration, see the *Net-Net EMS Configuration Guide* and the *Net-Net ACLI Reference Guide*.

SNMP Community Element

You need to ensure the `snmp-community` element is configured. Specifically, you need to ensure:

- IP address list contains the address of the host upon which EMS server is running. IP address(es) for SNMP communities for authentication purposes
- Access mode is READ-ONLY

Note: Discovery will either fail if SNMP is not configured properly. Or the discovery uses the record-by-record method even if the managed Net-Net SBC supports file-based discovery.

Trap Receiver Element

You need to ensure the `trap-receiver` element is configured. Specifically, you need to ensure

- IP address is that of the Net-Net EMS server
- Filter level is set to All.
- Community name matches the name in the SNMP community element

About Configuring the Discovery

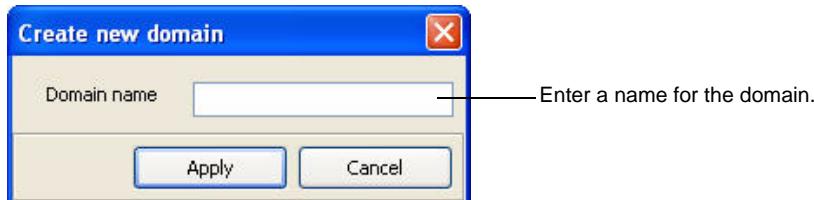
You need to create a domain in the Active configuration area before performing a Discovery. When configuring the Discovery, you choose the domain in which to store the discovered Net-Net SBCs.

Creating a New Domain

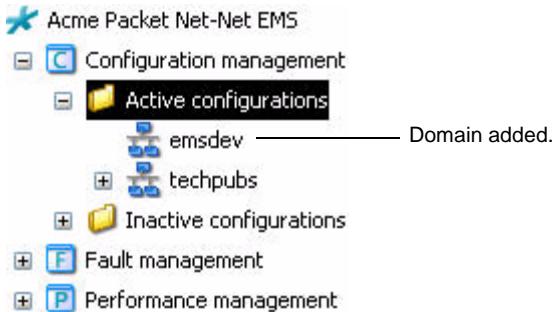
This section explains how to create a new domain. The Net-Net SBCs you discover are placed in a domain you define in the Active configurations area.

To add a domain:

1. Right-click Active configuration. The `create domain` option appears. (You can also choose `create domain` from the toolbar at the top of the window.)
2. Click the `create domain` option to select it. The Create new domain dialog box appears. For example:



3. Enter the name for the domain you want to add and click **Apply**. A status message window appears.
4. Click **OK**. The domain name appears under the Active configuration heading. In the following example the domain named `emsdev` has been added:



The domain is also automatically added to the Inactive configurations area.

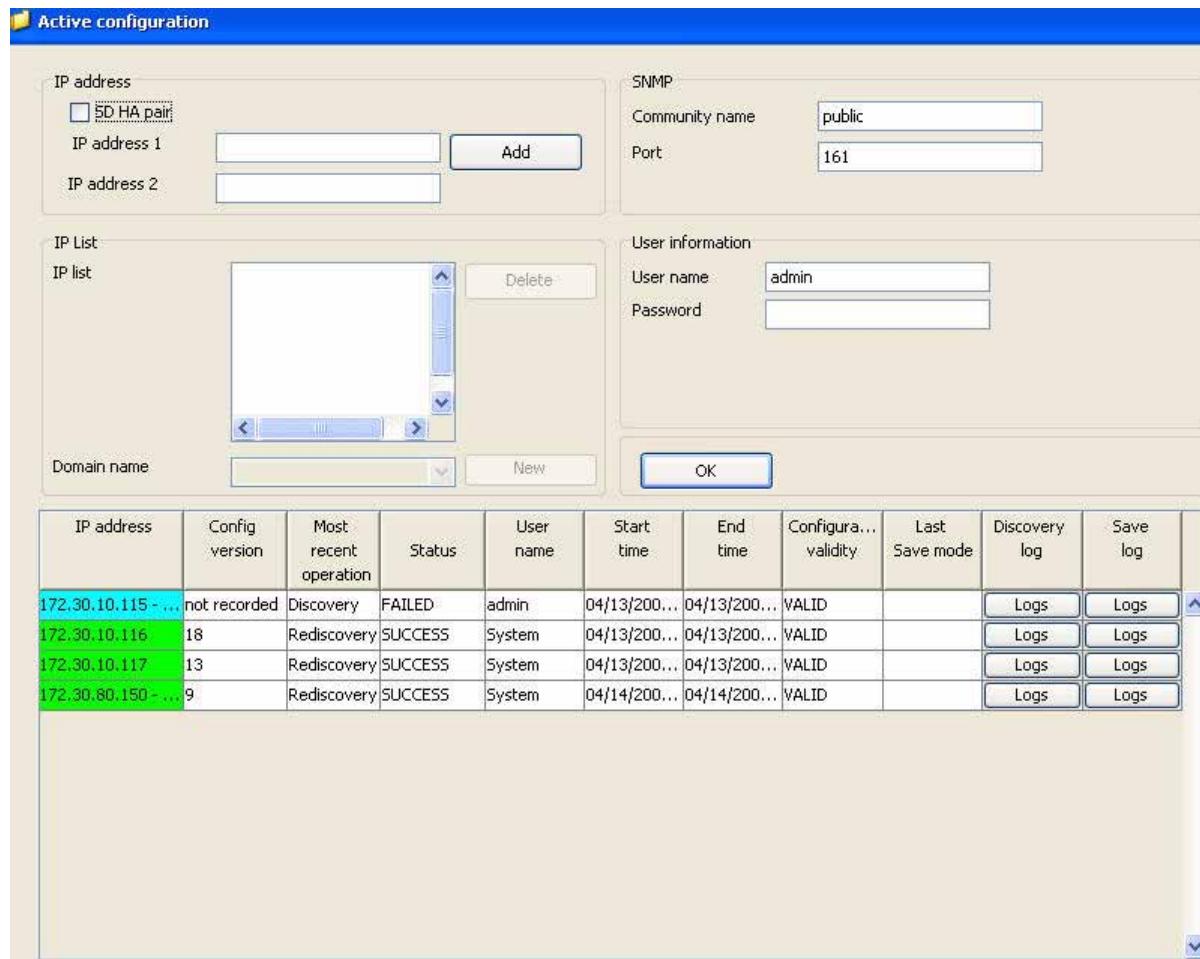
Accessing the Discovery Window

This section explains how to access the Discovery window. You use the Discovery window to enter the discovery configuration information and to view the discovery progress.

To access the Discovery window:

1. Click Active configurations in the Net-Net EMS navigation pane to display the Discovery window in the right pane.

For example:



You enter the Discovery configuration information in the section at the top of the window. The lower part of the window contains a Discovery table, see the following section for more information.

About the Discovery Table

The Discovery table contains information about the Discovery process. It also includes a Save log you can access to view information about saving a configuration. The following table lists the information contained in the Discovery table:

| Option | Description |
|------------------------|---|
| Host name/IP address | <p>Host name or IP address for the standalone Net-Net SBC (or for both Net-Net SBCs in an HA pair) being discovered. This cell is color coded to indicate whether the Net-Net is reachable (status updated by the polling mechanism).</p> <ul style="list-style-type: none"> • green: device is reachable • turquoise: device is not managed • red: device is unreachable (standalone or both Net-Net SBCs in an HA pair) • yellow: one of the Net-Net SBCs in an HA pair is unreachable |
| Config version | <p>The number identifying the configuration version of the Net-Net SBC being discovered. The possible options include:</p> <ul style="list-style-type: none"> • A numeric value: if a file-based discovery method is used and it is successful • “not recorded”: if record-by-record discovery method is used • An empty field: if the discovery was done in a release prior to EMS 6.2 and the EMS database was just upgraded to EMS 6.2 or a later release. After the EMS upgrade, a new invocation of discovery/rediscovery will update the empty field to a numeric value. |
| Most recent operation | <p>Most recent operation that has occurred for the Net-Net SBC. The operations include:</p> <ul style="list-style-type: none"> • Discovery • Rediscovery • Save |
| Status | <p>Status of the discovery or rediscovery or save</p> <ul style="list-style-type: none"> • In-progress: discovery or rediscovery or save is in progress • SUCCESS: discovery or rediscovery or save succeeded • FAILED: discovery or rediscovery failed |
| User name | Name of the user who invoked the discovery operation |
| Start time | Time the discovery or rediscovery operation started |
| End time | Time the discovery or rediscovery operation ended |
| Configuration validity | Indicates whether the Net-Net SBC's configuration is valid |
| Last Save mode | The last save operation performed: Full save or save |
| Discovery log | Access the Discovery log to view information about the Discovery process |
| Save log | Access the Save log to view information about the Save process |

About the Save Log

You can view information about Save configuration operations by viewing the Save log accessed from the Discovery table. For information about saving configurations, refer to the *Net-Net EMS Configuration Guide*.

Configuring the Discovery

This section explains how to configure a discovery. The discovery process identifies the Net-Net SBC in the network and collects configuration data that it stores in the Net-Net EMS database. You can configure discoveries for the following:

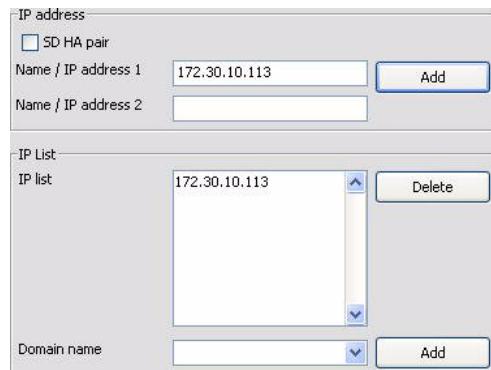
- standalone Net-Net SBC
- Net-Net SBC HA pair
- multiple systems (standalone and/or HA pairs) that have the same SNMP community name and port number, and the same ACP port.

Entering the Net-Net SBC Addresses

Standalone Net-Net SBC

To enter the address:

1. In the Discovery window, enter the IP address for the Net-Net SBC.
2. Click **Add**. The address appears in the IP list:



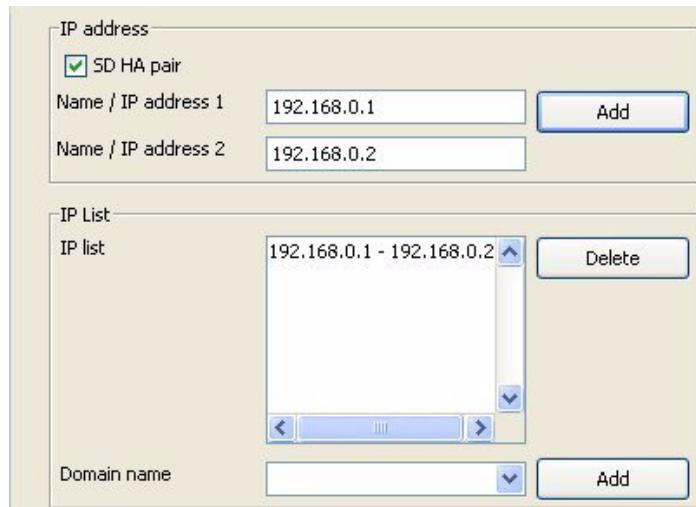
3. Complete the configuration by following the steps in *Completing the Configuration*.

Net-Net SBC HA Pair

To enter the addresses:

1. In the Discovery window:
 - **SD HA pair**—Click the checkbox.
 - **Name / IP address 1**—Enter the IP address for one of the Net-Net SBCs in the HA pair in the textbox.
 - **Name / IP address 2**—Enter the IP address for the second Net-Net SBC of the pair in the textbox.

2. Click **Add**. The addresses appear in the IP list:



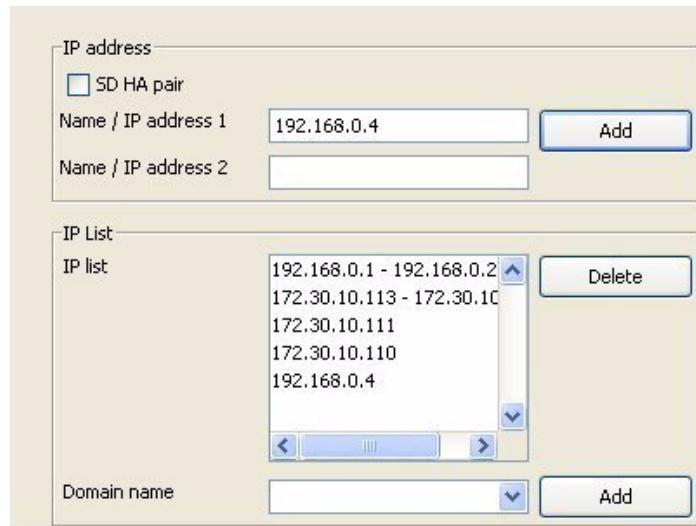
3. Complete the configuration by following the steps in *Completing the Configuration*.

Multiple Net-Net SBCs

To enter addresses:

1. In the Discovery window:
 - Enter the IP address for a standalone Net-Net SBC. See *Standalone Net-Net SBC* for details.
 - **SD HA pair**—Click the checkbox.
 - **Name / IP address 1**—Enter the IP address for one of the Net-Net SBCs in the HA pair in the textbox.
 - **Name / IP address 2**—Enter the IP address for the second Net-Net SBC of the pair in the textbox. See *Net-Net SBC HA Pair* for details.
2. Click **Add**. The address appears in the IP list.
3. Repeat steps 1 and 2 until you have added all IP addresses.

For example:



4. Complete the configuration by following the steps in *Completing the Configuration*.

Completing the Configuration

If discovering multiple Net-Net SBCs, the SNMP community name and port number, and the ACP port must be the same for all systems.

To complete the configuration:

1. Enter a domain name by clicking the **Domain name** text box or down arrow to pick from a list of existing domains. For example:

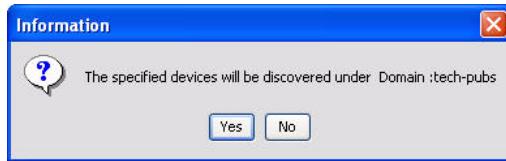


Or you can click **Add** to add a new domain. See *Creating a New Domain* for details.

2. Edit the default SNMP community name and port number if necessary. The SNMP community name is the name of an active community where this Net-Net SBC can send or receive SNMP information. Net-Net SBC events are reported to Net-Net EMS.
3. Edit the default Acme Control Protocol (ACP) port if necessary. The ACP port enables the Net-Net SBC to respond to ACP requests and is required for Net-Net EMS use.
4. Edit the user name if necessary.
5. Enter the password associated with the user name. All other areas are filled in for you. Valid user names and passwords include:
 - user and <login password> (for example: user and acme)
 - admin and <enable password> (for example: admin and packet)

Note: Perform the discovery as the admin user if you plan to save the configuration.

6. Click **OK**. The following message appears:



7. Click **Yes** to clear the message and continue the discovery.

The discovery process starts. A row is added to the Discovery table and the Status column shows the discovery is in progress:

| IP address | Config version | Most recent operation | Status | User name | Start time | End time | Configura... validity | Last Save mode | Discovery log | Save log |
|---------------------|----------------|-----------------------|---------|------------|--------------|--------------|-----------------------|----------------|---------------|----------|
| 172.30.10.113 | not recorded | Rediscovery | SUCCESS | admin | 04/07/200... | 04/07/200... | VALID | | Logs | Logs |
| 172.30.10.114 - ... | 116 | Rediscovery | SUCCESS | hongtest-1 | 04/07/200... | 04/07/200... | VALID | | Logs | Logs |
| 172.30.80.115 | 3417 | Rediscovery | SUCCESS | hongtest-1 | 04/07/200... | 04/07/200... | VALID | | Logs | Logs |
| 172.30.80.170 - ... | 161 | Rediscovery | SUCCESS | System | 04/07/200... | 04/07/200... | VALID | | Logs | Logs |

Color indicates status of IP host. Status indicates Discovery is in progress.

The color of the cells in the first column indicate the status of the IP host:

- green: host is reachable
- turquoise: host is not managed
- red: host is unreachable (standalone or both Net-Net SBCs in an HA pair)
- yellow: one of the Net-Net SBCs in an HA pair is unreachable

8. In the Discovery log column, click **Logs** to access the Discovery log for the host you are discovering. The Discovery log for that host appears. For example:

The screenshot shows a window titled "Discovery logs for 172.30.0.100". The window contains a table with four columns: Element Name, Status, Count, and Object Name. The table lists various network components and their status. At the bottom of the window are three buttons: Refresh, Export, and Close.

| Element Name | Status | Count | Object Name |
|--------------------|---------------|-------|--------------------------|
| systemConfig | true | 1 | sd100 |
| SYSTEMCONFIG | true | 1 | |
| RedundancyConfig | true | 1 | SDHANodeRedundancyConfig |
| REDUNDANCYCONFIG | true | 1 | |
| phyInterfaceConfig | true | 1 | M11 |
| PHYINTERFACECONFIG | true | 1 | |
| networkInterface | not available | 1 | no node added |
| trapReceiver | true | 1 | 10.0.200.63:162 |
| trapReceiver | true | 1 | 10.0.100.63:162 |
| TRAPRECEIVER | | 2 | |
| snmpCommunity | true | 1 | fg1 |
| snmpCommunity | true | 1 | tmi |
| snmpCommunity | true | 1 | public |
| SNMPCOMMUNITY | | 3 | |
| ntpConfig | true | 1 | NTPServer |
| NTPCONFIG | true | 1 | |
| bootParams | true | 1 | FTPServer |
| BOOTPARAMS | | 1 | |
| H323Config | true | 1 | H323Config |
| H323CONFIG | true | 1 | |
| NetworkParameters | true | 1 | NetworkParameters |
| NETWORKPARAMETERS | | 1 | |
| ipRoute | true | 1 | 10.0.200.0 |
| ipRoute | true | 1 | 10.10.10.10 |
| ipRoute | true | 1 | 101.101.101.101 |
| IPROUTE | | 3 | |
| sysACL | not available | 1 | no node added |
| lwfStackConfig | true | 1 | IWFConfig |
| IWFSTACKCONFIG | | 1 | |
| sipQoSMap | not available | 1 | filler node added |
| sipQoSMap | true | 1 | SipQoSMap |
| SIPQoSMAP | | 1 | |
| qoSOSipMap | not available | 1 | filler node added |
| q850SipMap | true | 1 | Q850SipMap |
| QoSOSipMap | | 1 | |

Click to refresh the data displayed in the log.

9. Click **Refresh** to update the information displayed in the log.

After the Discovery process is finished, the Discovery table is updated to display the status of the Discovery, Failed or Success:

The screenshot shows a table with columns: IP address, Config version, Most recent operation, Status, User name, Start time, End time, Configuration validity, Last Save mode, Discovery log, and Save log. The table lists four hosts: 172.30.10.113, 172.30.10.114, 172.30.80.115, and 172.30.80.170. The "Status" column indicates the discovery outcome. The "Discovery log" and "Save log" columns both show "Logs".

| IP address | Config version | Most recent operation | Status | User name | Start time | End time | Configuration validity | Last Save mode | Discovery log | Save log |
|---------------------|----------------|-----------------------|---------|------------|--------------|--------------|------------------------|----------------|---------------|----------|
| 172.30.10.113 | not recorded | Rediscovery | SUCCESS | admin | 04/07/200... | 04/07/200... | VALID | | Logs | Logs |
| 172.30.10.114 - ... | 116 | Rediscovery | SUCCESS | hongtest-1 | 04/07/200... | 04/07/200... | VALID | | Logs | Logs |
| 172.30.80.115 | 3417 | Rediscovery | SUCCESS | hongtest-1 | 04/07/200... | 04/07/200... | VALID | | Logs | Logs |
| 172.30.80.170 - ... | 161 | Rediscovery | SUCCESS | System | 04/07/200... | 04/07/200... | VALID | | Logs | Logs |

Color indicates whether IP host can be reached.

Status indicates Discovery is successful.

The Discovery log displays the final data and results of the Discovery. For example:

| Element Name | Status | Count | Object Name |
|--------------------|---------------|-------|--------------------------|
| systemConfig | true | | sd100 |
| SYSTEMCONFIG | | 1 | |
| RedundancyConfig | true | | SDNANodeRedundancyConfig |
| REDUNDANCYCONFIG | | 1 | |
| phyInterfaceConfig | true | | HII |
| PHYINTERFACECONFIG | | 1 | |
| networkInterface | not available | | no node added |
| trapReceiver | true | | 10.0.200.63:162 |
| trapReceiver | true | | 10.0.100.63:162 |
| TRAPRECEIVER | | 2 | |
| snmpCommunity | true | | rgi |
| snmpCommunity | true | | tmi |
| snmpCommunity | true | | public |
| SNMPCOMMUNITY | | 3 | |
| ntpConfig | true | | NTPServer |
| HTTPCONFIG | | 1 | |
| bootParams | true | | FTPServer |
| BOOTPARAMS | | 1 | |
| H323Config | true | | H323Config |
| H323CONFIG | | 1 | |

- Click **Close** to exit the Discovery log. Or to save the log data, click **Export**. The Export window appears displaying the default filename for the saved log in the format:

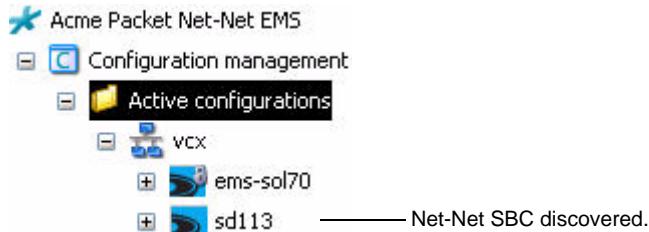
<Host IP address>-Discovery.txt

For example:

172.30.10.113-Discovery.txt

- Click **Close** to close the log window.

Upon completion of Discovery, the Net-Net SBC appears under the network name. The name of the Net-Net SBC is the same as that of the target name set in the boot parameters. For example:



From here, you make a copy of the Net-Net SBC that goes under the Inactive configurations heading. You can then modify the configuration before saving it back to the Net-Net SBC.

Moving the Discovered Net-Net SBC

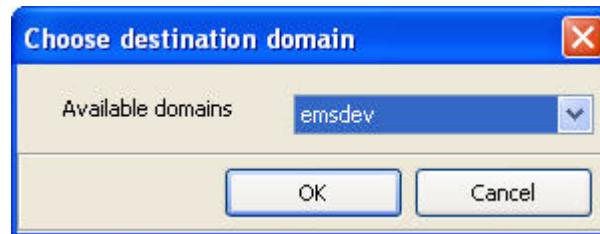
You can move the discovered Net-Net SBC to a different domain.

To move the discovered Net-Net SBC:

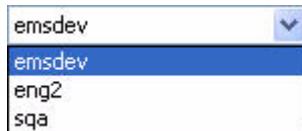
1. In the Active configurations area, right-click the name of the Net-Net SBC you want to move.
2. From the list of options, choose **Move**:

| | |
|------------------------------|--------------|
| Rediscovery | Ctrl+Shift+R |
| Reboot | Ctrl+Shift+B |
| Set offline | Ctrl+Shift+E |
| Copy for edit | Ctrl+Shift+Y |
| Create offline configuration | Ctrl+Shift+O |
| Create global configuration | Ctrl+Shift+G |
| Delete | Ctrl+Shift+D |
| Inventory details | Ctrl+Shift+I |
| Telnet to SD System | Ctrl+Shift+T |
| SSH to device | Ctrl+Shift+S |
| HDR operations | ▶ |
| Registration Cache | Ctrl+Shift+C |
| Lock | Ctrl+Shift+L |
| Unlock | Ctrl+Shift+U |
| Search configuration | Ctrl+F |
| Configuration inventory | Ctrl+N |
| Synchronize Alarms | Ctrl+A |
| Display config version | Ctrl+W |

The Choose destination domain window appears:



3. Click the down arrow next to Available domains to access the list of destinations:



4. Select the target domain's name from the list.
5. Click OK. A confirmation message appears.
6. Click Yes to continue with the move. The Net-Net SBC is moved to the new domain. If you have saved a copy of this Net-Net SBC to the Inactive configurations area, it also gets moved to the new domain.

Rediscovering Net-Net SBCs

This section explains how to rediscover Net-Net SBCs. You can manually perform a rediscovery to collect updated inventory data to store in the Net-Net EMS database. Rediscovery is also automatically performed when the node is activated or rebooted.

To rediscover a Net-Net SBC:

1. In the Active configuration area, right-click the name of the Net-Net SBC you want to rediscover. A list of options appears:

| | |
|------------------------------|--------------|
| Rediscovery | Ctrl+Shift+R |
| Reboot | Ctrl+Shift+B |
| Set offline | Ctrl+Shift+E |
| Copy For edit | Ctrl+Shift+Y |
| Create offline configuration | Ctrl+Shift+O |
| Create global configuration | Ctrl+Shift+G |
| Delete | Ctrl+Shift+D |
| Inventory details | Ctrl+Shift+I |
| Telnet to SD System | Ctrl+Shift+T |
| SSH to device | Ctrl+Shift+S |
| HDR operations | Ctrl+Shift+H |
| Registration Cache | Ctrl+Shift+C |
| Lock | Ctrl+Shift+L |
| Unlock | Ctrl+Shift+U |
| Search configuration | Ctrl+F |
| Configuration inventory | Ctrl+N |
| Synchronize Alarms | Ctrl+A |
| Display config version | Ctrl+W |

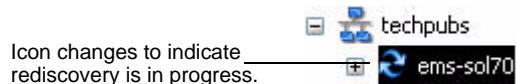
2. Choose Rediscovery. The following confirmation message appears:



3. Click Yes to continue. The following message appears:

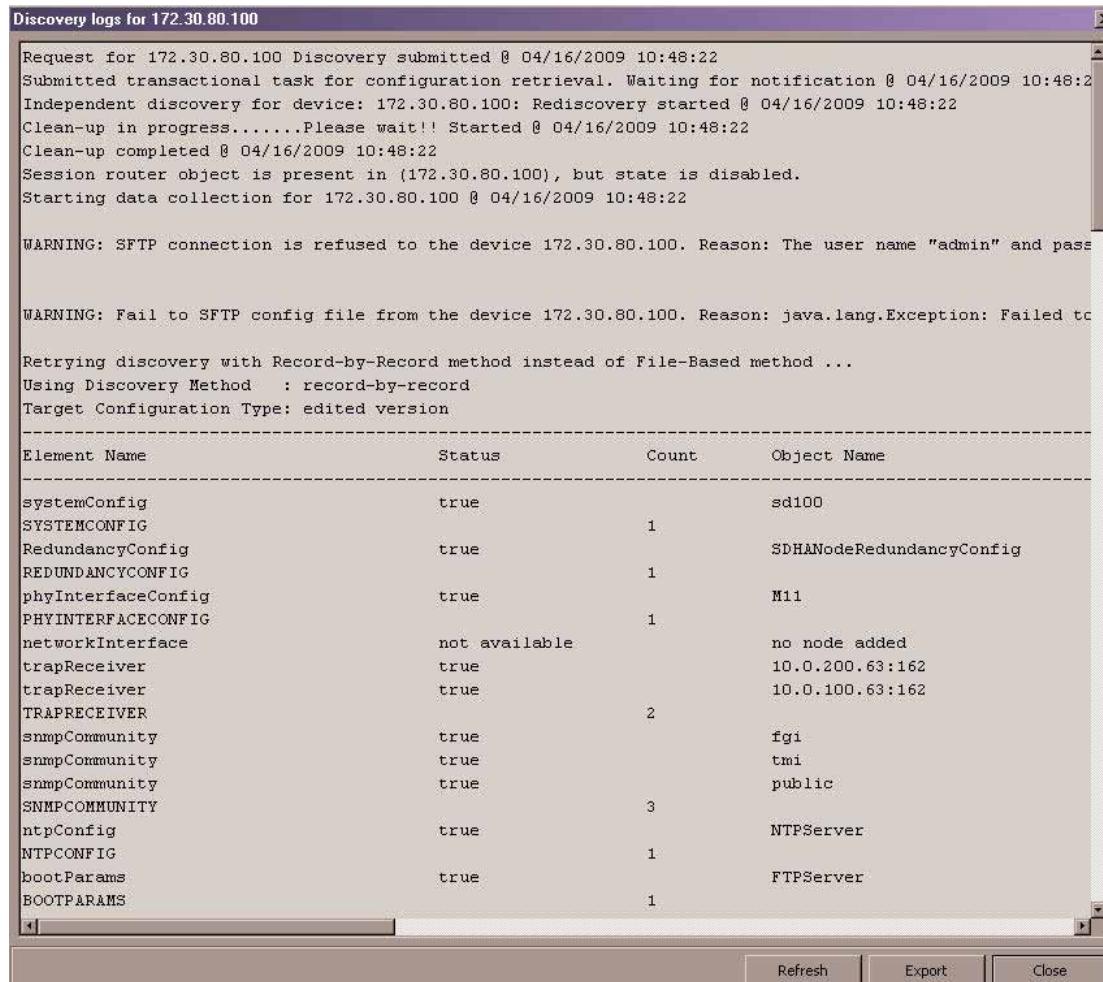


4. Click OK to clear the message. The rediscovery process begins. The icon for the Net-Net SBC in the Active configuration area changes to indicate rediscovery is occurring:



5. Click Active configuration to display the Discovery table. It will display the status of the rediscovery as being In Progress.

6. In the Discovery log column, click **Logs** to access the Discovery log for the host you are discovering. The Discovery log for that host appears displaying data about the rediscovery progress. For example:



The screenshot shows a window titled "Discovery logs for 172.30.80.100". The log output is as follows:

```

Request for 172.30.80.100 Discovery submitted @ 04/16/2009 10:48:22
Submitted transactional task for configuration retrieval. Waiting for notification @ 04/16/2009 10:48:22
Independent discovery for device: 172.30.80.100: Rediscovery started @ 04/16/2009 10:48:22
Clean-up in progress.....Please wait!! Started @ 04/16/2009 10:48:22
Clean-up completed @ 04/16/2009 10:48:22
Session router object is present in (172.30.80.100), but state is disabled.
Starting data collection for 172.30.80.100 @ 04/16/2009 10:48:22

WARNING: SFTP connection is refused to the device 172.30.80.100. Reason: The user name "admin" and pass

WARNING: Fail to SFTP config file from the device 172.30.80.100. Reason: java.lang.Exception: Failed to

Retrying discovery with Record-by-Record method instead of File-Based method ...
Using Discovery Method : record-by-record
Target Configuration Type: edited version

```

Below the log is a table showing the status of various configuration elements:

| Element Name | Status | Count | Object Name |
|--------------------|---------------|-------|--------------------------|
| systemConfig | true | | sd100 |
| SYSTEMCONFIG | | 1 | |
| RedundancyConfig | true | | SDHANodeRedundancyConfig |
| REDUNDANCYCONFIG | | 1 | |
| phyInterfaceConfig | true | | M11 |
| PHYINTERFACECONFIG | | 1 | |
| networkInterface | not available | | no node added |
| trapReceiver | true | | 10.0.200.63:162 |
| trapReceiver | true | | 10.0.100.63:162 |
| TRAPRECEIVER | | 2 | |
| snmpCommunity | true | | fgi |
| snmpCommunity | true | | tmi |
| snmpCommunity | true | | public |
| SNMPCOMMUNITY | | 3 | |
| ntpConfig | true | | NTPServer |
| NTPCONFIG | | 1 | |
| bootParams | true | | FTPServer |
| BOOTPARAMS | | 1 | |

At the bottom are buttons for Refresh, Export, and Close.

Click to refresh the data displayed in the log.

7. Click **Refresh** to update the information displayed in the log.

After the rediscovery finishes, the status is updated in the Discovery table:



| IP address | Config version | Most recent operation | Status | User name | Start time | End time | Configura... validity | Last Save mode | Discovery log | Save log |
|---------------------|----------------|-----------------------|---------|------------|--------------|--------------|-----------------------|----------------|---------------|----------|
| 172.30.10.113 | not recorded | Rediscovery | SUCCESS | admin | 04/07/200... | 04/07/200... | VALID | | Logs | Logs |
| 172.30.10.114 - ... | 116 | Rediscovery | SUCCESS | hongtest-1 | 04/07/200... | 04/07/200... | VALID | | Logs | Logs |
| 172.30.80.115 | 3417 | Rediscovery | SUCCESS | hongtest-1 | 04/07/200... | 04/07/200... | VALID | | Logs | Logs |
| 172.30.80.170 - ... | 161 | Rediscovery | SUCCESS | System | 04/07/200... | 04/07/200... | VALID | | Logs | Logs |

Rediscovery is successful.

Click to view progress information.

The Discovery log displays the final data and results of the rediscovery. For example:

The screenshot shows a window titled "Discovery logs for 172.30.80.100". The log content includes configuration details for various SBC components like callRecordingServer, qosConstraints, imsAkaProfile, etc., followed by a summary of statistics and commit logs. The bottom of the window features standard buttons: Refresh, Export, and Close.

```

Discovery logs for 172.30.80.100

callRecordingServer          not available      no node added
qosConstraints               not available      no node added
imsAkaProfile                not available      no node added
sshPubKeyRecord              true                  vvk
sshPubKeyRecord              true                  nmc
sshPubKeyRecord              true                  vishk
SSHPUBKEYRECORD             3
h248Config                   not available      no node added
h248MgcConfig                not available      no node added
h248MgConfig                 not available      no node added
ipsecNwIntfs                not available      no node added
h248MgConfig                 not available      no node added
h248Config                   not available      no node added
h248MgcConfig                not available      no node added
Integrity Check succeeded

Element Name           Status   Count   Object Name
General Stats          INFO     Total number of Elements added
Discovery of Device Configuration completed.

Rediscovery of device configuration completed @ 04/16/2009 10:48:24
Committing device configuration to DB @ 04/16/2009 10:48:24
Commit to DB completed @ 04/16/2009 10:48:24
Notification received status : FINISHED for transaction completion @ 04/16/2009 10:48:24

Starting Performance node creation @ 04/16/2009 10:48:25
Performance node creation status for 172.30.80.100 status true @ 04/16/2009 10:48:25

Starting retrieval of inventory data @ 04/16/2009 10:48:25
Inventory collection status for 172.30.80.100 status true @ 04/16/2009 10:48:26
Inventory status for 172.30.80.100 status true @ 04/16/2009 10:48:26

Update SD System state @ 04/16/2009 10:48:26
System state for 172.30.80.100 is online
Update SD System status for 172.30.80.100 status true @ 04/16/2009 10:48:26

```

8. Click **Close** to close the window. Or to save the log data, click **Export**. The Save window appears displaying the default filename for the saved log in the format:
<Host IP address>-Discovery.txt
For example:
172.30.80.70-Discovery.txt
9. Click **Close** to close the log window.

Display Configuration Version

Net-Net EMS provides a tool called display configuration version that lets you display and check the Net-Net EMS version of the configuration against the saved and/or running configuration versions on the Net-Net SBC.

The Net-Net EMS version of the Net-Net SBC configuration displayed in the display configuration version tool is based on the time of discovery or rediscovery, while the current Net-Net SBC saved and/or running configuration versions displayed are based on the time the tool was invoked.

This tool is compatible with file-based discovery (default) only. If the node is discovered, or rediscovered, as a result of record-by-record discovery, the Net-Net EMS config version is registered as an empty string in the database and you will get the following message: Configuration has no version because it is discovered from the latest edited configuration on the device. For more information on the types of discovery, see the *Net-Net EMS 4000 User Guide*, *Discovering Net-Net SBCs* chapter.

Discovery Process Sequences

The following table shows the discovery process using both types of discovery: file-based and record-by-record:

| Sequence Number | Sequence of Operation | EMS Configuration Version Number | Discovery Type |
|-----------------|--|----------------------------------|------------------|
| A | Initial discovery – Net-Net SBC 1 | “” | record-by-record |
| B | Copy for edit of Net-Net SBC 1 called “copy 1” | “” | |
| C | Rediscovery of Net-Net SBC 1 | 2955 | file-based |
| D | Copy for edit of Net-Net SBC 1 called “copy 2” | 2955 | |

Use-Case Scenarios

The following use-case scenarios show how the display configuration version appears when using both the record-by-record discovery mode and the file-based discovery mode.

- When **record-by-record** discovery is used to discover Net-Net SBC 1, the Net-Net EMS configuration version is displayed as an empty string (“”). When a copy of Net-Net SBC 1 is made, the configuration version for this copy is also displayed as an empty string (“”), as shown in sequences A and B.
- When **file-based** discovery is used to re-discover Net-Net SBC 1, the Net-Net EMS configuration version is displayed as 2955. When a copy is made of this rediscovered Net-Net SBC 1, the Net-Net EMS configuration version is also displayed as 2955, as shown in sequences C and D.

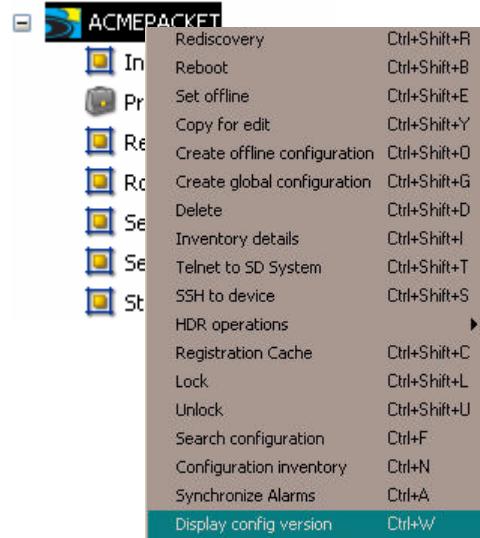
Viewing the Configuration Version

The following sections show how to view the Net-Net EMS configuration version and the Net-Net SBC saved and running configuration versions for both an active and an inactive configuration.

Active Configuration

To view the configuration versions for an active Net-Net SBC:

1. Right-click the active Net-Net SBC in the Net-Net EMS navigation tree.



The right-click menu appears.

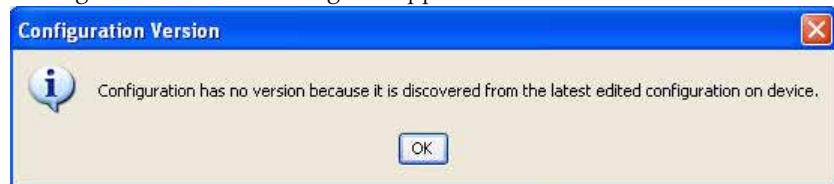
2. Click **Display config version**.

If the Net-Net SBC is discovered using file-based discovery, the Configuration Version dialog box appears with config version statistics.



3. Click **OK**.

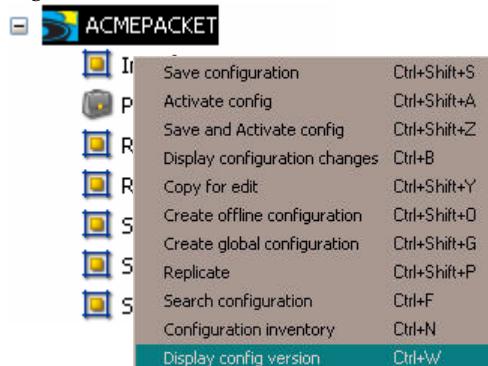
If the Net-Net SBC is discovered using record-by-record discovery, the Configuration Version dialog box appears without statistics.



4. Click **OK**.

Inactive Configuration**To view the configuration versions for an inactive Net-Net SBC:**

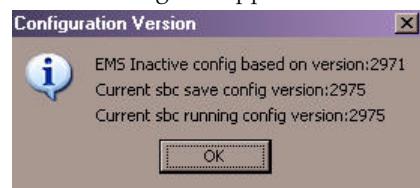
1. Right-click the inactive Net-Net SBC in the Net-Net EMS navigation tree.



The right-click menu appears.

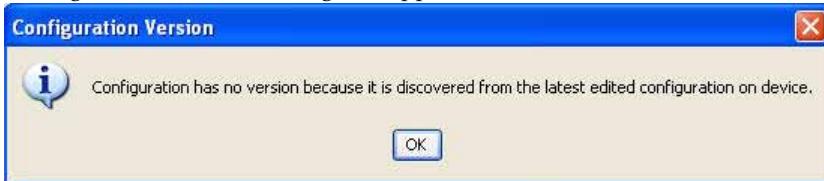
2. Click **Display config version**.

If the Net-Net SBC is discovered using file-based discovery, the Configuration Version dialog box appears with config version statistics.



3. Click **OK**.

If the Net-Net SBC is discovered using record-by-record discovery, the Configuration Version dialog box appears without statistics.

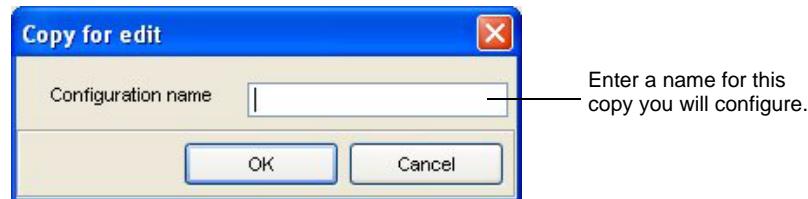


4. Click **OK**.

Copying the Net-Net SBC

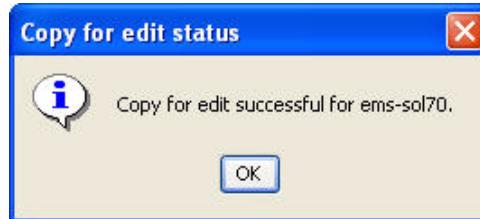
To copy the Net-Net SBC configuration to edit:

1. Click the newly discovered Net-Net SBC to select it.
2. Right-click to access the popup menu of options. (You can access the same list from the **SD system** option on the toolbar across the top of the screen.)
3. Click **copy for edit** to select it. The Copy for edit screen appears. For example:

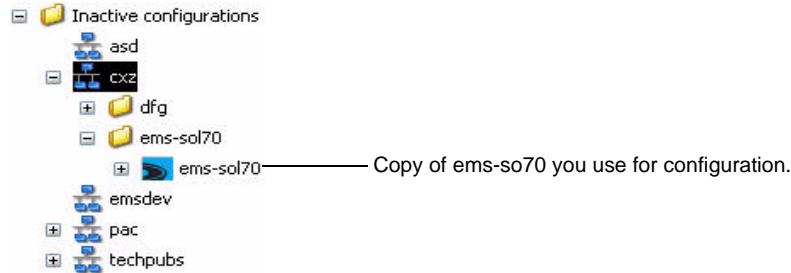


4. Enter a name for this Net-Net SBC copy which you will configure and click **OK**. You can use a descriptive name to indicate this is a copy. For example, **ems-so70_Updated**. (You cannot use spaces when naming the copy.)

A progress message appears, followed by a status message:



5. Click **OK** to clear the message. A copy of the Net-Net SBC was placed under the Inactive configurations area:



You can now edit the copy of the Net-Net SBC and save the changed configuration to the Net-Net SBC. Refer to the *Net-Net EMS Configuration Guide* for details about configuring, saving, and activating a Net-Net SBC.

After the configuration is saved and activated, the Net-Net SBC notifies Net-Net EMS that its configuration has changed. Net-Net EMS automatically initiates a rediscovery process for the Net-Net SBC in the background. The progress bar at the bottom of the screen turns blue as the rediscovery begins. The icon in the left pane changes.

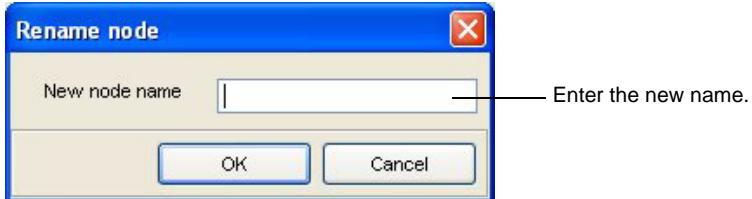
When the rediscovery is complete, the Net-Net SBC in the Active configurations list reflects the newly activated configuration and the icon returns to its original form. The Most recent operation column in the Discovery window lists Rediscovery for that Net-Net SBC.

Renaming the Net-Net SBC Configuration Copy

You can rename the copy of the Net-Net configuration located in the Inactive configurations area.

To rename the Net-Net SBC configuration:

1. Right-click the copy of Net-Net-SBC.
2. Choose **rename**. The Rename node window appears. For example:



3. **New node name**—Enter the new name.
4. Click **OK**.

Introduction

The *Net-Net EMS User Guide* does not include detailed information about configuring Net-Net SBCs. This section does provide an overview of the Net-Net SBC configuration process and contains information about Net-Net EMS GUI features that relate to configuring Net-Net SBCs. You can refer to the *Net-Net EMS Configuration Guide* for complete details about configuring Net-Net SBCs.

About Net-Net 4000 SBCs

This guide focuses on the Net-Net 4000 family of SBCs. The Net-Net 4000 series of SBCs include two distinct 4000 platforms, the Net-Net 4250 and Net-Net 4500. It also includes the Net-Net 3800 series, which complements Acme Packet's Net-Net 4000 (as well as the Net-Net 2000 and Net-Net 9000) series. Net-Net 3800 supports all of the same SBC functions and features as the Net-Net 4000 family, with some minor changes in licensing.

You can identify the specific type of Net-Net SBC you are managing by its icon in the GUI's navigation pane and by the information on the System window in the display pane.

See the ACLI version of the documentation set for complete information about the different members of the Net-Net 4000 family of SBCs.

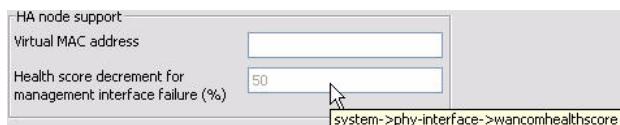
Configuration Overview

When you configure a Net-Net SBC, you follow a specific order. The recommended configuration order consists of the following:

- physical layer
- network interface
- realm and steering pool/media manager
- signaling services (SIP, H.323, MGCP)
- session agents
- routes

Tool Tips

While configuring a Net-Net SBC, you can position your cursor over a parameter field or checkbox to view a tool tip. A tool tip displays the complete path to the corresponding ACLI parameter:



Using Net-Net EMS to Configure the Net-Net SBC

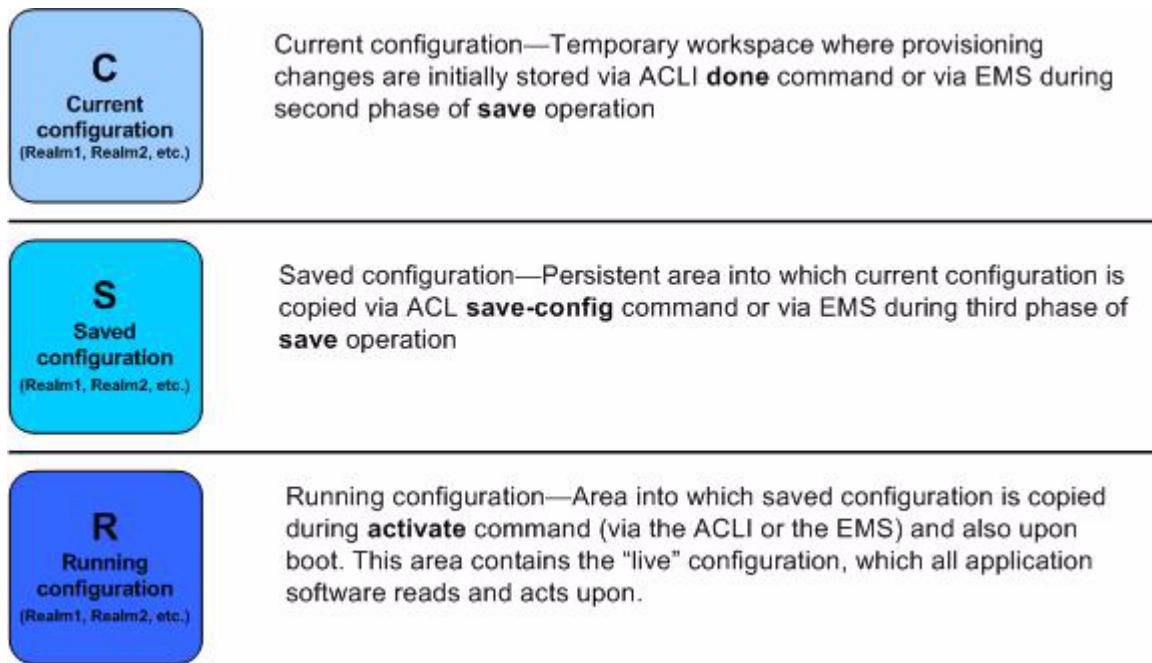
You must create all new configurations and make edits to existing configurations in the inactive configuration branch of the Net-Net EMS navigation tree. You then save and activate the inactive configuration to apply the new configurations and edits on your Net-Net SBC.

Storing Configurations

The Net-Net Session Border Controller (SBC) uses three separate areas to store configurations, as shown in the following diagram.

Relationship Between ACLI/EMS

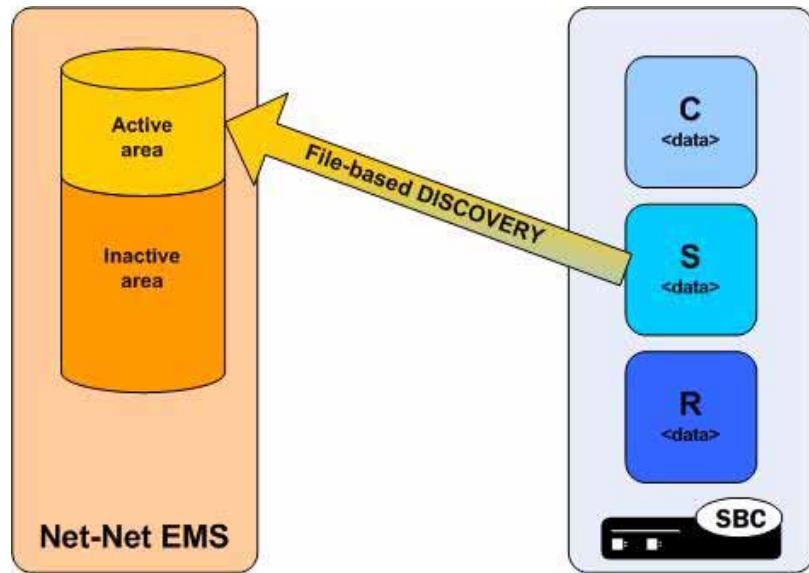
Whether using the ACLI or the Net-Net EMS to configure the Net-Net SBC, when you make changes to the configuration, you must perform a save and activate in order for the changes to take effect. The following image illustrates the phases of the configuration process for ACLI and Net-Net EMS. The save and activate steps are different for each interface, but they achieve the same results.



Discovery

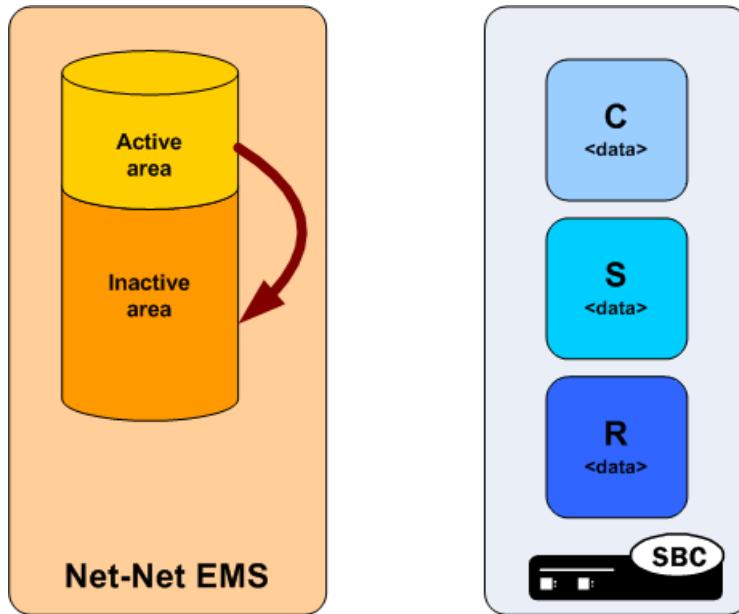
During the file-based discovery/rediscovery process, the Net-Net EMS uploads the configuration from the saved configuration area on the Net-Net SBC into its database, and creates a Net-Net SBC icon in the active folder to represent this configuration.

The active copy of a configuration is read-only.



Copy-for-Edit

During the copy-for-edit process, the Net-Net EMS makes a complete, writeable copy of the configuration in the inactive area. This operation has no effect on the Net-Net SBC.



Net-Net EMS Save Methods

There are two methods for saving a configuration in Net-Net EMS: save and full save. The sections below explain these two methods. For additional details, see *Saving Configurations* in this chapter.

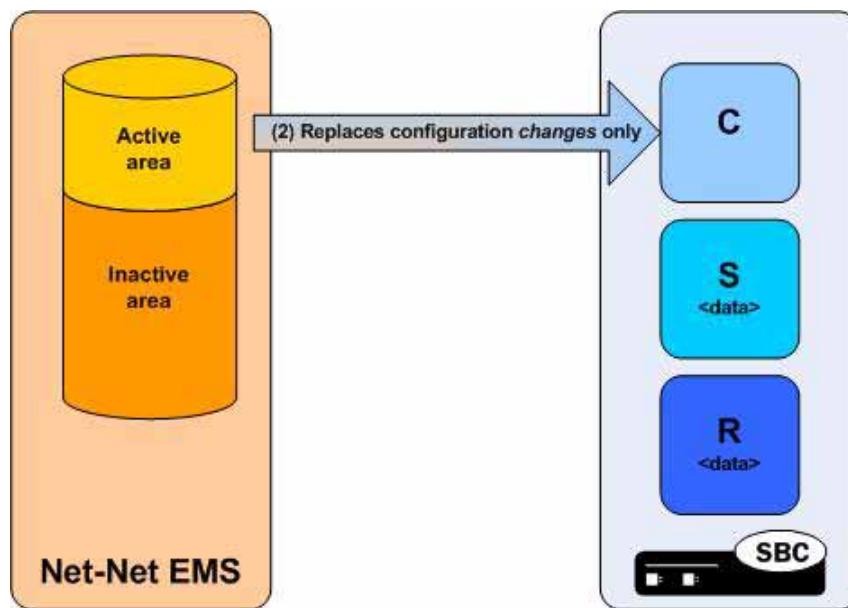
Save Method

The Net-Net EMS save method is the default save method and consists of four phases:

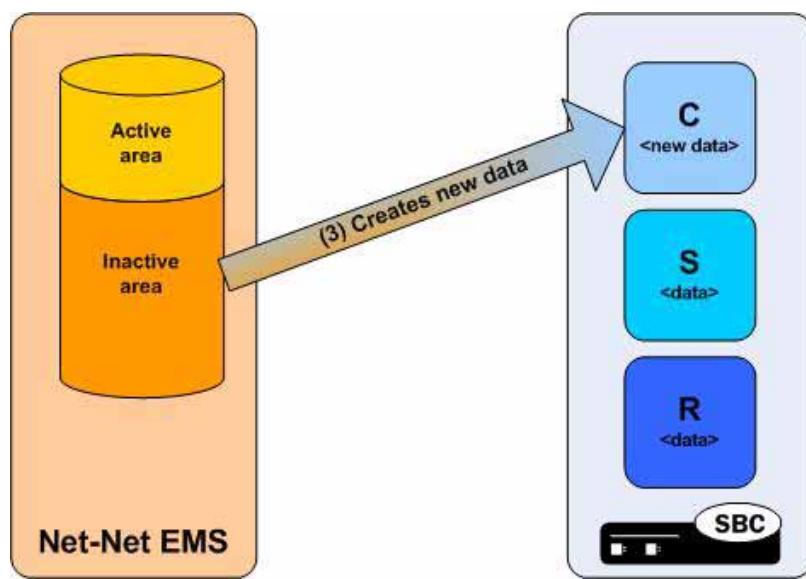
1. Phase 1—When you launch the save process, a save session identifier string is generated. This string contains your user name and the current system uptime. Net-Net EMS stores your save session identifier string, along with your changes made to this Net-Net SBC configuration copy.

During a save session, other save requests to the same configuration copy are queued in the order received by the Net-Net EMS client.

2. Phase 2—The Net-Net EMS replaces only those configuration elements that were modified on this Net-Net SBC configuration copy. Your new configuration elements are saved, along with the rest of the original Net-Net SBC configuration copy.

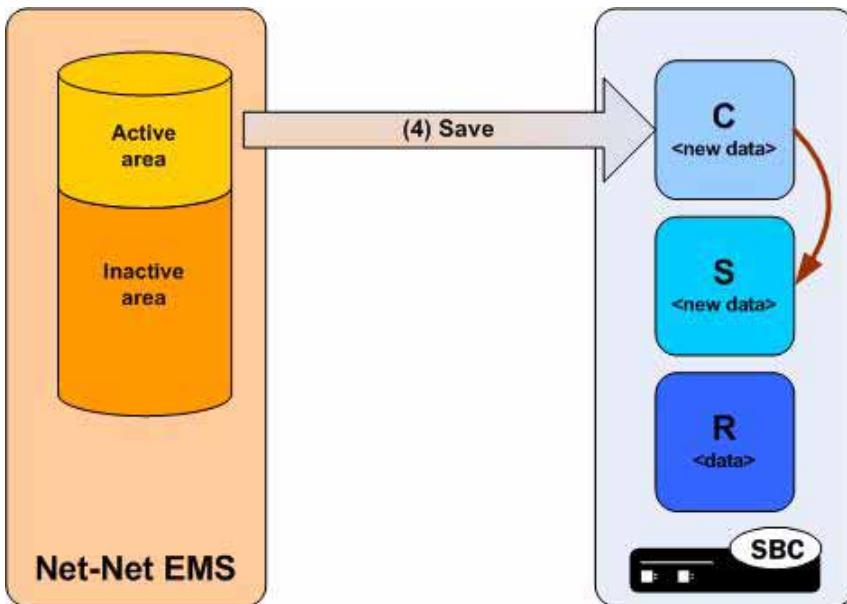


3. Phase 3—The Net-Net EMS downloads the chosen inactive configuration from the Net-Net EMS database into the current configuration area on the Net-Net SBC.



4. Phase 4—The Net-Net EMS instructs the Net-Net SBC to “save” the previously downloaded information by copying the current configuration data to the saved configuration area.

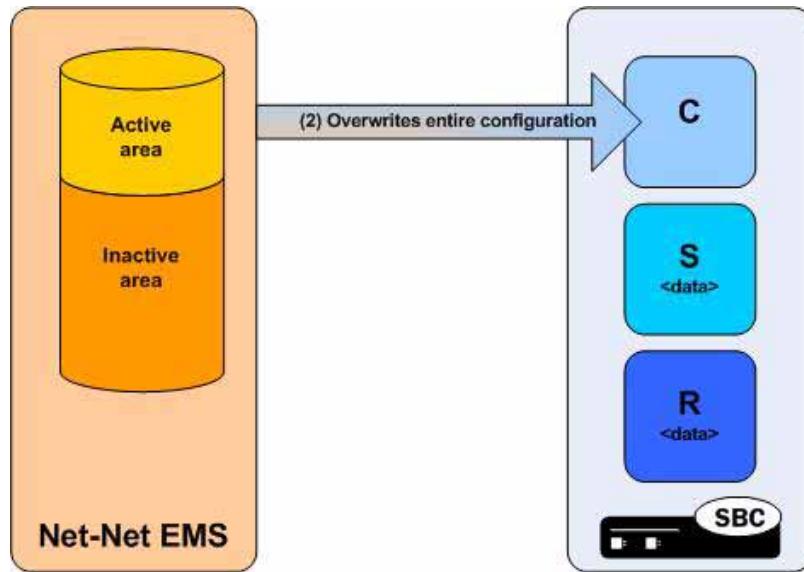
This operation is the same one that takes place on the Net-Net SBC when you enter the **save-config** command at the ACLI system prompt.



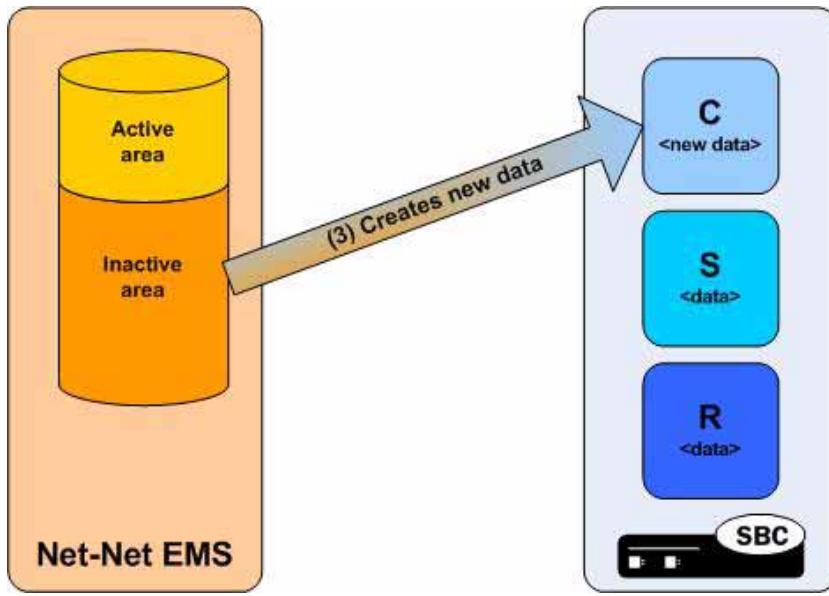
Full Save Method

The Net-Net EMS full save method consists of five phases:

1. Phase 1—The current configuration area on the Net-Net SBC is locked, preventing ACLI users from issuing a **done** or **exit** command from within **config-terminal** mode. It also prevents other Net-Net EMS write operations against the node's configuration.
2. Phase 2—The area holding the current configuration on the Net-Net SBC is erased.

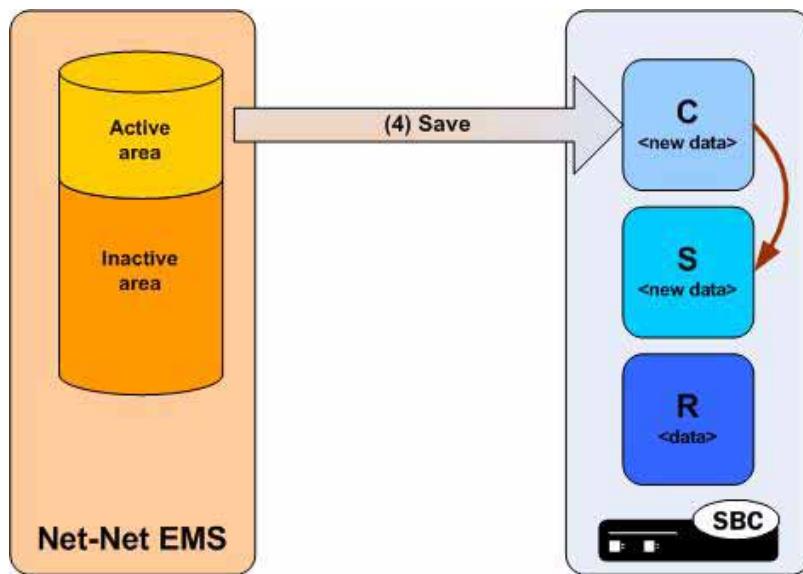


3. Phase 3—The Net-Net EMS downloads the chosen inactive configuration from the Net-Net EMS database into the current configuration area on the Net-Net SBC.



4. Phase 4—The Net-Net EMS instructs the Net-Net SBC to “save” the previously downloaded information by copying the current configuration data to the saved configuration area.

This operation is the same one that takes place on the Net-Net SBC when you enter the **save-config** command at the ACLI system prompt.

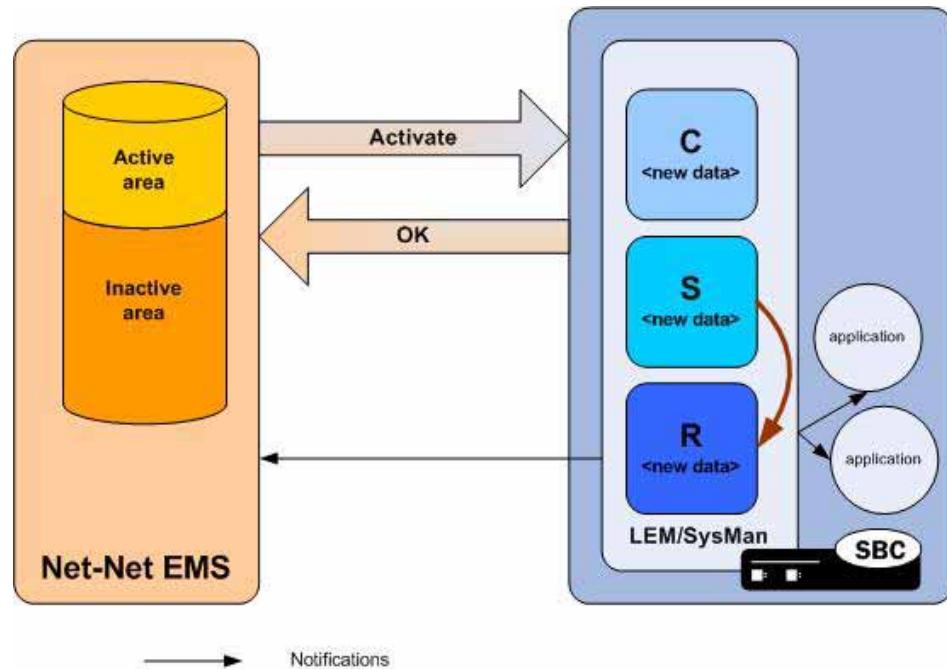


5. Phase 5—The current configuration area on the Net-Net SBC is unlocked.

EMS Activate

During the Net-Net EMS activation process, the Net-Net EMS instructs the Net-Net SBC to activate the saved configuration by making a copy of it in the running configuration area and notifying all the internal Net-Net SBC applications to re-read their data from that area.

This operation is the same one that takes place on the Net-Net SBC when a user types **activate-config** at the ACLI.



The Net-Net SBC returns a response to the Net-Net EMS for the activation request. A positive response means the Net-Net SBC has accepted and initiated the activate request. It takes some further time before the full activation is complete, including all the internal Net-Net SBC application notifications.

Since Net-Net EMS itself is one of the applications notified during that subsequent notification process, it eventually triggers automatic rediscovery of active configuration copy. When that refresh is complete, the entire activation cycle can be considered complete from the Net-Net EMS point of view.

Error Paths

At any time during the operations described above, an error may occur. For example, communication between the EMS and the Net-Net SBC could be disrupted.

This section offers suggested error-handling techniques.

Error during Discovery

- Net-Net SBC—None needed. The Net-Net SBC is unaffected, and EMS will automatically delete any remnants of the failed active configuration copy. In the case of rediscovery, EMS will automatically roll back to the previously discovered data.
- Net-Net EMS—The active copy of data in the Net-Net EMS is now stale, in that it has not been updated to reflect the latest changes on the Net-Net SBC. Manual intervention is required to force a rediscovery again. No further provisioning changes should be made via Net-Net EMS until the situation is resolved.

Error during Copy

- Net-Net SBC—None needed. The Net-Net SBC is unaffected, and Net-Net EMS will automatically delete any remnants of the failed inactive configuration copy.
- Net-Net EMS—None needed, other than reporting feedback that the provisioning attempt has failed and should be restarted.

Error during Save: Phases 1, 2, or 3

- Net-Net SBC—Regardless of which phase the operation is in when the error occurs, the Net-Net SBC remains fully operational. The running configuration copy has not been touched.
- Net-Net SBC—if the error occurs in phase 1 or phase 2, the current configuration area on the Net-Net SBC is now suspect. The first recovery procedure is to try the save operation again using the same configuration copy, because the data within the Net-Net EMS database remains intact. If that fails, the only resort is manual intervention. Manual intervention would involve either:
 - Using the Net-Net EMS GUI to attempt to save the configuration to the Net-Net SBC again, or
 - Using the ACLI to restore a configuration from the backup archive on the Net-Net SBC itself

Even in the absence of such a backup, the previous configuration can still be manually restored to the current configuration area through more detailed ACLI-based procedures performed with the help of Acme Packet Technical Assistance Center (TAC).

- Net-Net SBC—if the error occurs in phase 3, the current configuration area is acceptable, but the saved configuration is suspect. The recovery procedures are the same.

- Net-Net EMS—After the manual recovery procedures have been completed on the SBC side, a rediscovery should be initiated from EMS to ensure that its active copy is in sync with the Net-Net SBC's restored configuration.

Error during Activate

- Net-Net SBC—An activate error indicates that Net-Net SBC was unable to propagate the entire new configuration to the internal application software or that the configuration was rejected by the application software.

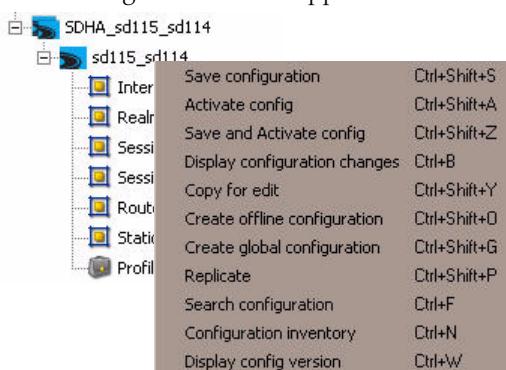
Such an error could potentially effect Net-Net SBC operational behavior. The recovery procedure is to save and activate a known good configuration from the Net-Net EMS database. If that also fails, manual intervention via the ACLI is required to restore a configuration from the backup archive on the Net-Net SBC itself.

- Net-Net EMS—After the manual recovery procedures have been completed on the Net-Net SBC side, you should initiate a rediscovery from the Net-Net EMS to ensure that its active copy is synchronized with the Net-Net SBC's restored configuration.

Save and Activate EMS Commands

To access the Net-Net EMS save and activate commands:

1. Right click the Net-Net SBC you are configuring in the Net-Net EMS navigation tree. The right click menu appears.



2. Click one of the following Net-Net EMS save and activate options:
 - **Save configuration**—To perform a save operation on this configuration
 - **Activate config**—To perform an activate operation on this configuration
 - **Save and Activate config**—To perform a save and activate operation on this configuration

Saving Configurations

There are two methods for saving a configuration in Net-Net EMS: save and full save. The save process (also known as incremental save) modifies only those configuration elements you have changed. Your new configuration elements are saved along with the rest of the original configuration on the Net-Net SBC. During the save process, multiple users can work simultaneously on the same Net-Net SBC configuration copy.

The full save process erases all previously-configured elements on the Net-Net SBC. During the full save process, other users are not able to access this Net-Net SBC configuration copy until all configuration elements are successfully replaced and saved. Only users with admin privileges can perform a full save operation.

Save Method

When you launch the save process, a save session identifier string is generated. This string contains your user name and the current system uptime. Net-Net EMS stores your save session identifier string and your changes made to this Net-Net SBC configuration copy in the configuration changes table as records, also referred to as a staging table. These records make up the save session and display during the save process.

Other users can view the configuration changes table to see all of the records that make up your save session. The configuration changes table includes a field indicating whether a change record is currently being saved or not, and a field indicating the success or failure of the save operation. If you make additional configuration changes while your save operation is in progress, your new changes will not be part of the ongoing save session. You must begin a new save session to include these changes.

During a save session, other save requests to the same configuration copy are queued in the concurrent multiple save request queue in the order received by Net-Net EMS client, and are subsequently processed.

All commands, with the exclusion of save, are not permitted when at least one incremental save is launched.

Early Contention Detection

Early contention detection occurs when two Net-Net EMS users try to modify the same configuration object; for example, edit the same service/protocol within the same realm on the same Net-Net SBC configuration copy. Net-Net EMS detects conflicts by checking the configuration changes table for changes made to a Net-Net SBC configuration copy. All session changes are recorded in the configuration changes tables by the user ID, configuration copy, and save session. If a conflict is found, you will be stopped from editing or deleting the record with a pop-up message: "This record is currently staged by other user. Please try after it is saved to SBC."

When you are working within the same configuration copy of a Net-Net SBC as other users, you can view their changes from within the configuration changes tables (each configuration change is logged with the user's ID and time stamp). This way, you can choose to work in a configuration element not currently being modified by another user.

Users with administrator privileges can transfer the ownership of another user's records to themselves. This transfer eliminates a potential conflict that might occur if the user and the admin user attempt to modify the same configuration object on

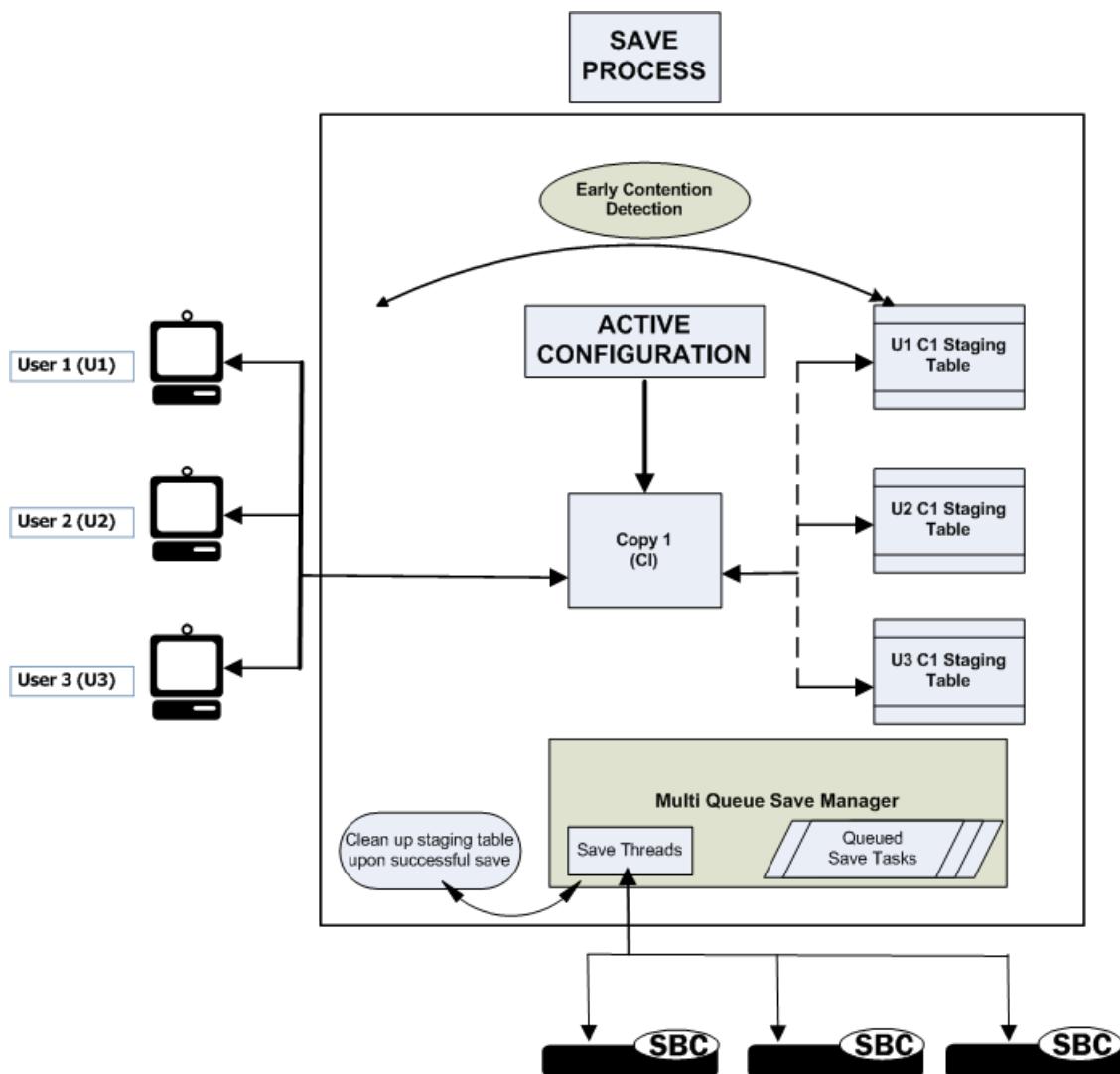
the same Net-Net SBC configuration copy. Following the transfer of records, the admin user can continue to work on the same Net-Net SBC configuration copy they would otherwise be locked out of.

Users with administration privileges can create new users and new user groups, and set group-based authorization where users are assigned to groups with different levels of authorization.

By setting authorization, you assign permissions to the group to which a user belongs. The permissions for that group are assigned to the user. When a user logs into Net-Net EMS, they can access features and functionality based on the permissions assigned to them. For more information about administrator permissions, please see the *Net-Net EMS Administration Guide*.

Example of Save Process

The figure below illustrates the save process.



Configuration Operations Lockout

A configuration operations lockout can occur if a conflict is detected during the configuration validation between the Net-Net EMS and the Net-Net SBC during a save process. One way such a conflict could occur is if an ACLI user or a Net-Net EMS user modified a configuration element on the Net-Net SBC that conflicts with another users modifications in the current save task.

Once a configuration copy is locked it can no longer be used. At this point, you can view and write down all of your failed changes listed in the configuration changes table. You must then make a fresh Net-Net SBC configuration copy, reconfigure your changes, and attempt another save. The locked out Net-Net SBC configuration copy must be deleted by an admin user.

You can minimize configuration operations lockout by working with the same Net-Net SBC configuration copy (not multiple Net-Net SBC configuration copies). Checking the current records stored in the configuration changes table before making changes ensures your work will not conflict with another user working with the same configuration element in the same Net-Net SBC copy.

Full Save Method

If you have full save configuration permission, you can perform an optional full save. The full save process erases the entire configuration on the Net-Net SBC and replaces it with the full set of information you are saving from the configuration copy. During the full save process, a new set of object IDs are generated on the Net-Net SBC. These object IDs uniquely identify each configuration instance of each configuration type. When a full save is in progress, other users cannot modify the same Net-Net SBC configuration copy. They must wait until the full save has successfully completed.

To determine if a full save operation has been started, refer to the discovery table column, "Last save mode," found in the Active configuration window. This column will display full save when a full save operation has been initiated for a Net-Net SBC configuration copy. You can also view Last save mode status from the Discovered node properties window. This is accessed by right clicking on the Host name/IP address in the Active configuration window. Click Properties.

Following a full save, all existing copies of this Net-Net SBC become stale. It is not possible to perform an incremental save on these stale copies. Net-Net EMS will not permit incremental save attempts. If a save is attempted on one of these copies following a full save, you will get the following message: "Normal save operation is not allowed on this copy since this copy is stale." From this point forward, only full save operations are permitted on these existing configuration copies.

Performing Save and Full Save

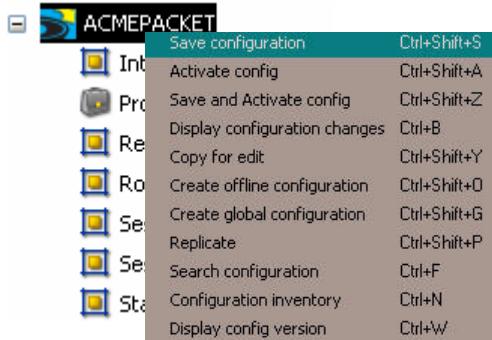
If you have the required permissions, you can perform both a save operation and a full save operation. Anyone belonging to the admin user group has permission to perform full save.

Performing a Save Operation

When you do not have full save permissions granted, you can perform save and save and activate operations only.

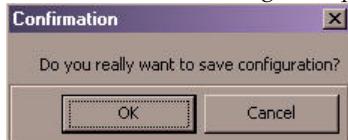
To perform a save configuration operation:

1. Right click the Net-Net SBC you are configuring in the Net-Net EMS navigation tree. The right click menu appears.



2. Click **Save configuration**.

The Confirmation dialog box appears.

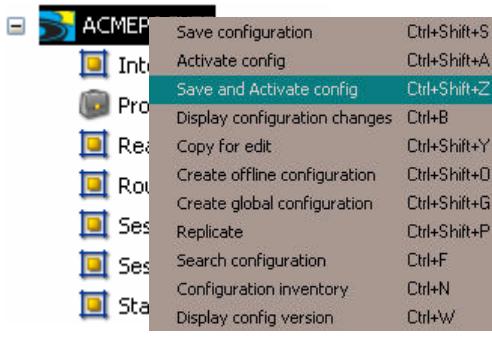


3. Click **OK**.

Performing a Save and Activate Operation

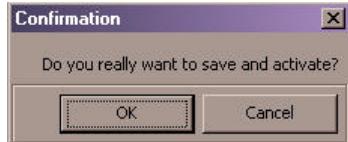
To perform save and activate:

1. Right click the Net-Net SBC you are configuring in the Net-Net EMS navigation tree. The right click menu appears.



2. Click **Save and Activate config**.

The Confirmation dialog box appears.



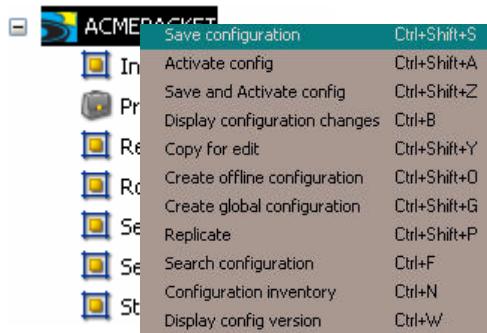
3. Click **OK**.

Performing a Full Save Operation

When you have full save permissions granted, you can perform a full save operation.

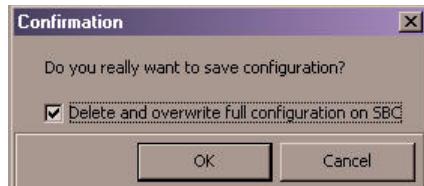
To perform a full save operation:

1. Right click the Net-Net SBC you are configuring in the Net-Net EMS navigation tree. The right click menu appears.



2. Click **Save configuration**.

The Confirmation dialog box appears.

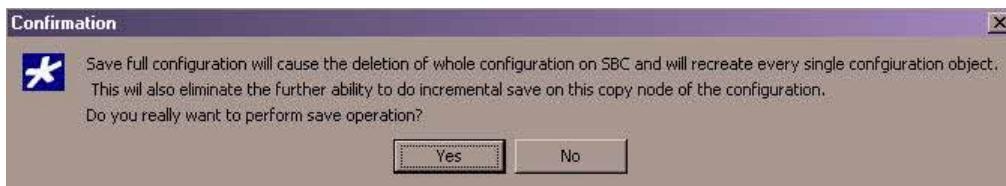


3. **Delete and overwrite full configuration on SBC**—(*Authorized admin users only*) Click the checkbox to perform a full save operation on this Net-Net SBC. (The full save operation erases the entire existing cache and creates a new one, which includes your changes.)

Note: You must have Save full configuration permissions assigned in order to perform this operation.

4. Click **OK**.

The Confirmation message appears.



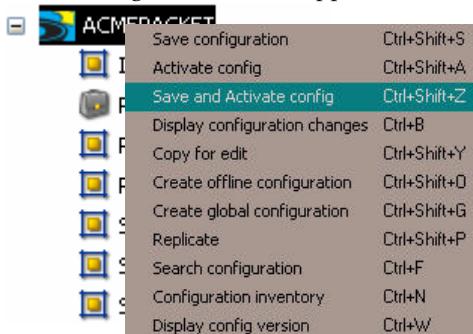
5. Click **Yes** to continue or **No** to cancel this operation.

Performing a Full Save and Activate Operation

When you have full save permissions granted, you can perform a full save activate operation.

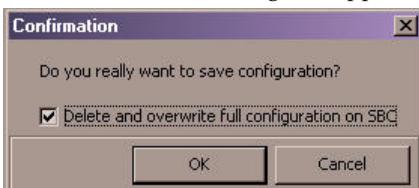
To perform full save and activate operation:

1. Right click the Net-Net SBC you are configuring in the Net-Net EMS navigation tree. The right click menu appears.



2. Click **Save and Activate config**.

The Confirmation dialog box appears.

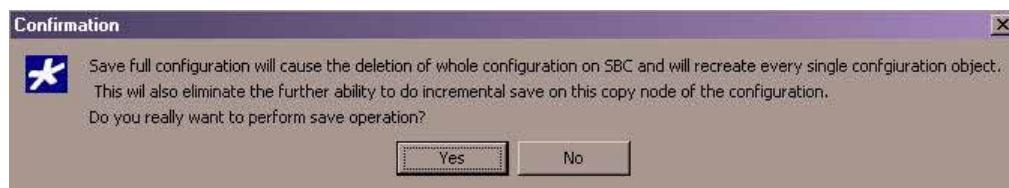


3. **Delete and overwrite full configuration on SBC**—(*Authorized admin users only*) Click the checkbox to perform a full save operation on this Net-Net SBC. (The full save operation erases the entire existing cache and creates a new one, which includes your changes.)

Note: You must have Save full configuration permissions assigned in order to perform this operation.

4. Click **OK**.

The Confirmation message appears..

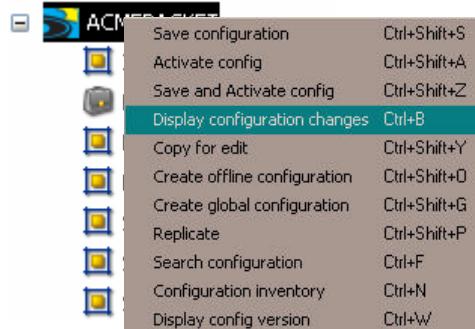


5. Click **Yes** to continue or **No** to cancel this operation.

Accessing the Configuration Changes Table

To review configuration changes for a Net-Net SBC configuration copy:

- Right click the Net-Net SBC you are configuring to open the right-click menu.



- Click **Display configuration changes**. The Configuration changes for this Net-Net SBC configuration copy appear.
- Current list of users with active session**—Click the down arrow to view the list of users that currently have an active save session on this Net-Net SBC configuration copy.

Click the user whose current save session you want to view. Click **All** to view all users with a current save session.



The Session log displays the configuration changes for the user(s) you select.

The screenshot shows a window titled "Configuration changes for sd150_sd151 Copy: SDHA_sd150_sd151". At the top, there is a dropdown menu labeled "Current list of users with active session" with "admin" selected. Below this is a table titled "Session log" with the following columns: Type, Instance, SBC, User, Operation, Time stamp, and Save session sta... (partially visible). The table contains several rows of data, each representing a configuration change made by the user "admin". At the bottom of the window are buttons for Transfer, Refresh, Export, and Close.

| Type | Instance | SBC | User | Operation | Time stamp | Save session sta... |
|-----------------|-----------------------|-------------|-------|-----------|-----------------------|----------------------|
| realmConfig | realm-63 | sd150_sd151 | admin | ADD | 2009-03-27-20-34-0... | admin2009-03-27-2... |
| steeringPool | realm-63#11.11.76.... | sd150_sd151 | admin | ADD | 2009-03-27-20-34-0... | admin2009-03-27-2... |
| sipInterface | realm-63 | sd150_sd151 | admin | ADD | 2009-03-27-20-34-1... | admin2009-03-27-2... |
| sessionAgent | SA-63 | sd150_sd151 | admin | ADD | 2009-03-27-20-34-1... | admin2009-03-27-2... |
| localPolicy | Route124 | sd150_sd151 | admin | ADD | 2009-03-27-20-34-1... | admin2009-03-27-2... |
| sipManipulation | sipman-63 | sd150_sd151 | admin | ADD | 2009-03-27-20-34-2... | admin2009-03-27-2... |
| realmConfig | realm-64 | sd150_sd151 | admin | ADD | 2009-03-27-20-34-2... | admin2009-03-27-2... |
| steeringPool | realm-64#11.11.79.... | sd150_sd151 | admin | ADD | 2009-03-27-20-34-3... | admin2009-03-27-2... |
| sipInterface | realm-64 | sd150_sd151 | admin | ADD | 2009-03-27-20-34-5... | admin2009-03-27-2... |
| sessionAgent | SA-64 | sd150_sd151 | admin | ADD | 2009-03-27-20-35-0... | admin2009-03-27-2... |

The Session log displays data pertaining to a particular session for a selected user(s):

- Type—Top level object type for which modifications have been made
- Instance—One or more instances within a top level object where modifications have been made
- SBC—Net-Net SBC to which modifications have been made

- User—The user that made modifications to a Net-Net SBC copy
- Operation—Type of operation performed by a user: Delete, Add, Modify
- Timestamp—Date and time (in milliseconds) when changes were made to this Net-Net SBC copy
- Save Session Status—Includes the save session ID, which is generated when a save operation is executed, and the status of the save operation: success, failed, and configuration operations lockout

Note: Session log details are automatically deleted following a successful save operation.

4. Click one of the buttons to perform the following actions:
 - Transfer—(*Authorized administrator users only*), Transfers the ownership of staged records from the selected user to you.
 - Refresh—Refreshes the data for this session log by updating with the most recent configuration changes on this Net-Net SBC copy. There is no automatic refresh.
 - Export—Exports this session log to a local file system for review or archive purposes
 - Close—Closes the Session log window

Locking Your Configuration

You can mark a configuration in either the Active or the Inactive configuration list as locked, which prevents other users from modifying that Net-Net SBC configuration using Net-Net EMS. While locked, you can make your edits to the configuration but no other user can modify it nor perform any operations such as copy it for edit, save it, activate it, and so on. Locking the active node ensures that only one user can provision the node by performing all right-click operations, except for the inventory function.

The lock state is saved to the database and is preserved across standalone server restarts and HA failovers. An audit trail entry is logged for the node locking and unlocking operations.

Locking active and inactive configuration nodes in Net-Net EMS applies only to the nodes maintained in Net-Net EMS. It has no impact on the Net-Net SBC itself or on the users of the Acme Packet command line interface (ACLI).

Lock Privileges

The node locking feature is available to users with the SD system configuration and Admin privileges. In addition, the Admin user can override any user's lock to unlock a node. This privilege is enabled by default for the Admin user. See the *Net-Net EMS Administration Guide* for more information about permissions. If you try to lock a node already locked by another user, the error message that appears contains the name of that other user.

Locking and Unlocking an Inactive Configuration

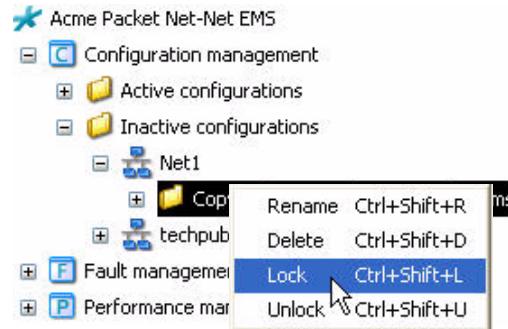
When you lock your copy of a Net-Net SBC configuration in the Inactive configuration area, all nodes below that configuration node are also locked to prevent other users from modifying them. Only the user who locks the configuration

can modify it. The configuration only becomes available to other users after it is unlocked.

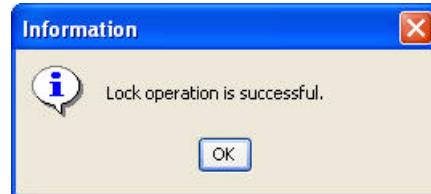
Only the user who locked the node can unlock it, with the exception of the user with Admin privileges. The Admin user can always override any user's lock by unlocking a node.

To lock an inactive configuration:

- Right-click the configuration in the Inactive configuration area.

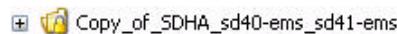


- Choose Lock from the pop-up list of options. A confirmation message appears.



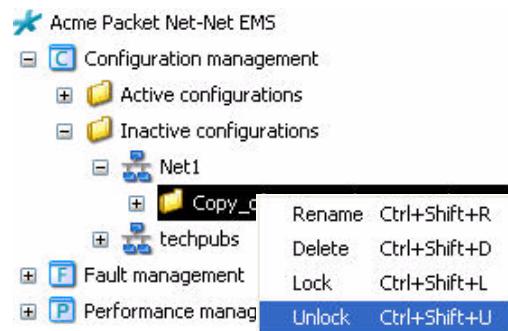
- Click OK to clear the message.

The Net-Net SBC icon in the navigation pane changes to indicate it is locked.

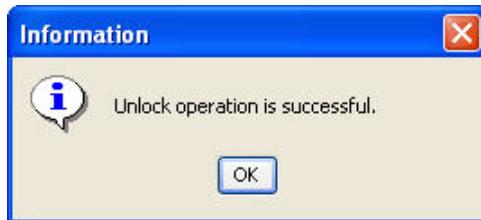


Unlocking an inactive configuration:

- Right-click the configuration in the Inactive configuration area.



- Choose **Unlock**. A confirmation message appears.



- Click **OK** to clear the message. The Net-Net SBC icon in the navigation pane no longer displays a lock.

Locking and Unlocking an Active Configuration

When you lock an active node, only you will be able to perform the right-click operations:

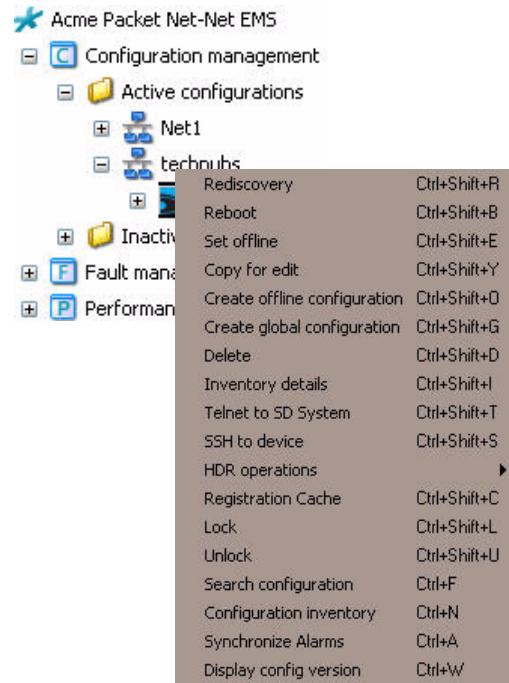
- Rediscovery
- Reboot
- Set offline
- Move
- Copy for edit
- Create offline configuration
- Delete
- Inventory details
- Telnet to System
- SSH to device
- HDR Operations
- Registration Cache
- Lock
- Unlock
- Search configuration
- Configuration inventory
- Synchronize Alarms

Note: Because the Rediscovery operation is locked-out, automatic rediscovery of the Net-Net SBC is blocked. Automatic rediscovery occurs when a configuration on the Net-Net SBC is activated or the Net-Net SBC is rebooted. The user who locked the node has to manually perform a Rediscovery after saving and activating changes to a locked node.

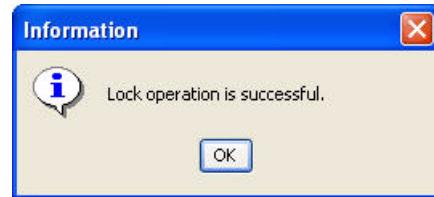
When you lock an active node, you lock the inactive copies associated with that node. All operations for those inactive copies are blocked. Any inactive configuration copies made by other users prior to the active node being locked cannot be applied to the Net-Net SBC while the active node is locked.

To lock an active configuration:

1. Right-click the configuration in the Active configuration area.

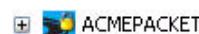


2. Choose Lock from the pop-up list of options. A confirmation message appears.

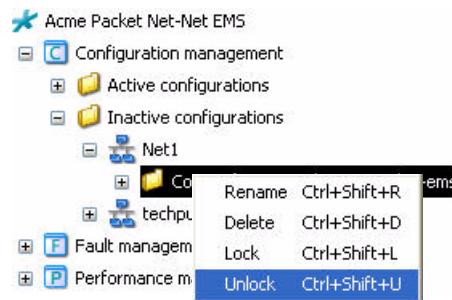


3. Click OK to clear the message.

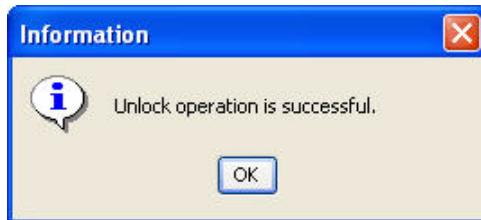
The Net-Net SBC icon in the navigation pane changes to indicate it is locked.

**Unlocking an inactive configuration:**

1. Right-click the configuration in the Inactive configuration area.



- Choose **Unlock**. A confirmation message appears.



- Click **OK** to clear the message. The Net-Net SBC icon in the navigation pane no longer displays a lock.

Configuration Search

You can search for and view top-level objects (for example, sip-interface, SIP manipulation) within an **active** node or **inactive** copy node by typing the Net-Net EMS label or the corresponding ACLI parameter name.

Once you access the configuration object, double-click it to view the details. A window appears and displays the valid settings. You can edit these settings from this window.

Note: Active nodes and nodes locked by another user can only be viewed. Inactive and unlocked nodes can be viewed and edited if the user has the appropriate privileges.

Caveats

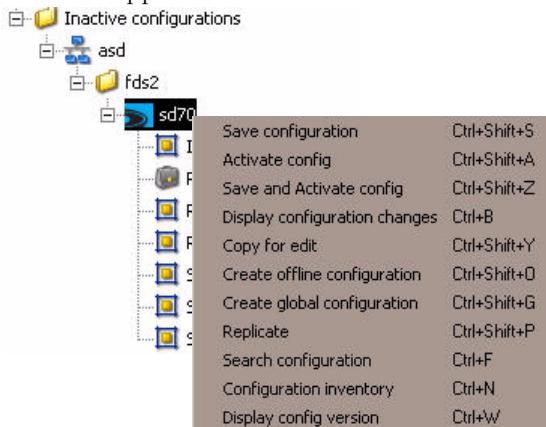
Certain types of configuration objects are not supported:

- Single-instance configuration elements, such as IWF and media manager configuration
- Configuration sub elements that do not lend themselves to viewing outside of the context of their parent element (for example, SIP header rules and element rules)

Searching for Configuration Objects

To use the search configuration function:

- Right-click a Net-Net SBC Active or Inactive configuration. A pop-up list of functions appears.



2. Click Search configuration. The Select an object to search window appears.
3. Choose a configuration object by either:
 - Clicking the down arrow to scroll through the list. Click on the desired object to select it.
 - Typing the object name in the text field. If the name is found in the list, it will auto-complete once enough of the word is typed to distinguish it from others in the list.

Several configuration objects may share similar names, for example, media policy, media profile, and media router. In these instances, you can type “media” and then click the desired object in the list, or keep typing until the object populates the text field. Typing “media po” will populate with “media policy.”

For unique object names, you can type as little as one letter to locate the desired configuration object. For example, when you type “P” the field is populated with “Physical interface.”



The following table lists a brief explanation of top-level objects. You can search for these top-level objects using the Net-Net EMS label or the corresponding ACLI parameter names. See the *ACLI Reference Guide* for parameter names.

| Top-Level Object | Description |
|------------------------------|---|
| Access control | Accesses the Edit Access control window. See the <i>Security</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Account servers | Accesses the Edit Account servers window. See the <i>SIP Signaling Services</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Alarm threshold | Accesses the Edit Alarm threshold window. See the <i>RADIUS Accounting Management</i> chapter in the <i>Net-Net Accounting Guide</i> for more information. |
| Authentication radius server | Accesses the Edit Authentication radius server window. See the <i>Getting Started</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| CODEC policy | Accesses the Edit CODEC policy window. See the <i>Transcoding</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Certificate record | Accesses the Edit Certificate record window. See the <i>Using Net-Net EMS</i> chapter in the <i>Net-Net EMS User Guide</i> for more information. |
| DNS config | Accesses the Edit DNS config window. See the <i>Realms and Nested Realms</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |

| Top-Level Object | Description |
|----------------------------|--|
| ENUM config | Accesses the Edit ENUM config window. See the <i>Session Routing and Load Balancing</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Enforcement profile | Accesses the Edit Enforcement profile window. See the <i>SIP Signaling Services</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| External bandwidth manager | Accesses the Edit External bandwidth manager window. See the <i>Performance Management</i> chapter in the <i>Net-Net EMS User Guide</i> for more information. |
| External policy server | Accesses the Edit External policy server window. See the <i>Admission Control and Quality of Service Reporting</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| H323 service | Accesses the Edit H323 service window. See the <i>H323 Signaling Services</i> chapter in the <i>Net-Net EMS 4000 Configuration Guide</i> for more information. |
| H323 stack | Accesses the Edit H323 stack window. See the <i>H323 Signaling Services</i> chapter in the <i>Net-Net EMS 4000 Configuration Guide</i> for more information. |
| HMR | Accesses the Edit HMR window. See the <i>SIP Signaling Services</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Host routes | Accesses the Edit Host routes window. See the <i>System Configuration</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Interface | Accesses the Edit Interfaces window. See the <i>System Configuration</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| IPSec security association | Accesses the Edit IPSec security association window. See the <i>Security</i> chapter in the <i>Net-Net EMS 4000 Configuration Guide</i> for more information. |
| IPSec security policy | Accesses the Edit IPSec security policy window. See the <i>Security</i> chapter in the <i>Net-Net EMS 4000 Configuration Guide</i> for more information. |
| LR tables | Accesses the Edit LR tables window. See the <i>IMS Support</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Local policy | Accesses the Edit Local policy window. See the <i>Session Routing and Load Balancing</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Local response map | Accesses the Edit Local response map window. See the <i>SIP Signaling Services</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Local routing | Accesses the Edit Local routing window. See the <i>IMS Support</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| MGCP config | Accesses the Edit MGCP config window. See the <i>MGCP/NCS Signaling Services</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |

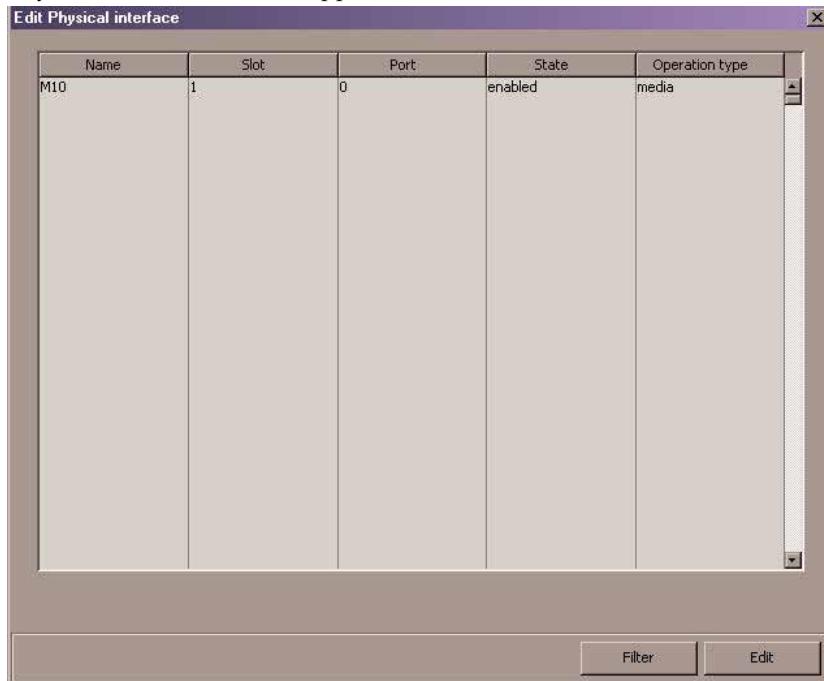
| Top-Level Object | Description |
|----------------------------------|---|
| Management interface access list | Accesses the Edit Management interface access list window. See the <i>Security</i> chapter in the <i>Net-Net EMS 4000 Configuration Guide</i> for more information. |
| Media policy | Accesses the Edit Media policy window. See the <i>Realms and Nested Realms</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Media profile | Accesses the Edit Media profile window. See the following chapters for more information: <i>H.323 Signaling Services</i> , <i>IWF Services</i> , <i>Session Routing and Load Balancing</i> , or <i>External Policy Server</i> , all found in the <i>Net-Net EMS Configuration Guide</i> . |
| Media router | Accesses the Edit Media route window. See the <i>Realms and Nested Realms</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| NM control | Accesses the Edit NM control window. See the <i>Admission Control and Quality of Service Reporting</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Net management control | Accesses the Edit Net management control window. See the <i>Admission Control and Quality of Service Reporting</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Network interface | Accesses the Edit Network interface window. See the <i>System Configuration</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Physical interface | Accesses the Edit Physical interface window. See the <i>System Configuration</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Q850 SIP map | Accesses the Edit Q850 SIP map window. See the <i>SIP Signaling Services</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| QoS marking profile | Accesses the Edit QoS marking profile window. See the <i>Realms and Nested Realms</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| RPH Policy | Accesses the Edit RPH Policy window. See the <i>Security</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| RPH Profile | Accesses the Edit RPH Profile window. See the <i>Security</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Radius server | Accesses the Edit Radius server window. See the <i>Getting Started</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Realm | Accesses the Edit Realm window. See the <i>Realms and Nested Realms</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Realm media access | Accesses the Edit Realm media access window. See the <i>Realms and Nested Realms</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |

| Top-Level Object | Description |
|----------------------|--|
| Route | Accesses the Edit Route window. See the <i>Session Routing and Load Balancing</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| SIP NAT | Accesses the Edit SIP NAT window. See the <i>SIP Signaling Services</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| SIP Q850 map | Accesses the Edit SIP Q850 map window. See the <i>SIP Signaling Services</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| SIP Q850 mappings | Accesses the Edit SIP Q850 mappings window. See the <i>SIP Signaling Services</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| SIP enforcement | Accesses the Edit SIP enforcement window. See the <i>SIP Signaling Services</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| SIP feature | Accesses the Edit SIP feature window. See the <i>SIP Signaling Services</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| SIP interface | Accesses the Edit SIP Services window. {SIP Services includes SIP interface, SIP Nat interface, and SIP Option tag.} See the <i>SIP Signaling Services</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| SIP manipulation | Accesses the Edit SIP manipulation window. See the <i>SIP Signaling Services</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| SIP option tag | Accesses the Edit SIP option tag window. See the <i>SIP Signaling Services</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| SIP response map | Accesses the Edit SIP response map window. See the <i>SIP Signaling Services</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| SNMP community | Accesses the Edit SNMP community window. See the <i>System Configuration</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Security association | Accesses the Edit Security association window. See the <i>Security</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Security policy | Accesses the Edit Security policy window. See the <i>Security</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Session agent | Accesses the Edit Session agent window. See the <i>SIP Signaling Services</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Session agent group | Accesses the Edit Session agent group window. See the <i>SIP Signaling Services</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |

| Top-Level Object | Description |
|---------------------|---|
| Session constraints | Accesses the Edit Session constraints window. See the <i>Admission Control and Quality of Service Reporting</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Session group | Accesses the Edit Session group window. See the <i>Admission Control and Quality of Service Reporting</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Session translation | Accesses the Edit Session translation window. See the <i>Address Translation</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Static flow | Accesses the Edit Static flow window. See the <i>Static Flows</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Steering pools | Accesses the Edit Steering pools window. (Steering pools may also be invoked using the Net-Net EMS label, Realm media address.) See the <i>Realms and Nested Realms</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Surrogate agent | Accesses the Edit Surrogate agent window. See the <i>IMS Support</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Syslog servers | Accesses the Edit Syslog servers window. See the <i>System Configuration</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| System access list | Accesses the Edit System access list window. See the <i>Security</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| TLS profile | Accesses the Edit TLS profile window. See the <i>Security</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Translation profile | Accesses the Edit Translation profile window. See the <i>Address Translation</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Translation rules | Accesses the Edit Translation rules window. See the <i>Address Translation</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Trap destination | Accesses the Edit Trap destination window. See the <i>System Configuration</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |
| Trap receiver | Accesses the Edit Trap receiver window. See the <i>System Configuration</i> chapter in the <i>Net-Net EMS Configuration Guide</i> for more information. |

4. Click OK. Net-Net EMS searches for and displays the configuration screen for the object.

For example, if you had chosen the Physical interface top-level object, the Edit Physical interface window appears.



From here, refer to the *Net-Net EMS Configuration Guide*, or the *Net-Net EMS Accounting Guide* for configuration instructions.

Introduction

With work order administration you can perform global software upgrades and global parameter changes across a targeted group of Net-Net SBCs. You create a customized work order, assign your Net-Net SBCs (also referred to as targeted devices), to your work order, and execute it to apply the changes.

Note: The Net-Net EMS does not support work order administration for the following configuration elements: MGCP endpoint profile and Class policy.

Work orders support three types of operations:

- Software upgrade only: Allows you to automatically upgrade the software version for multiple Net-Net SBCs.
- Global parameter changes only: Allows you to automatically provision multiple Net-Net SBCs by changing configuration parameters.
- Combined software upgrade and global parameter changes: Allows you to perform a software upgrade followed by global parameter changes to multiple Net-Net SBCs.

A work order consists of:

- Work order type: Software upgrade, global parameter changes, or both a software upgrade, followed by global parameter changes.
- Platform: The Net-Net SBC platform chosen for this work order, for example Net-Net 3800. You cannot pick more than one platform for a work order.
- Targeted devices: The devices specified within the work order grouped by platform and software version, for example, Net-Net 4000, release 6.0.0, and according to device node: Standalone Net-Net SBCs or HA pairs. You cannot have both types of device nodes within one work order.
- Work flow: A predefined work flow that defines the execution procedure (steps to be performed on the targeted Net-Net SBCs) and is based on the type of work order you select: Software upgrade only, global parameter changes only, or software upgrade followed by global parameter changes.
- Device tasks: The individual operations performed on the targeted devices.

About Work Order Administration

Work orders begin in the Work Order Administration window accessed by clicking Work Order Administration in the Tools menu.

Predefined Work Flows

There is a predefined work flow process for each of the three types of work orders. A predefined work flow is the automated steps the Net-Net EMS performs to complete the work order. Once you select the type of work order you want to execute and the targeted devices you want to configure, the Net-Net EMS processes these steps until your work order is completed. Refer to "Procedural Steps for Work

Orders" on page 142 for tables listing the steps and corresponding processes for all work-order scenarios.

Each predefined work flow has a corresponding predefined rollback process, in case a rollback to the previous state is necessary. You cannot edit the predefined work flows.

Software Upgrade

If you are performing a software upgrade only, once your work order is created, you can manually execute it or set it to execute automatically at a time you specify. For example, you can configure Net-Net EMS to perform these upgrades during a maintenance window. Net-Net EMS then upgrades the targeted Net-Net SBCs in your work order one-at-a-time until the work order is completed.

Global Parameter Changes

If you are performing global parameter changes, you must first create a global configuration group, which is similar to the Net-Net EMS domain for your global configuration. Next, you create your global configuration with the provisioning changes you want to send to your selected group of targeted devices. The global configuration attributes can be set from default values or can be taken from the configuration of an existing Net-Net SBC. Next, you create the work order, associate the global configuration with the work order and execute it, or schedule it to execute.

When the global parameter changes are completed, the inactive copy of the configuration is updated along with the Net-Net SBCs running configuration, ensuring the inactive copy is synchronized with the running configuration on the Net-Net SBC that has been modified.

Net-Net EMS automatically picks the inactive copy with the latest modification timestamp if multiple copies of inactive configurations exist for a Net-Net SBC, however, it is up to the user to ensure that the selected copy is up-to-date with the device.

Combined Upgrade and Parameter Changes

If you are performing a combined software upgrade and global parameter changes, Net-Net EMS always executes the software upgrade portion of the work order first. The global parameter changes always execute after software upgrades.

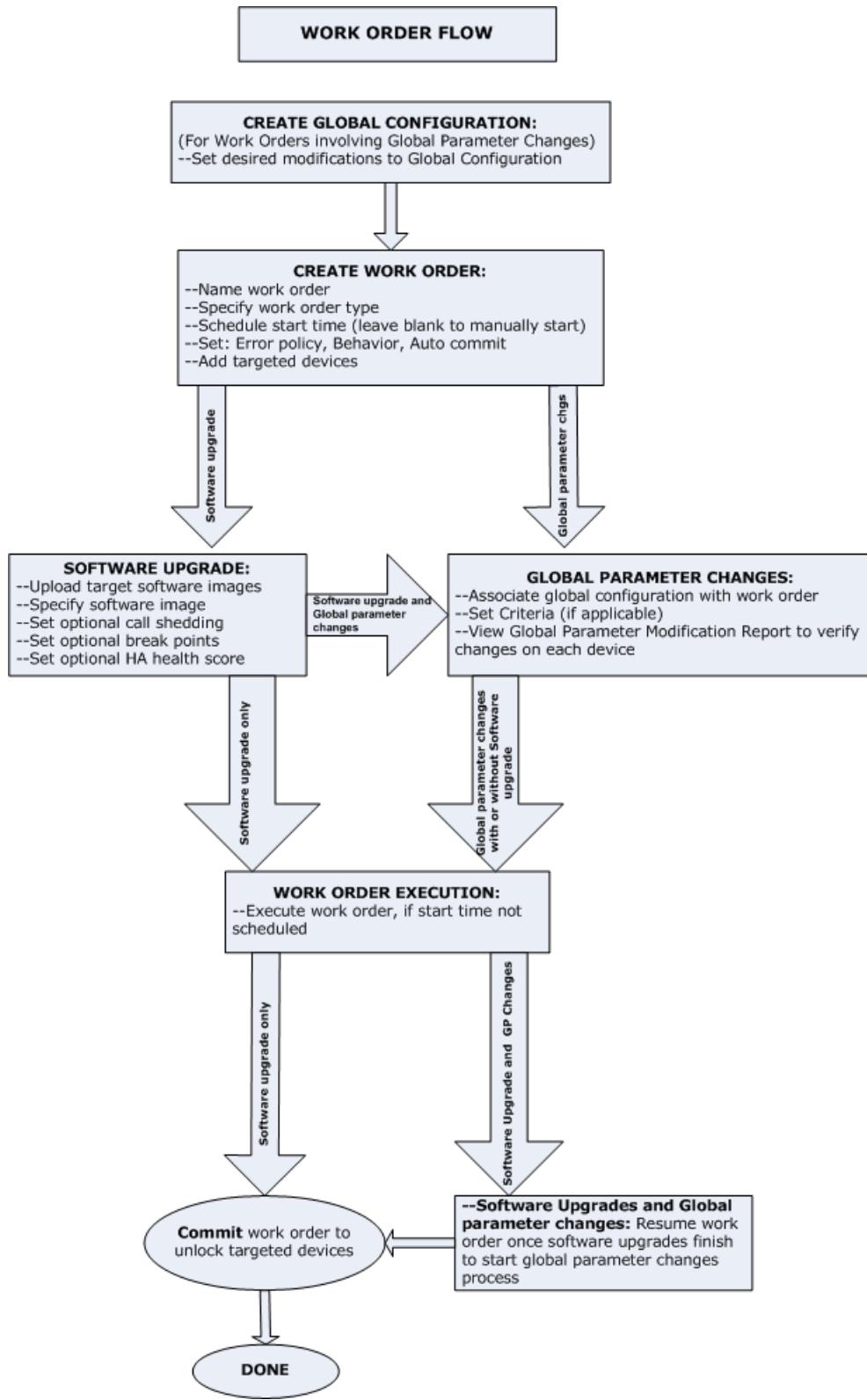
Work Order Phases

There are three phases for work orders:

5. Preparation—Determine the type of work order you need to create:
 - Software upgrade: You must archive the new and existing (i.e., running) software images in the event you need to roll back.
 - You must ensure that sufficient space exists on the flash file system of all targeted devices to hold the target software image.
 - Global parameter changes: You must create the global configuration.
6. Creation and modification—Create the work order by giving it a unique name, specifying its type, scheduling the start date and time (or leaving the start time blank to manually start it) and setting the error policy and behavior. You also select the targeted devices to which you want to assign to this work order.
 - If you are performing a software upgrade, you must specify the target software image.

- Configure optional call shedding (a configurable threshold of active calls).
 - Set an optional breakpoint (a pause after a device is upgraded).
 - Set an optional health score threshold (for HA nodes only).
 - Global parameter changes: you must specify the global configuration you created during the work order preparation phase.
7. Execution and committal—The work order executes at the date and time set during the configuration phase, or you can manually execute the work order. Once the work order executes, you commit the work order to unlock all targeted devices associated with the work order. If a targeted device is linked to a work order that has not been committed, no other users can copy and configure that Net-Net SBC.
- Note:** You can schedule a maximum of four concurrent work orders to execute within a 24-hour period and, you can have a maximum of four concurrent work orders running at any one time.
- Note:** When a work order has completed, but has not yet been committed, it retains a lock on all its targeted devices. This means that no other operations can be performed on those devices.

The following diagram illustrates the work order flow.



Before You Start

User Permissions

The work order operations you can perform depend on the user permissions you have assigned. With the following user permissions assigned, you can perform operations relating to global software upgrades and global parameter changes:

- Administration: Create, modify, execute, and control a work order. With administration privileges, you can also delete a work order.
- Provisioner: Execute and control (start, abort, pause, resume, or commit) a work order.
- Monitor: View work orders only.

For more information about permissions, please see the *Net-Net EMS Administration Guide*.

High Availability Requirements

To use work order administration with a Net-Net EMS HA pair, archived and backup configuration files must exist on both Net-Net EMS hosts running as an HA pair. The SFTP server must be running on both UNIX systems for the Net-Net EMS HA pairs to automatically transfer any software images or configuration backup data retrieved from the Net-Net SBC.

You must ensure:

- SFTP server is running on both the active and standby Net-Net EMS.
- Port number 22 is open if a firewall exists between the Net-Net EMS servers.
- You have a valid user name and password for SFTP access that are common to both the active server as well as the standby server.

Note: Acme Packet strongly recommends that the nnems user be configured as the SFTP user. See the *Net-Net EMS Installation Guide* for more information.

- SFTP user name and password are configured on the active Net-Net EMS.

For additional information on configuring HA pairs, see the *Net-Net EMS High Availability Guide*.

Software Image Archive Management

Before you create your work order, you must upload the correct software image to the device software image archive home directory under the Software Image Archive Management tab of the Work Order Administration window. For more information about loading software images, refer to the *Net-Net EMS Configuration Guide, Getting Started* chapter.

The Software Image Archive Management tab displays the Net-Net SBC software image files that you manually uploaded to Net-Net EMS (via FTP or by copying the image from a CD).

You navigate to the Software Image Archive Management tab by clicking Work Order Administration in the Tools menu. From here you can view the software image files, or you can delete them from Net-Net EMS. The device software image archive home directory is listed above the device software image table.

Specifying the Software Image Directory

When you start up Net-Net EMS for the first time, it checks for the existence of a software image directory.

If it does not exist, Net-Net EMS creates it and sets ownership of the directory contents to your defined non-root EMS users (the standard being nnems) with owner read-write-execute permissions. You can have Net-Net EMS create the software image directory in a different location upon first startup.

For instructions on specifying the software image directory location, refer to the *Net-Net EMS Installation Guide, Software Image Directory for Work Order Administration* section.

Note: If you have a Net-Net EMS HA pair, you must upload the correct software image to both servers in the pair.

The screenshot shows a web-based application interface for managing software images. At the top, there is a navigation bar with tabs: 'Work Orders' and 'Software Image Archive Management'. The 'Software Image Archive Management' tab is active. Below the navigation bar, the title 'Device software image archive home /opt/ACMEPacket/devices/softwareImages' is displayed. The main content area is a table listing ten device software images. The table has three columns: 'Device software image name', 'Size(Bytes)', and 'Date'. The data is as follows:

| Device software image name | Size(Bytes) | Date |
|----------------------------|-------------|------------------------------|
| nnC511p40.gz | 13578370 | Thu Jun 03 17:24:42 EDT 2010 |
| nnC600m4.gz | 14398776 | Thu Jun 03 17:25:16 EDT 2010 |
| nnC600p8.gz | 13968257 | Thu Jun 03 17:25:33 EDT 2010 |
| nnSC610m5.xz | 8035444 | Thu Jun 03 17:26:11 EDT 2010 |
| nnSC610p3.gz | 15051235 | Sat Apr 24 00:40:08 EDT 2010 |
| nnSC620p3.xz | 7244888 | Thu Apr 22 01:51:04 EDT 2010 |
| nnSCX620m1.xz | 11061756 | Thu Jun 03 17:26:45 EDT 2010 |
| sd414p22.gz | 10268829 | Thu Jun 03 17:24:10 EDT 2010 |
| sd414p53.gz | 10544898 | Thu Jun 03 17:24:26 EDT 2010 |

At the bottom right of the table, there are two buttons: 'Refresh' and 'Delete'. At the very bottom right of the entire interface, there is a 'Cancel' button.

Software Image Archive Management Data

The following software image archive management information is displayed by the Net-Net EMS:

| Data | Description |
|------------------------------------|---|
| Device software image archive home | The directory the software image files are uploaded to. |
| Device software image name | Name of the Net-Net SBC software image. |
| Size | Size of the software image file in Bytes. |
| Date | Date and time when the file was stored to the disk. |

Software Image Archive Management Actions

The software archive management action buttons allow you to:

| Action | Description |
|---------|--|
| Refresh | Refreshes the software image file data. |
| Delete | Manually deletes the selected software image file from the archive home directory. |
| Cancel | Closes the work order administration window. |

Software Version Requirements

There are two types of software version requirements that apply under certain work order conditions:

- Global parameter changes only: The software version of the global configuration must match the Net-Net SBCs running software version.
- Software upgrade and global parameter changes: The software version of the global configuration must match the target Net-Net SBC software version.

If there are no Net-Net SBCs selected in the work order's targeted device table, the Select SBC dialog box lists all of the Net-Net SBCs managed by the Net-Net EMS server. However, once you add your first Net-Net SBC to the Targeted devices table, the SBC dialog list adjusts to reflect only those Net-Net SBCs with the same hardware type, same software release version, and the same configuration type: HA pair, or standalone device, as the first Net-Net SBC you added.

Software Downgrade Capability

There may be instances when you want to downgrade the software version for multiple Net-Net SBCs. You can perform a software downgrade across a group of targeted devices. The procedure is virtually the same for a downgrade as for an upgrade. The difference is when you select your target software image, you choose a lower software version than the currently-running software version.

Work Order Administration Graphical User Interface

Work orders are created and maintained through the Work Order Administration window, which is accessed by clicking Work Order Administration in the Tools menu.

The Work Order Administration window contains two tabs: Work Orders and Software Image Archive Management. From here you create new work orders, delete any unused work orders, and perform other functions described in the work order actions table below.

Work Orders Tab

Two tables are displayed in the work orders tab of the Work Order Administration window: Work orders and Device tasks. Each table contains data pertaining to the work order in general, and the device tasks contained within each individual work order.

The screenshot shows the 'Work Order Administration' window with the 'Work Orders' tab selected. The window has a toolbar at the top with buttons for Logs, Refresh, Create, Pause, Start, Report, View, Edit, Abort, Commit, Copy, and Delete. Below the toolbar are two tables: 'Work orders' and 'Device tasks'. The 'Work orders' table has columns for Name, Type, Device count, Target SW version, Status, Start time, and End time. The 'Device tasks' table has columns for Name, IP address, Original SW image, Status, Progress, Start time, and End time. Both tables show data for multiple entries.

| Name | Type | Device count | Target SW version | Status | Start time | End time |
|---------------|-----------------------|--------------|-------------------|-------------------|---------------------|---------------------|
| TonyGPTest1 | GP Changes | 2 | SC6.2.0 | NotScheduled | | |
| TonyGpSwTest1 | SW Upgrade+GP Changes | 1 | nnSC620p3.xz | NotScheduled | | |
| TonySwTest1 | SW Upgrade | 1 | nnC600m5.gz | Paused | 2010-06-23 13:24:45 | 2010-06-23 13:24:54 |
| TonySwTest10 | GP Changes | 0 | Unknown | PartialConfigured | | |
| TonyTest1 | SW Upgrade | 1 | nnSC620p3.xz | Committed | 2010-06-23 07:33:39 | 2010-06-23 07:42:43 |
| TonyTest2 | SW Upgrade | 1 | nnSC620p3.xz | Committed | 2010-06-23 07:43:26 | 2010-06-23 10:48:26 |
| TonyTest4 | SW Upgrade | 1 | nnSC620p3.xz | Paused | 2010-06-23 13:12:47 | 2010-06-23 13:24:20 |

| Name | IP address | Original SW image | Status | Progress | Start time | End time |
|-------|---------------|-------------------|--------|----------|------------|----------|
| sd180 | 172.30.80.180 | SC6.2.0 | Ready | 0/5 | | |
| sd181 | 172.30.80.181 | SC6.2.0 | Ready | 0/5 | | |

The Work orders table displays a status summary of the three types of work orders created and maintained in Net-Net EMS.

If you are performing a software upgrade only, three sections appear on the Edit work order window. You access this window by clicking on your work order in the Work order table of the Work Order Administration window and clicking **Edit**. Or, when you create a work order, after you name it, the Edit work order window opens.

General Work Order Attributes:

| | |
|--------------------------------------|------------------------------------|
| Name | SW_GlobalParam-BOS |
| Type | SW upgrade + Global parameter c... |
| Start date and time | [Empty field] ... |
| Error policy | Log error and proceed |
| Behavior | Automatic |
| <input type="checkbox"/> Auto commit | |
| Device type | Net-Net 4250 Standalone |
| Last modified date | 2010-06-02 12:38:38 |

Targeted devices:

| Name | IP address | Current SW image | Inactive copy |
|-------|---------------|------------------|---------------|
| sd180 | 172.30.80.180 | nnC600m5.gz | |
| sd181 | 172.30.80.181 | nnC600m5.gz | |

Add **Delete**

Work flow:

Software upgrade | Global parameter changes |

Target software image: [Empty field] ...

Pause and unlock after loading software image

| Step | Description | Pause after |
|------|---------------------------------------|--------------------------|
| 1 | Check available space at the device | <input type="checkbox"/> |
| 2 | Archive current device software image | <input type="checkbox"/> |
| 3 | Push software image to the device | <input type="checkbox"/> |
| 4 | Edit image name in boot parameters | <input type="checkbox"/> |
| 5 | Do call shedding | <input type="checkbox"/> |
| 6 | Reboot the device | <input type="checkbox"/> |
| 7 | Rediscover the device | <input type="checkbox"/> |

Call shedding **Set HA health score**

Refresh **View Rep...** **Apply** **Cancel**

The first section describes the attributes of the work order: for example, the name, type, and error policy for this work order. The second section lists the Net-Net SBCs selected for this work order and appear in the Targeted devices table. The third section contains the work flow for this work order.

If you are performing global parameter changes, a fourth section called Attribute modification appears on this window. The Attribute modification section lists the parameter names and new values for each parameter change.

Work Order Actions

You can perform the following actions from the Work Orders tab of the Work Order Administration window. The buttons are disabled (or grayed out) when an action cannot be performed at a particular time.

| Action | Description |
|---------|---|
| Logs | Launches the work order log. |
| Refresh | Causes the Net-Net EMS to retrieve the work orders from the server and display the most current status. |
| Create | Launches the Create/Edit work order view. |
| Pause | Waits for the currently-running task to finish and stops gracefully, putting the work order in a paused state. |
| Start | Starts a scheduled or unscheduled work order immediately, restarts a work order, or resumes a work order, depending on the work order state. |
| Report | Launches the Global parameter changes work order report. The button is disabled for Software upgrades. |
| View | Launches the Create/Edit work order view in read-only mode; no configuration changes are possible. |
| Edit | Launches the Create/Edit work order view for editing purposes; a work order cannot be modified if its state is running, stopped, success, or failed. |
| Abort | Aborts the work order (work orders in stopped, failed, success, or scheduled states can be aborted.) <ul style="list-style-type: none"> • After a stopped, failed, or success work order is aborted, all changes on all targeted Net-Net SBCs are rolled back (if required) to their original software version and/or configuration. • After a scheduled work order is aborted, its state changes to unscheduled. |
| Commit | Manually commits a selected work order. The targeted devices are unlocked once a work order is committed. Only work orders with statuses of: Success, failed, abort, or abortFailed can be committed. |
| Copy | Duplicates an existing work order configuration and puts the work order in a partially-configured state. You have to modify the copy of the work order before it can be executed. |
| Delete | Deletes the selected work order from the Net-Net EMS database. The Net-Net EMS will never automatically delete a work order, even when the work order has successfully completed. A work order can only be deleted if its status is PartialConfigured, NotScheduled, or Committed. |

Work Order Table Data

The following table defines the data displayed in the Work orders table:

| Data | Description |
|---------------------|--|
| Name | Name you give the work order. |
| Type | <p>Type of the work order:</p> <ul style="list-style-type: none"> • Software upgrade • Global parameter change • Software upgrade and global parameter changes <p>Global parameter changes always follow the software upgrade process.</p> |
| Device count | Number of targeted device nodes (standalone Net-Net SBCs or HA pairs) the work order will execute. An HA pair is considered one device node. |
| Targeted SW version | <p>Software version on the targeted Net-Net SBCs when:</p> <ul style="list-style-type: none"> • Creating software upgrade work orders; it is the software image version that will be installed. • Creating global parameter changes only work orders; it is the currently-running software version on targeted Net-Net SBCs. |

| Data | Description |
|------------|---|
| Status | <p>The possible statuses of the work order:</p> <ul style="list-style-type: none"> • PartiallyConfigured: Configuration is incomplete. • NotScheduled: Start time is not yet configured. • Scheduled: The start time is configured and scheduled to begin at a set date and time. • WaitStarting: Work order is placed into a run-waiting queue by the Net-Net EMS scheduler and awaits the scheduled time to start running. • Running: Work order started and is currently processing. • Pausing: Work order pauses after Pause is initiated by user. • Paused: Work order stopped completely (initiated by setting an error policy to halt). You must manually resume a stopped task or abort the task. • Resuming: Work order resumes processing. • Success: Work order completed successfully, but has not yet been committed. • Failed: Work order failed during execution. • StartCommitting: Work order is in the StartCommitting state. • Committing: Work order is in the process of committing the changes designated. • Committed: Changes successfully executed by this work order are committed. Until you commit, the former software version, files are still available and you have the opportunity to abort this work order and restore the original software version and/or configuration. • CommitFailed: Work order failed to commit and some of the locked resources or the auto-generated files may fail to remove. • StartAborting: Work order is in the beginning process of aborting. • Aborted: Work order has been successfully aborted. All changes made on all targeted Net-Net SBCs are rolled back and the Net-Net SBCs retain their original state prior to the work order execution. • AbortFailed: Work order failed to abort due to a failure of a device rollback process. • Preloading: This status applies to software upgrades only. The state the work order is in when the "Pause and unlock after loading software image" parameter is enabled in the software upgrade configuration, and the work order is loading the target software image to all targeted devices. • PreloadPause: This status applies to software upgrades only. This state occurs after the work order successfully delivered the target software image to the targeted devices and unlocked the devices. • LockingResources: State when the work order locks all necessary resources. • LockResourceFailed: Work order failed to lock all necessary resources. You can restart the work order in this state. |
| Start time | The Net-Net EMS server start date and local time for this work order. |
| End time | <p>The end time is the Net-Net EMS local time when:</p> <ul style="list-style-type: none"> • The work order finished successfully and paused. • A failed condition has been met and the work order stopped as a result of the failure. • The user manually stops a work order already in progress. |

About Device Tasks

Device tasks are the individual tasks performed for each targeted device in the work order, for example, upgrading the software image on the device, adding a local policy, editing a next hop IP address for a route, and so on. The Device tasks table is found on the Work Order Administration window and displays the information defined below.

| Device tasks | | | | | | |
|--------------|---------------|--------------------|---------|----------|---------------------|---------------------|
| Name | IP address | Current SW version | Status | Progress | Start time | End time |
| sd180 | 172.30.80.180 | SC6.1.0 | Success | 12/12 | 2010-06-02 11:47:48 | 2010-06-02 11:51:36 |
| sd181 | 172.30.80.181 | SC6.1.0 | Success | 12/12 | 2010-06-02 11:52:22 | 2010-06-02 12:03:47 |

Device Task Data

The following table lists the data that pertains to device tasks.

| Data | Description |
|-------------------|---|
| Name | Name of the Net-Net SBC, or targeted device, which can be a standalone device or an HA pair. |
| IP address | Net-Net SBC management IP address. For HA pairs, the IP addresses for each Net-Net SBC appear. |
| Original SW image | Original software image for this Net-Net SBC. |
| Status | <p>Status of an individual task:</p> <ul style="list-style-type: none"> • Ready: Task is ready to run and waiting. • ResetToReady: When a work order resumes, all failed tasks are reset to this state to distinguish it from the initial Ready state. • Running: Task has begun and is running. • Starting: An intermediate state between the Ready and Running states when you submit or resubmit the device task. • Pausing: An intermediate state between Running and Paused states. • Paused: Task was stopped completely, initiated by an error policy to halt the process. A stopped task must be resumed manually, or aborted. • Success: Task has completed execution successfully. • Failed: Task has failed to successfully complete. Any changes made are rolled back. • StartRollingBack: A task starts to abort when you initiate the abort process. • RollingBack: A task is executing the rollback procedure and you manually abort the procedure, or the device task automatically rolls back due to an error during the procedure. • Rolledback: Rollback procedure is successful. • RollbackFailed: A task does not successfully rollback and failure occurs. • Prefloding: A task is loading the target software image to the device. • PrefloadPaused: A task has loaded the target software image to the device and is paused. • PrefloadFailed: A task failed to load the target software image to the device. |
| Progress | <p>Total number of procedural steps completed for this device task. For example, 12/12 indicates 12 steps have completed in a 12-step process within a work order scenario.</p> <p>For a definition of the procedural steps within a work order scenario, refer to "Procedural Steps for Work Orders" on page 142</p> |

| Data | Description |
|------------|--|
| Start time | Net-Net EMS local time that the work order is scheduled to start, or the time when a task within the work order has started. If the work order has not reached its scheduled start time, all individual tasks for this work order will display the same start time. When an individual task begins, the processing start time replaces the scheduled time. |
| End time | Net-Net EMS local time when: <ul style="list-style-type: none"> • Work order finished successfully and stopped. • Failed condition has been met and the work order stopped as a result of the failure. • User manually stops a work order already in progress. |

Software Image Archive Management Tab

The Software Image Archive Management tab is found on the Work Order Administration window and is accessed from the Tools menu; select Work Order Administration. This tab displays the Net-Net SBC software image files that you manually uploaded to the Net-Net EMS (via FTP or by copying the image from a CD.)

Refer to "Software Image Archive Management" on page 115 for more information about this tab.

Edit Work Order Window

You edit your work order from the Edit work order window. The window is accessed by clicking Work Order Administration in the Tools menu. From here you can select an existing work order in the Work order table and click **Edit**, or you can click **Create**, which prompts you to name your work order. Once named, the Edit work order window automatically opens.

The screenshot shows the 'Edit work order' window with the following sections:

- General Configuration:**
 - Name: SW_GlobalParam-BOS
 - Type: SW upgrade + Global parameter c...
 - Start date and time: (empty input field)
 - Error policy: Log error and proceed
 - Behavior: Automatic
 - Auto commit
 - Device type: Net-Net 4250 Standalone
 - Last modified date: 2010-06-02 12:38:38
- Targeted devices:**

| Name | IP address | Current SW image | Inactive copy |
|-------|---------------|------------------|---------------|
| sd180 | 172.30.80.180 | nnC600m5.gz | |
| sd181 | 172.30.80.181 | nnC600m5.gz | |
- Work flow:**
 - Software upgrade | Global parameter changes |
 - Target software image: (empty input field)
 - Pause and unlock after loading software image
 - Work flow steps table:

| Step | Description | Pause after |
|------|---------------------------------------|--------------------------|
| 1 | Check available space at the device | <input type="checkbox"/> |
| 2 | Archive current device software image | <input type="checkbox"/> |
| 3 | Push software image to the device | <input type="checkbox"/> |
| 4 | Edit image name in boot parameters | <input type="checkbox"/> |
| 5 | Do call shedding | <input type="checkbox"/> |
| 6 | Reboot the device | <input type="checkbox"/> |
| 7 | Rediscover the device | <input type="checkbox"/> |

Buttons at the bottom include: Call shedding, Set HA health score, Add, and Delete.

Universal Work Order Parameters

The top portion of the Edit work order window includes parameters that apply to all three types of work orders. The following table defines the parameters you configure for all work orders.

| Data | Description |
|---------------------|--|
| Name | Name you give the work order. |
| Type | <p>Type of the work order:</p> <ul style="list-style-type: none"> • Software upgrade. • Global parameter change. • Software upgrade and global parameter changes. <p>Global parameter changes always follow the software upgrade process.</p> |
| Start date and time | <p>Net-Net EMS local time you set for this work order to execute. Leave this parameter blank if you want to execute the work order on demand.</p> |
| Error policy | <p>Determines how to handle errors when they occur during the execution of the work order. You can choose:</p> <ul style="list-style-type: none"> • Log error and proceed (default): Targeted device that experienced the error will be rolled back to its original configuration state and the work order will proceed to the next targeted device in the work order list. • Stop: Targeted device that experienced the error will be rolled back to its original configuration state and the work order will stop. You must manually resume, or abort, the work order. • Stop and rollback: All targeted devices processed up to the time of the error will be rolled back to their original configuration states and the work order will stop. |
| Behavior | <p>Behavior you want to apply to this work order. The two types of behaviors are:</p> <ul style="list-style-type: none"> • Automatic (default): Software upgrade or global parameter changes proceeds on each targeted device without requiring intervention. • Device-level: The software upgrade or global parameter changes pause after each targeted device finishes updating. You must manually continue on to the next targeted device listed in the work order. <p>If an error occurs during the work order execution, the behavior is controlled by the error policy.</p> |
| Auto commit | <p>Work order will be automatically committed after execution. Only work orders with a success status are automatically committed. The default is disabled. When disabled, you must manually commit the work order from the work order administration window to unlock the devices associated with it.</p> |
| Device type | <p>A read-only field that populates when you select the first targeted device in a software upgrade work order or a software upgrade and global parameter changes work order. This field is empty when no device is chosen.</p> |
| Last modified date | <p>A read-only field that shows the Net-Net EMS local time when the work order was last modified.</p> |

About Targeted Devices

The Targeted devices table is universal to all work order types and is found beneath the universal parameters on the Edit work order window. This table lists the targeted

devices you add to this work order. You must add targeted devices for all three types of work orders. You do this by clicking **Add** beneath the Targeted devices table on the Edit work order window. You can add Net-Net SBCs with the following platforms and configurations:

- Net-Net 4000 standalone device
- Net-Net 4000 HA pair
- Net-Net 4500 standalone device
- Net-Net 4500 HA pair
- Net-Net 3800 standalone device
- Net-Net 3800 HA pair

The targeted devices you select must all be:

- From the same platform, for example, Net-Net 4000
- Either standalone devices or HA pairs; mixes are not allowed
- Running the same software release version, for example, C6.1.
 - The patch level can be different.
 - The maintenance level can be different, for example, C6.1M1 and C6.1M2 can be part of the same work order

If there are no Net-Net SBCs selected in the work order's targeted device table, the Select SBC dialog box lists all of the Net-Net SBCs managed by the Net-Net EMS server. However, once you add your first Net-Net SBC to the Targeted devices table, the SBC dialog list adjusts to reflect only those Net-Net SBCs with the same hardware type, same software release version, and the same configuration type: HA pair, or standalone device, as the first Net-Net SBC you added.

Once you have added targeted devices to a work order, information about each appears in the Targeted devices table shown below.

| Targeted devices | | | | |
|------------------|---------------|------------------|--------------------------|--|
| Name | IP address | Current SW image | Inactive copy | |
| sd180 | 172.30.80.180 | nnC600m5.g2 | SW_GP_sd180_0 | |
| sd181 | 172.30.80.181 | nnC600m5.g2 | SW_GP_sd181_1 | |
| | | | Add Delete | |

Targeted Devices Data

The following data pertains to each targeted device listed in your work order.

| Data | Description |
|------------|--|
| Name | Name of the Net-Net SBC, or targeted device, which can be a standalone device or an HA pair. |
| IP address | Net-Net SBC management IP address. For HA pairs, the IP addresses for each Net-Net SBC appear. |

| Data | Description |
|------------------|---|
| Current SW image | Currently running software image on this targeted device. |
| Inactive copy | <p>Pertains to the global parameter changes work order. You should make sure the selected inactive copy configuration is synchronized with the running configuration before beginning the work order.</p> <p>For a work order with both a software upgrade and global parameter changes, there are no inactive copies of configuration following the software upgrade; Net-Net EMS creates a new inactive copy configuration after the software upgrade process is completed.</p> |

About Work Flow

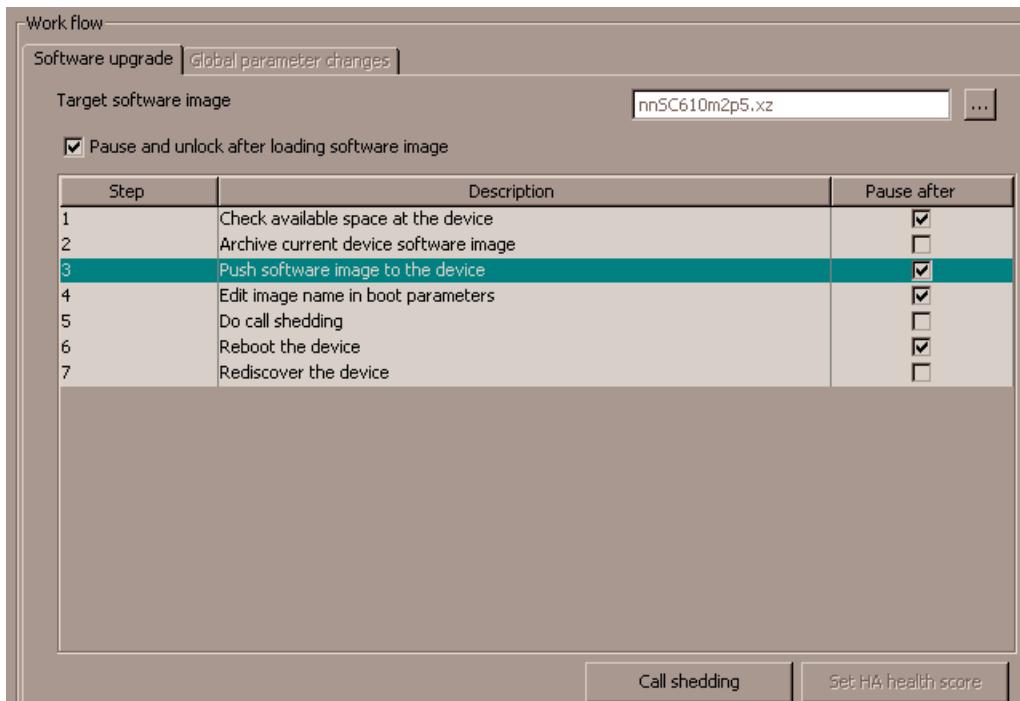
The Work flow portion of the work order is found beneath the Targeted devices table on the Edit work order window and it contains two tabs:

- Software upgrade: Pertains to software upgrades.
- Global parameter changes: Pertains to global parameter changes.

The tabs are disabled when the work order does not include either a software upgrade or global parameter changes as shown in the image below.

Software Upgrade Tab

The Software upgrade tab includes parameters you configure for software upgrades and a list of the procedural steps performed during all software upgrades.



The following table defines the parameters specific to software upgrades.

| Data | Description |
|---|--|
| Target software image | Software image you are upgrading to. |
| Pause and unlock after loading software image | (Optional) The work order is paused after the software image is delivered to all targeted devices. The targeted devices are unlocked once the software is successfully delivered. |
| Break points | (Optional) An intentional stoppage of the work order. When you insert a break point, the work order is stopped after the step preceding the break point successfully completes. You must manually resume the work order. |
| Call shedding | (Optional) During the software upgrade process, the Net-Net SBC will not be rebooted with the new image until the call threshold is reached. |
| Set HA health score | (Optional) Set a health score threshold value for HA pairs only. |

Global Parameter Changes Tab

The Global parameters tab includes parameters you configure for global parameter changes. There are two parameters above the Configuration table:

- Global configuration: You select the global configuration for this work order. The modifications you made to your global configuration are assigned to your work order and are applied to the targeted devices when you execute the work order.
- Version number: A read-only field that contains the software version for this global configuration

| Element name | Element instance | Sub-element inst... | Sub-sub-element... | Operation | Criteria |
|---------------------|---------------------|---------------------|--------------------|-----------|----------------------------|
| SubscribeEvent | | * | | Modify | SubscribeEvent:type=A... |
| EnforcementProfile | hong-enforcement | | | Modify | EnforcementProfile:nam... |
| SubscribeEvent | | test | | Delete | EnforcementProfile:nam... |
| MediaProfile | hong3-media#hong... | | | Modify | MediaProfile:name=ACM... |
| MediaPolicyMedia... | | | send | Delete | MediaPolicyTosSetting:m... |

Configuration Table Data

The Configuration table is found under the Work flow section of the Edit work order window and is a summary of all configuration changes made in the global configuration for this work order. These changes are applied to the targeted devices in your work order when the work order is executed.

The following table defines the parameters specific to global parameter changes in the configuration table:

| Data | Description |
|--------------------------|---|
| Element name | Net-Net SBC configuration element name. |
| Element instance | Multiple key values separated by a space, for example, "val1 val2 val3 val4". |
| Sub-element instance | String value of the key for a sub-element instance. |
| Sub-sub-element instance | String value of the key for a sub-sub-element instance. |
| Operation | <p>Operation performed on this element:</p> <ul style="list-style-type: none"> • Modify: Attributes in the element were changed in this global configuration. • Add: This element was added to this global configuration. • Delete: This element was deleted from this global configuration. |
| Criteria | <p>Criteria used to select the instance(s) of multi-instance elements on the targeted Net-Net SBCs.</p> <p>You will automatically be prompted with the names of all attributes (criteria) that make up the primary key for the selected type of configuration element.</p> <p>The syntax must:</p> <ul style="list-style-type: none"> • Exactly match the specified instance: Input text can be any valid string, for example, IP address string 1.1.1.1, or domain name string, for example, jk.acmepacket.com. • Match any one of the specified multiple instances: The input string can have multiple values separated by a special delimiter (;), for example, 1.1.1.1;12.12.12.12;jk.acmepacket.com. |

Configuration Table Actions

The following table defines the actions you can perform. The buttons are disabled (or grayed out) when an action cannot be performed at a particular time.

| Action | Description |
|--------------|--|
| Refresh | Retrieves the work orders from the server and displays the most current status. |
| Set criteria | <p>Launches the set criteria dialog box for this selected element. You will automatically be prompted with the names of all attributes (criteria) that make up the primary key for the selected type of configuration element.</p> <p>The criteria used to select the instance(s) of multi-instance elements on the targeted Net-Net SBCs:</p> <ul style="list-style-type: none"> • Exactly match the specified instance: Input text can be any valid string, for example, IP address string 1.1.1.1, or domain name string, for example, jk.acmepacket.com. • Match any one of the specified multiple instances: The input string can have multiple values separated by a special delimiter(;), for example, 1.1.1.1;12.12.12.12;jk.acmepacket.com. |

About Attribute Modification

The Attribute modification table is specific to global parameter changes and is found on the Global parameter changes tab of the Edit work order window, beneath the Configuration table. It provides details of the global parameter changes for each modified element listed in the Configuration table. When you highlight an element in the Configuration table the Attribute modification table displays all of the modified attributes for that element in the configuration table.

Note: You may see some attributes in the table that were not hand-modified, but are set as default values. That is OK.

| Element name | Element instance | Sub-element instance | Sub-sub-element ins... | Operation | Criteria |
|--------------|------------------|----------------------|------------------------|-----------|----------------------------|
| SessionAgent | sip-sa | | | Modify | SessionAgent:hostname=A... |

| Name | New value |
|------|-----------|
| port | 5061 |

Attribute Modification Data

The following table defines the data listed in the Attribute modification table.

| Data | Description |
|-----------|--|
| Name | Attribute name associated with this element instance |
| New value | New value you configured for this attribute |

Universal and Work-Order Specific Procedures

The following sections are a combination of the universal procedures you perform for all types of work orders, along with the work-order specific procedures you perform based on the work order type you are creating.

The sections begin with performing a software upgrade and follow sequentially. When a section appears for the first time, it contains procedural steps with corresponding GUI images. Wherever possible, you are referred to these sections containing the information you need at a specific point in the work order administration process.

Performing a Software Upgrade

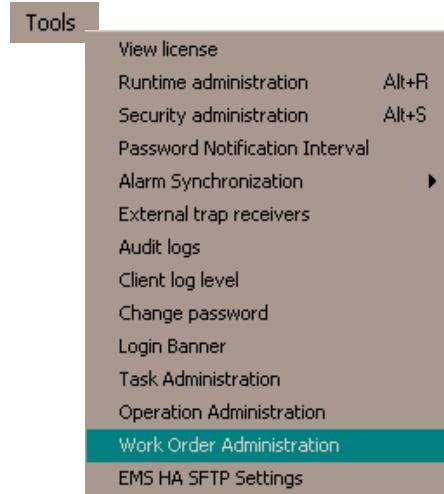
The following procedures show you how to create a work order to perform a software upgrade across a group of targeted devices. First you load your target software image(s) to the software image archive home directory under the Software Image Archive Management tab of the Work Order Administration window. For more information, refer to "Software Image Archive Management" on page 115.

You create your work order, specifying your work order type, and other configurable policies. Next, you pick the targeted devices you want to upgrade and select the target software image. Finally, you set optional call shedding, break points, and an HA health score (applicable to HA pairs only). All of these steps are explained in detail below.

Creating a Software Upgrade Work Order

To create a software upgrade work order:

1. Click the Tools menu in the top menu bar and click Work Order Administration.



The Work Order Administration window appears.

2. Click the Work Orders tab.
3. Click **Create**. The Create work order dialog box appears.

4. **Work order name**—Enter the descriptive name you want to give this work order. The name must be an alphanumeric value from 1 to 24 characters in length.



5. Click **OK**. The Edit work order window appears with the name you assigned to this work order in the Name field. Below is an image of the Edit work order window.

| Name | IP address | Current SW image | Inactive copy |
|------|------------|------------------|---------------|
| | | | |

| Step | Description | Pause after |
|------|-------------|-------------|
| | | |

- Type—Click SW upgrade in the drop down list.



Configuring Target Software Image for Software Upgrades

This procedure is mandatory for all software upgrades.

To configure the target software image for a software upgrade:

- Scroll to Work flow.
- Click the Software upgrade tab.
- Target software image**—Click to open the Select SBC software image dialog box.
- Click the target software image in the Select SBC software image table that you want to upgrade to.

| Select SBC software image | | |
|---------------------------------|-------------|-------------------------------------|
| Device software image file name | Size (KB) | Date/Time created |
| nnC600m5.gz | 14139 | Wed May 12 23:19:14 EDT 2010 |
| nnSC610m2p3.xz | 7733 | Tue May 04 11:38:36 EDT 2010 |
| nnSC610m2p4.xz | 7730 | Tue May 04 11:38:36 EDT 2010 |
| nnSC610m2p5.xz | 7742 | Tue May 04 11:38:37 EDT 2010 |
| nnSC610m3p1.xz | 7819 | Tue May 04 11:38:37 EDT 2010 |
| nnSC610m4.xz | 7826 | Tue May 04 11:38:38 EDT 2010 |
| nnSC620.xz | 7073 | Tue May 04 11:38:38 EDT 2010 |
| nnSC620m1.xz | 7105 | Tue May 04 11:38:40 EDT 2010 |
| nnSC620m2.xz | 7118 | Tue May 04 11:38:39 EDT 2010 |
| nnSC620p1.xz | 7073 | Tue May 04 12:22:25 EDT 2010 |
| nnSC620p2.xz | 7076 | Thu May 06 19:55:22 EDT 2010 |
| nnSC620p2_ORIG.xz | 7076 | Tue May 04 12:22:24 EDT 2010 |
| nnSC620p3.xz | 7075 | Thu May 06 19:07:41 EDT 2010 |
| nnSC620p3_ORIG.xz | 7075 | Thu Apr 22 11:21:43 EDT 2010 |

OK Cancel

- Click OK. The target software image updates with the software image you selected.



Configuring Optional Software Upgrade Parameters

You can configure optional parameters within the software upgrade work order to pause at certain points during the work order process. There are two optional pause settings you can choose from, enabling the **Pause and unlock after loading software image** parameter and/or inserting break points.

Configuring Optional Pause and Unlock After Loading Software Image

When the optional **Pause and unlock after loading software image** parameter is enabled, the work order is paused after the software image is delivered to all targeted devices. The targeted devices are unlocked once the software is successfully delivered. The work order can be later resumed, at which point the Net-Net SBCs will be rebooted using the new images.

To configure pause and unlock after loading software image:

- From the Edit work order window, scroll to Work flow and click the Software upgrade tab.
- Pause and unlock after loading software image**—Click the checkbox to enable the preload pause state for software upgrade work orders. The default is **disabled**.

Pause and unlock after loading software image

Configuring Optional Break Points

You can set optional break points after any step during the work order processing. A break point is an intentional stoppage of the work order. When you insert a break point, the work order is stopped after the step preceding the break point successfully completes. You must manually resume the work order.

To configure break points:

- From the Edit work order window, scroll to Work flow and click the Software upgrade tab.
- Pause after**—Click the checkbox in the Pause after column next to the step in the Step table to initiate a pause after this step completes successfully. You can insert as many breakpoints as you want. The default is unchecked, or **disabled**. The table describes:
 - Step—The number of this task in the work flow order
 - Description—Description of the task associated with this step
 - Pause after—When checked, enables a break point after this step has successfully completed. The default is **disabled**.

| Step | Description | Pause after |
|------|------------------------------------|-------------------------------------|
| 1 | Get available space at the SBC | <input checked="" type="checkbox"/> |
| 2 | Archive current SBC software image | <input checked="" type="checkbox"/> |
| 3 | Push file to SBC | <input checked="" type="checkbox"/> |
| 4 | Retrieve boot parameters | <input checked="" type="checkbox"/> |
| 5 | Push boot Parameters | <input checked="" type="checkbox"/> |
| 6 | Reboot SBC | <input checked="" type="checkbox"/> |
| 7 | Rediscover SBC | <input checked="" type="checkbox"/> |

Configuring Optional Call Shedding

You can configure optional call shedding. With call shedding, during the software upgrade process the Net-Net SBC reboots when the active-call threshold reaches its limit. You can check the performance management MIB to view the current call-shedding count. For more information about the performance management MIB, refer to the *Net-Net 4000 MIB Reference Guide*.

To configure call shedding:

- From the Edit work order window, scroll to Work flow and click the Software upgrade tab.
- Click **Call shedding**. The Call shedding dialog box appears.
- Reject new calls**—Click the checkbox to enable call shedding, whereby the Net-Net SBC rejects new calls during the software upgrade process. The default is **disabled**.

Reject new calls

4. **Active call threshold on SBC**—Enter the threshold number of active calls below which the upgrade/downgrade reboot proceeds automatically.

| | |
|------------------------------|----|
| Active call threshold on SBC | 80 |
|------------------------------|----|

5. Click **OK**.

Configuring a Health Score for HA Pairs Only

If you are configuring an HA pair, you can set a health score threshold value. During the software upgrade process, the Net-Net EMS checks the health score to determine if the Net-Net SBCs are in a stable condition.

Note: If the health score value is set, and the device health is not above the health score value, the software upgrade will not proceed.

Once a new health score value is set, it is displayed in the work flow description check. By default the health score is set to 100%. Set HA health score is disabled when configuring standalone devices.

To configure the health score threshold for HA pairs:

1. From the Edit work order window, scroll to Work flow and click the Software upgrade tab.
2. Click **Set HA health score**. The Set HA Health Score dialog box appears.
3. **Health score threshold (%)**—Enter the health score percentage for this HA pair from 1 to 100 percent.



4. Click **OK**.

Applying Changes

Once you create your software upgrade work order and customize the optional parameter settings, you apply your changes. Refer to "Apply Configuration Changes" on page 160 for information to perform this procedure.

Executing Work Order

Once your work order is created and your configuration is applied, you are ready to execute. You perform this step if you are manually executing your work order. Otherwise, your work order will execute at the date and time you set.

To manually execute your work order:

1. Refer to "Executing a Work Order on Demand" on page 146 for information to perform this procedure.

Committing Work Order

Once your work order is executed, you must commit your work order to unlock all targeted devices associated with your work order.

To commit your work order and unlock all targeted devices associated with your work order:

1. Refer to "Universal Procedure for Committing a Work Order" on page 148 for information to perform this procedure.

Configuring Universal Parameters

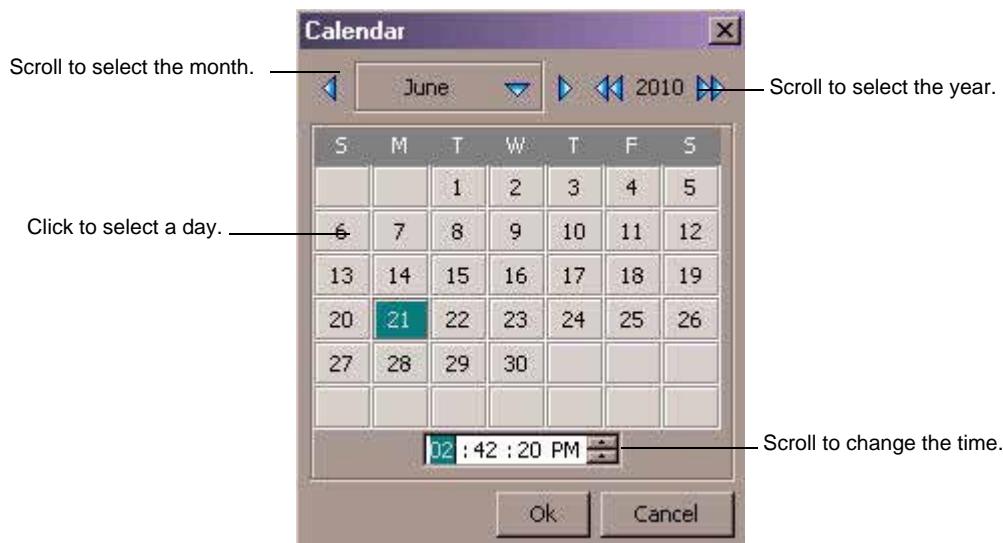
The following parameters are configured no matter what type of work order you choose to execute. These procedures apply to all three types of work orders.

Scheduling Work Order Start Date and Time

This is an optional parameter. You can execute your work order on demand, or you can schedule it to start at a specified date and time.

To schedule the start date and time:

1. From the Work Order Administration window, click on the Work Orders tab.
2. Click the work order you want to schedule the start date and time for and click **Edit**. The Edit work order administration window appears.
3. **Start date and time**—Leave this parameter blank if you want to execute your work order on demand. Otherwise, click  to access the Calendar.



4. Choose the month and the year by using the arrows to scroll to the needed options.
5. Choose the day by clicking the appropriate cell.
6. Choose AM/PM to set ante-meridiem or post-meridiem by scrolling up or down in the time textbox.
7. Click in the time textbox and enter the hour, minutes, and seconds.
8. Click **OK** to exit the Calendar and apply the values.

If you set the time for a period that has passed, you will get an error message.



9. Click **OK** to clear the message.

10. Click **Apply**.

Configuring the Error Policy

The error policy you configure determines how errors are handled when they occur during the execution of your work order.

To configure the error policy:

1. From the Work Order Administration window, click on the Work Orders tab.
2. Click the work order you want to schedule the start date and time for and click **Edit**. The Edit work order administration window appears.
3. **Error policy**—Click the error policy in the drop down list that you want to apply to this work order. The error policy determines how to handle errors when they occur during the execution of the work order. You can choose:
 - Log error and proceed (default)—The targeted device that experienced the error will be rolled back to its original configuration state and the work order will proceed to the next targeted device in the work order list
 - Stop—The targeted device that experienced the error will be rolled back to its original configuration state and the work order will stop. You must manually resume, or abort, the work order
 - Stop and rollback—All targeted devices processed up to the time of the error will be rolled back to their original configuration states and the work order will stop



4. Click **Apply**.

Configuring the Behavior

You configure the behavior you want to apply to this work order.

To set the behavior:

1. From the Work Order Administration window, click on the Work Orders tab.
2. Click the work order you want to schedule the start date and time for and click **Edit**. The Edit work order administration window appears.
3. **Behavior**—Click the work order behavior you want to apply to this work order in the drop down list. The two types of behaviors are:
 - Automatic (default)—The software upgrade or global parameter changes proceeds on each targeted device without requiring intervention
 - Device-level—The software upgrade or global parameter changes pause after each targeted device finishes updating. You must manually continue on to the next targeted device listed in the work order

If an error occurs during the work order execution, the behavior is controlled by the error policy.



4. Click **Apply**.

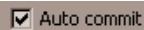
Enabling Auto Commit

This is an optional parameter. When a work order has completed, but has not yet been committed, it retains a lock on all its targeted devices. This means that no other operations can be performed on those devices. Once a work order is committed, the devices associated with the work order are unlocked. If you enable auto commit, your work order will be automatically committed after execution. Only work orders with a success status are automatically committed. The default is **disabled**. When **disabled**, you must manually commit the work order from the work order administration window to unlock the devices associated with it.

Until you commit, you have the opportunity to abort this work order and perform a rollback to restore the original software version and/or original configuration settings.

To enable auto commit:

1. From the Work Order Administration window, click on the Work Orders tab.
2. Click the work order you want to schedule the start date and time for and click **Edit**. The Edit work order administration window appears.
3. **Auto commit**—Click the check box to enable auto commit for this work order. The work order will be automatically committed after execution.



Note: Once a work order is committed, rollback is no longer possible. When you commit a work order, all targeted devices associated with this work order are unlocked.

4. Click **Apply**.

Adding Targeted Devices

You add the targeted devices you want to apply to your work order. Refer to "About Targeted Devices" on page 126 for more information about targeted devices.

To add targeted devices to your work order:

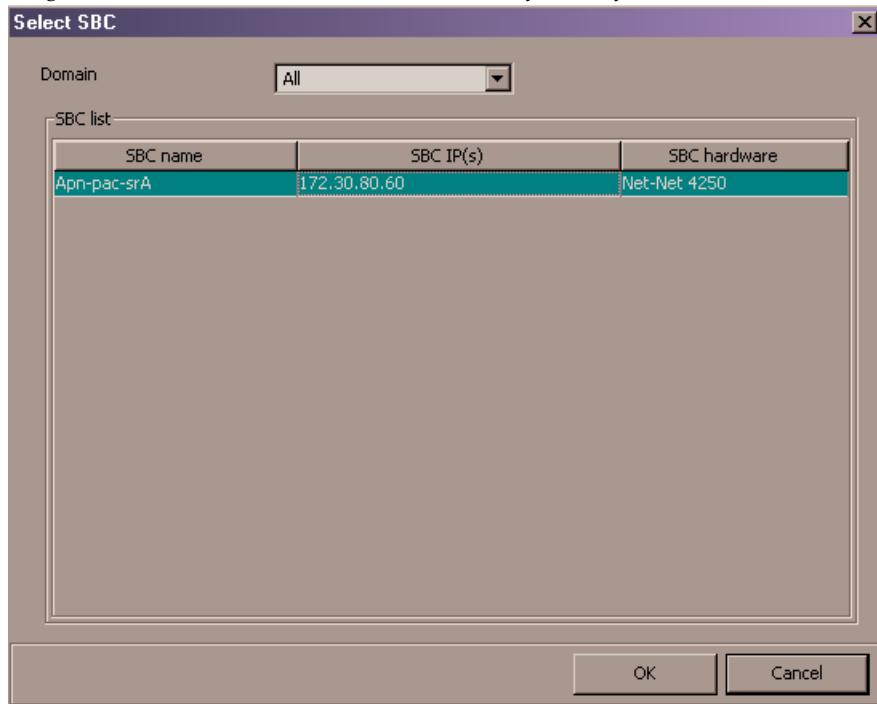
1. From the Work Order Administration window, click on the Work Orders tab.
2. Click the work order you want to schedule the start date and time for and click **Edit**. The Edit work order administration window appears.
3. **Targeted devices**—Click **Add** to add your targeted Net-Net SBCs to this work order. The Select SBC dialog box appears.
4. **Domain**—Click **All** to pick the targeted devices from all available domains. Or click a particular domain in the drop down list to narrow the targeted devices to this domain only.

Note: You can add all of the targeted devices within a domain only if they share the same hardware platform and are running the same software release version.



5. Click the targeted devices you want to add in the SBC list and click **OK**.

6. Repeat steps 3 through 5 to add additional targeted devices. To add multiple targeted devices at one time, hold the **Ctrl** key while you click each device.



7. Click **OK**. The Net-Net SBCs appear in the targeted devices table.
8. Click **Apply**.

Procedural Steps for Work Orders

Each type of work order contains a predefined work flow that defines the execution procedure sequentially in a step-by-step process. As the work order goes through the execution process, the Work Order Administration window displays which step it is at in this process. The steps are found in the Device tasks table, under the Progress column. The steps for each type of work-order scenario are defined in the tables below.

Note: The rollback procedural steps listed below are based on the full rollback procedures when rolling back a successfully-executed device task. The rollback procedural steps may vary if the rollback process is initiated when a work order fails or is aborted during the execution process.

| Device tasks | | | | | | | |
|--------------|---------------|-------------------|---------|----------|---------------------|---------------------|--|
| Name | IP address | Original SW image | Status | Progress | Start time | End time | |
| sd180 | 172.30.80.180 | SC6.1.0 | Success | 12/12 | 2010-06-02 11:47:48 | 2010-06-02 11:51:36 | |
| sd181 | 172.30.80.181 | SC6.1.0 | Success | 12/12 | 2010-06-02 11:52:22 | 2010-06-02 12:03:47 | |

Software Upgrade for a Standalone Device

This table defines the procedural steps for a software upgrade involving a standalone device.

| Step | Description |
|------|--|
| 1 | Checks available space for the device. |
| 2 | Archives the current device software image. |
| 3 | Pushes the software image to the device. |
| 4 | Edits the image name in the boot parameters. |
| 5 | Performs call shedding. |
| 6 | Reboots the device. |
| 7 | RedisCOVERS the device. |

Software Upgrade for an HA Pair

This table defines the procedural steps for a software upgrade involving an HA pair.

| Step | Description |
|------|---|
| 1 | Checks available space for both devices. |
| 2 | Checks status and health for both devices. |
| 3 | Archives the current device software image. |
| 4 | Pushes the software image to both devices. |
| 5 | Edits the image name in the boot parameters for the standby device. |
| 6 | Reboots the standby device. |
| 7 | Performs call shedding. |
| 8 | Checks the health of the standby device. |
| 9 | Forces a failover if the standby device becomes the active device. |
| 10 | Edits the image name in the boot parameters for the new standby device. |

| Step | Description |
|-------------|---------------------------------|
| 11 | Reboots the new standby device. |
| 12 | RedisCOVERS the devices. |

Global Parameter Changes for a Standalone Device or an HA Pair

This table defines the procedural steps for global parameter changes involving a standalone device or an HA pair.

| Step | Description |
|-------------|---|
| 1 | Copies the inactive configuration for backup. |
| 2 | Checks the status of the device. |
| 3 | Retrieves the running configuration data file. |
| 4 | Updates the inactive configuration. |
| 5 | Saves and activates the inactive configuration. |

Software Upgrade and Global Parameter Changes for a Standalone Device

This table defines the procedural steps for a software upgrade followed by global parameter changes involving a standalone device.

| Step | Description |
|-------------|--|
| 1 | Checks available space for the device. |
| 2 | Archives the current device software image. |
| 3 | Pushes the software image to the device. |
| 4 | Edits the image name in the boot parameters. |
| 5 | Performs call shedding. |
| 6 | Reboots the device. |
| 7 | RedisCOVERS the device. |
| 8 | Makes a copy of the inactive configuration for backup. |
| 9 | Checks the status of the device. |
| 10 | Retrieves the running configuration data file. |
| 11 | Updates the inactive configuration. |
| 12 | Saves and activates the inactive configuration. |

Software Upgrade and Global Parameter Changes for an HA Pair

This table defines the procedural steps for a software upgrade followed by global parameter changes involving an HA pair.

| Step | Description |
|-------------|--|
| 1 | Checks available space for both devices. |
| 2 | Checks status and health score for both devices. |
| 3 | Archives the current device software image. |
| 4 | Pushes the software image to both devices. |

| Step | Description |
|-------------|---|
| 5 | Edits the image name in the boot parameters for the standby device. |
| 6 | Reboots the standby device. |
| 7 | Performs call shedding. |
| 8 | Checks the health of the standby device. |
| 9 | Forces a failover if standby becomes active. |
| 10 | Edits the image name in the boot parameters for the new standby device. |
| 11 | Reboots the new standby device. |
| 12 | RedisCOVERS the devices. |
| 13 | Makes a copy of the inactive configuration for backup. |
| 14 | Checks the status of the device. |
| 15 | Retrieves the running configuration data file. |
| 16 | Updates the inactive configuration. |
| 17 | Saves and activates the inactive configuration. |

Software Rollback for a Standalone Device

This table defines the procedural steps for a software rollback involving a standalone device.

| Step | Description |
|-------------|--|
| 1 | Pushes files to the device. |
| 2 | Edits the image name in the boot parameters. |
| 3 | Reboots the device. |
| 4 | RedisCOVERS the device. |

Software Rollback for an HA Pair

This table defines the procedural steps for a software rollback involving an HA pair.

| Step | Description |
|-------------|--|
| 1 | Pushes the files to both devices. |
| 2 | Retrieves status and health score from both devices. |
| 3 | Edits the image name in the boot parameters from the standby device. |
| 4 | Reboots the standby device. |
| 5 | Performs call shedding. |
| 6 | Performs switchover to standby device. |
| 7 | Edits the image name in the boot parameters from the standby device. |
| 8 | Reboots the new standby device. |
| 9 | RedisCOVERS the device. |

Global Parameter Changes Rollback for a Standalone Device or an HA Pair

This table defines the procedural steps for a rollback of global parameter changes involving a standalone device or an HA pair.

| Step | Description |
|-------------|---|
| 1 | Pushes the original running configuration back to the device. |
| 2 | Restores the backup configuration on the device. |
| 3 | Saves and activates the configuration on the device. |
| 4 | Restores the inactive configuration. |

Global Parameter Changes and Software Rollback for a Standalone Device

This table defines the procedural steps for global parameters rollback followed by a rollback of the software version involving a standalone device.

| Step | Description |
|-------------|---|
| 1 | Pushes the original running configuration back to the device. |
| 2 | Restores the backup configuration on the device. |
| 3 | Saves and activates the configuration on the device. |
| 4 | Restores the inactive configuration. |
| 5 | Pushes files to the device. |
| 6 | Edits the image name in the boot parameters. |
| 7 | Reboots the device. |
| 8 | RedisCOVERS the device. |

Global Parameter Changes and Software Rollback for an HA Pair

This table defines the procedural steps for global parameters rollback followed by a rollback of the software version involving an HA pair.

| Step | Description |
|-------------|--|
| 1 | Pushes the original running configuration back to the device. |
| 2 | Restores the backup configuration on the device. |
| 3 | Saves and activates the configuration on the device. |
| 4 | Restores the inactive configuration. |
| 5 | Pushes the files to both devices. |
| 6 | Retrieves status and health score from both devices. |
| 7 | Edits the image name in the boot parameters from the standby device. |
| 8 | Reboots the standby device. |
| 9 | Performs call shedding. |
| 10 | Performs switchover to standby device. |
| 11 | Edits the image name in the boot parameters from the standby device. |
| 12 | Reboots the new standby device. |
| 13 | RedisCOVERS the device. |

Universal Procedure for Executing a Work Order on Demand

The following procedure is universal to all work order types and must be performed to execute your work order (unless you have scheduled a start date and time for your work order to begin processing).

Work Order Execution

You can execute your work order on demand, or you can schedule a date and time for your work order to execute. Refer to "Scheduling Work Order Start Date and Time" on page 138 for details about scheduling a work order date and time.

A work order is considered "running" when it is in one of the following states:

- running
- pausing
- resuming
- start committing
- committing
- start aborting
- aborting

Active Device Tasks Within a Running Work Order

A device task is an individual operation performed on the targeted device(s) and runs sequentially in the work order. An active device task is a device task in one of the following states:

- starting
- running
- pausing
- start aborting
- aborting

Executing a Work Order on Demand

To execute your work order on demand:

1. Click the Work Orders tab from the Work Order Administration window of your work order.

- Click the work order you want to execute in the Work orders table. The device tasks associated with this work order appear in the Device tasks table below the Work orders table.

The screenshot shows the 'Work Order Administration' window. At the top, there are tabs for 'Work Orders' and 'Software Image Archive Management'. Below the tabs, the 'Work orders' section displays a table with one row:

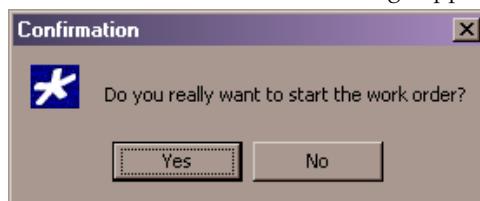
| Name | Type | Device count | Target SW version | Status | Start time | End time |
|--------------------|-----------------------|--------------|-------------------|--------------|------------|----------|
| SW_GlobalParam-BOS | SW Upgrade+GP Changes | 2 | nnSC610m4p4.gz | NotScheduled | | |

Below the table is a row of buttons: Logs, Refresh, Create, Pause, Start, View, Edit, Abort, Commit, Copy, and Delete. The 'Device tasks' section shows a table with two rows:

| Name | IP address | Original SW image | Status | Progress | Start time | End time |
|-------|---------------|-------------------|--------|----------|------------|----------|
| sd180 | 172.30.80.180 | C6.0.0 | Ready | 0/12 | | |
| sd181 | 172.30.80.181 | C6.0.0 | Ready | 0/12 | | |

At the bottom of the window are additional buttons: Logs, Refresh, Pause, Resume, Abort, and Submit.

- Click **Start**. A confirmation message appears.



- Click **Yes**.
- Click **Refresh** to confirm the Status changes from Not started to Running.

The screenshot shows the 'Work Order Administration' window again. The 'Work orders' table now shows the work order has started:

| Name | Type | Device count | Target SW version | Status | Start time |
|--------------------|-----------------------|--------------|-------------------|---------|---------------------|
| SW_GlobalParam-BOS | SW Upgrade+GP Changes | 2 | nnSC610m4p4.gz | Running | 2010-06-02 10:39:00 |

Universal Procedure for Committing a Work Order

After you execute a work order, it must be committed in order to unlock the targeted devices associated with it. Only work orders with a status of Success, Failed, Aborted, AbortFailed, or CommitFailed can be committed. When you commit a work order rollback is no longer possible, and all targeted devices associated with this work order are unlocked and can be assigned to another work order, or can be copied for other configuration.

You can automatically commit your work order. By enabling the **Auto commit** parameter, the work order is automatically committed after a successful execution. The default is **disabled**. When disabled, you must manually commit the work order. Refer to "Enabling Auto Commit" on page 140 for more information about **Auto commit**.

Until you commit, you have the opportunity to abort this work order and perform a rollback to restore the original software version and/or original configuration settings.

Manually Committing a Work Order

To manually commit a work order:

1. From the Work Order Administration window, click the Work orders tab.
2. Click the work order you want to commit and click **Commit**. A confirmation dialog box appears.



3. Click Yes.
4. Click Refresh to confirm the work order status changed from Success to Committed.

| Work Order Administration | | | | | | |
|---------------------------|-----------------------|-----------------------------------|-------------------|-----------|---------------------|---------------------|
| Work Orders | | Software Image Archive Management | | | | |
| Work orders | | | | | | |
| Name | Type | Device count | Target SW version | Status | Start time | End time |
| SW_GlobalParam-BOS-c2 | SW Upgrade+GP Changes | 2 | nnSC610m5.xz | Committed | 2010-06-02 11:52:22 | 2010-06-02 12:19:09 |

Performing Global Parameter Changes

The following procedures show you how to create a work order to perform global parameter changes across a group of targeted devices.

Before you create your global parameter changes work order, you must create a global configuration group. The global configuration group is similar to a domain and stores the global configurations you create in conjunction with your work orders. All global configurations must belong to a global configuration group. You can create multiple global configuration groups, each containing global configurations for various hardware platforms and software versions. The global configuration icons are gray, whereas the Net-Net EMS domain icons are blue.



In the following configuration example, we will create a work order to perform global parameter changes on one targeted device. Since we are performing global parameter changes, the first step in the process is to create a global configuration group.

Creating a Global Configuration Group

To create a global configuration group:

1. In the Net-Net EMS navigation tree, right click the Inactive configurations folder. A pop-up menu appears.
2. Click Create Global Config Group.



The Create new global configuration group dialog box appears.

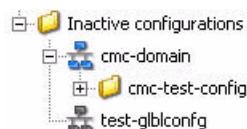
3. **Global configuration group name**—Enter the name you want to give to this global configuration group.



4. Click **Apply**. A dialog box appears indicating the group was successfully added.



5. Click **OK**. The new global configuration group is added to the Net-Net EMS navigation tree beneath Inactive configurations, represented by a gray icon.



Creating a Global Configuration

When performing global parameter changes, you must create a global configuration, which becomes part of your work order. The global configuration is a Net-Net SBC configuration that is a general purpose container for holding your configuration changes. It is not tied to a specific device the way that normal inactive configurations are.

You create and/or modify the global configuration with the parameter changes you want applied to your targeted devices. Once the global configuration is assigned to your work order, the configuration attributes within are sent to the targeted devices once the work order is executed.

There two ways to create a global configuration:

1. You can use an existing Net-Net SBC to seed your global configuration. In this instance, the parameter values are copied from this Net-Net SBC.
2. You can create a default global configuration that is effectively empty.

Although a global configuration created from an existing Net-Net SBC may have many parameters configured, only those parameters you add or modify are applied to your targeted devices. For example, if I make a copy of Net-Net SBC 4000A, and I modify two realms and add a session agent, my targeted devices will be updated with the two revised realms and the new session agent only.

A global configuration can be modified, or deleted, when it is not yet referenced by a work order. Once the global configuration becomes a part of a work order, it cannot be changed or deleted.

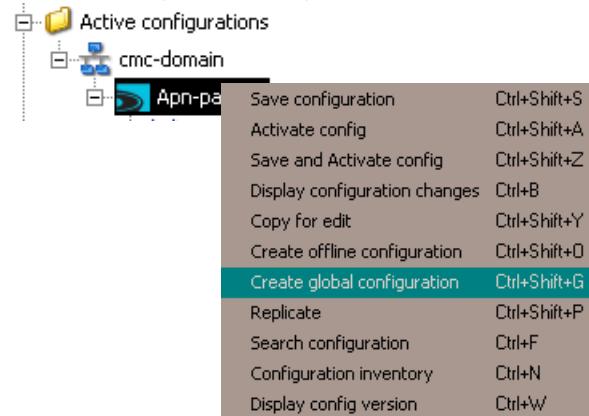
Creating a Global Configuration from an Existing Net-Net SBC

You can create a global configuration by copying an existing Net-Net SBC. Your copy will contain all of the configuration values of the Net-Net SBC you copied.

To create a global configuration from an existing Net-Net SBC configuration:

Note: Before you create a global configuration, you must first create your global configuration group. Refer to "Creating a Global Configuration Group" on page 149 for more information.

1. In the Net-Net EMS navigation tree, right click the Net-Net SBC in Active configurations from which you want to copy data. A pop-up menu appears.
2. Click **Create global configuration**.



The Create global configuration dialog box appears.

3. **Configuration name**—Enter the name you want to give to this global configuration. The name must be an alphanumeric value from 1 to 24 characters in length.



4. **Global configuration group**—Click the global configuration group this global configuration will be part of in the drop down list.



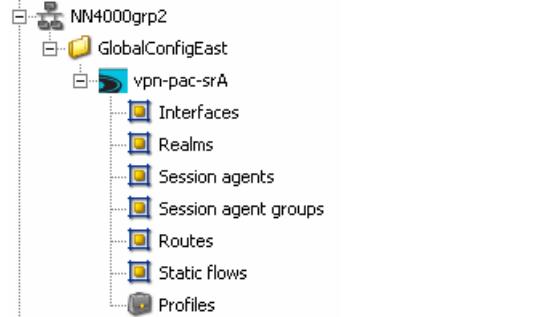
5. Click **OK**. Your request is sent to the server.
6. Click **OK** to close the Create global configuration request dialog box.



7. Click **OK** to close the Copy for edit status dialog box.



Your global configuration is found under the global configuration group.



Creating a Global Configuration Using Net-Net SBC Default Values

You can create a global configuration by using Net-Net SBC default parameter values. This Net-Net SBC does not contain additional customized configurations.

Note: Before you create a global configuration, you must first create your global configuration group. Refer to "Creating a Global Configuration Group" on page 149 for more information.

To create a global configuration using default Net-Net SBC parameter values:

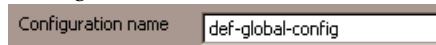
1. In the Net-Net EMS navigation tree, right click the Net-Net SBC global configuration group where you want to assign this global configuration. A pop-up menu appears.

2. Click Create default global configuration.

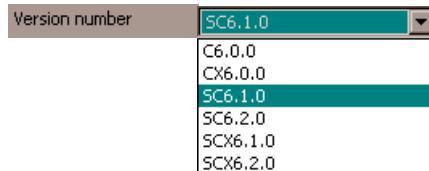


The Create default global SD configuration dialog box appears.

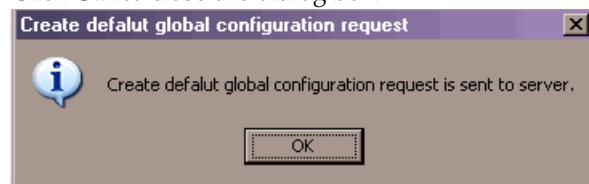
3. **Configuration name**—Enter the name you want to give this default global configuration. The name must be an alphanumeric value from 1 to 24 characters in length.



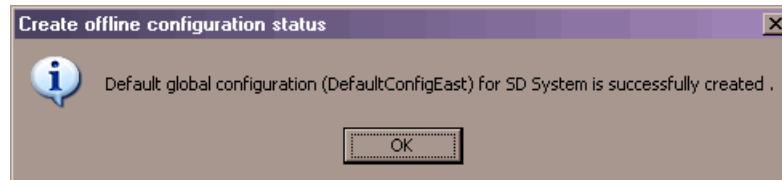
4. Version—Click the software version of the Net-Net SBC you want to use for your default global configuration in the drop down list. The software version you select is the software version you are upgrading to, if performing a software upgrade. Otherwise, it is the software version of the currently-running device.



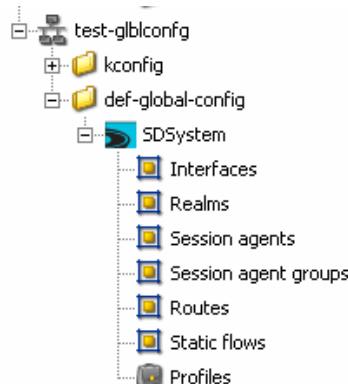
5. Click OK. Your request is sent to the server.
6. Click OK to close the dialog box.



7. Click OK to close the dialog box.



Your default global configuration is found under the global configuration group.



Modifying your Global Configuration

Once you have created your default global configuration or your global configuration from an existing Net-Net SBC, you can make your configuration changes that you want to apply to your targeted Net-Net SBCs.

If you choose a default global configuration, you will have to add all desired configuration elements since the configuration is empty. In addition, parameters within the created configuration elements will be set to their default values unless you modify them.

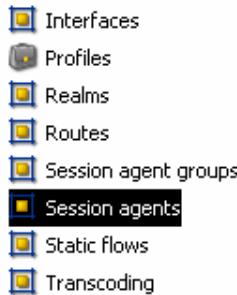
If you choose to work with a global configuration copied from an existing Net-Net SBC, you can modify the parameters within this configuration.

In the example below, we will add a new session agent called sa-burlington. We will add a textual description for this session agent and change the IP port.

Creating a Session Agent Example

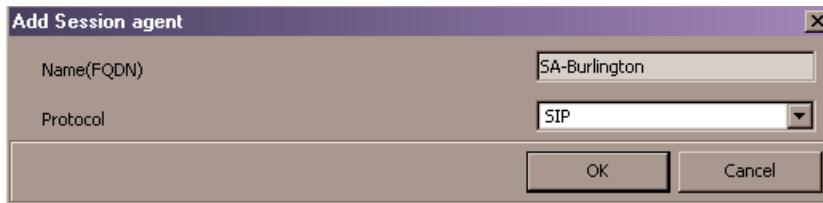
To create a new session agent:

1. Click Session agent in the Net-Net EMS navigation tree.



The Session agent window appears in the display pane.

2. Click **Add**. The Add session agent dialog box appears.
3. **Name(FQDN)**—Enter the name you want to apply to this session agent.
4. **Protocol**—Click the protocol you want to apply to this session agent. You can choose from SIP or H.323.



5. Click **OK**. The Edit session agent window appears.
6. **Description**—Enter a description to identify this session agent.
7. **IP Port**—Enter the IP port you want for this session agent.
8. Click **Apply**.

Note: All parameter values other than Name(FQDN), Protocol, Description, and IP port will be set to their default values.

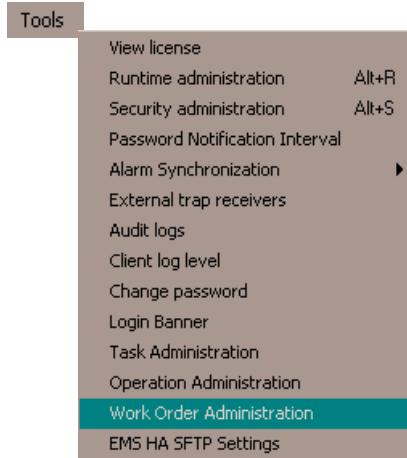
Once you make all of your configuration changes in your global configuration, you create your work order. The changes made in your global configuration are applied to your work order when you associate the global configuration to your work order in the next section.

Creating a Global Parameter Changes Work Order

You create your work order after creating your global configuration group and your global configuration. The modifications you made to your global configuration are assigned to your work order and are applied to the targeted devices you assign to the work order.

To create a global parameter changes work order:

1. Click the Tools menu in the top menu bar and click Work Order Administration.

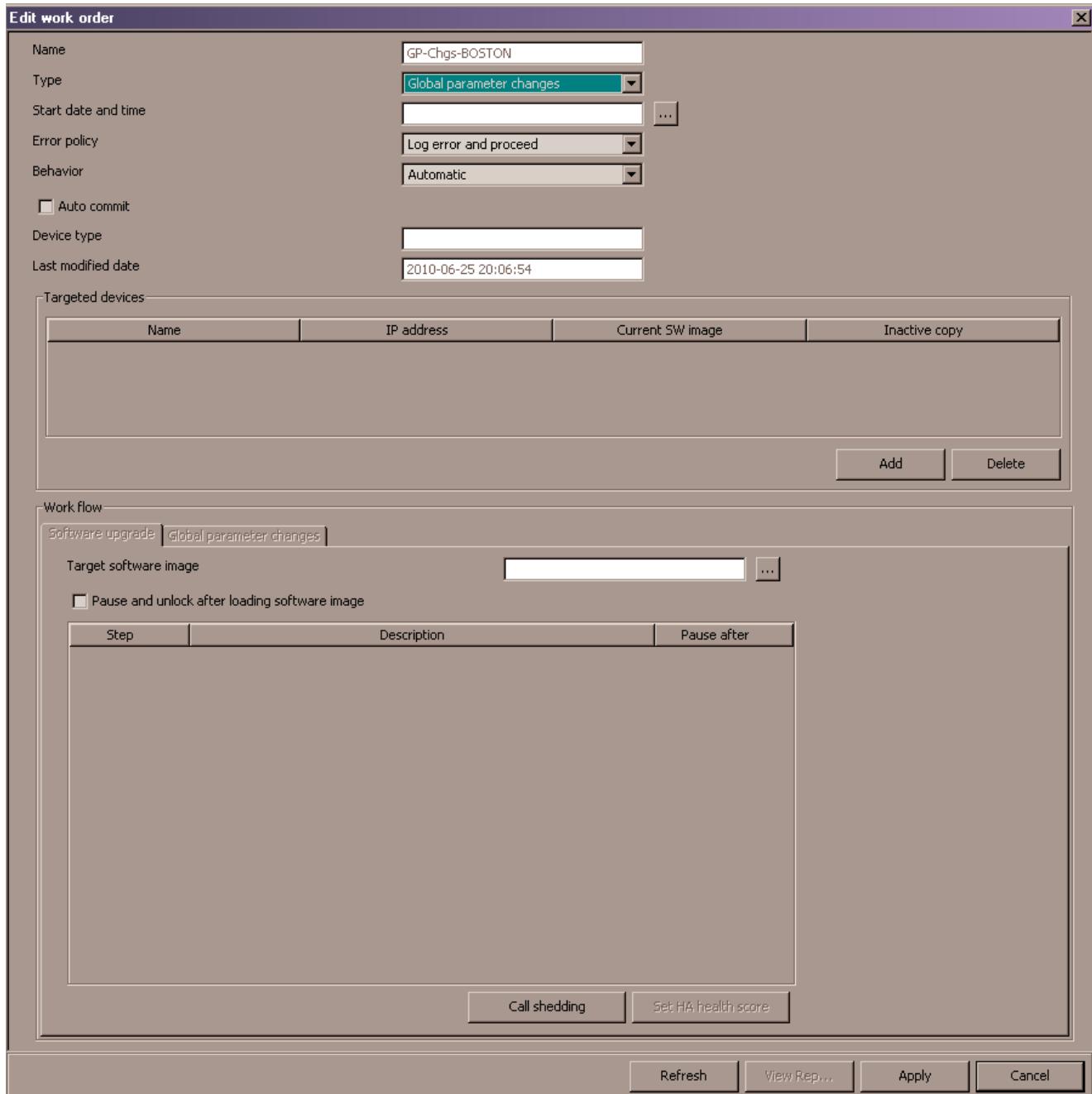


The Work Order Administration window appears.

2. Click the Work Orders tab.
3. Click Create. The Create work order dialog box appears.
4. **Work order name**—Enter the descriptive name you want to give this work order. The name must be an alphanumeric value from 1 to 24 characters in length.



5. Click OK. The Edit work order window appears with the name you assigned to this work order in the Name field.



6. Type—Click Global parameter changes in the drop down list.



Configuring Universal Parameters

To configure the universal parameters for your global parameter changes work order:

- Refer to "Configuring Universal Parameters" on page 138 to configure the universal set of parameters for this software upgrade work order.

Modifying Global Configuration

To modify the global configuration:

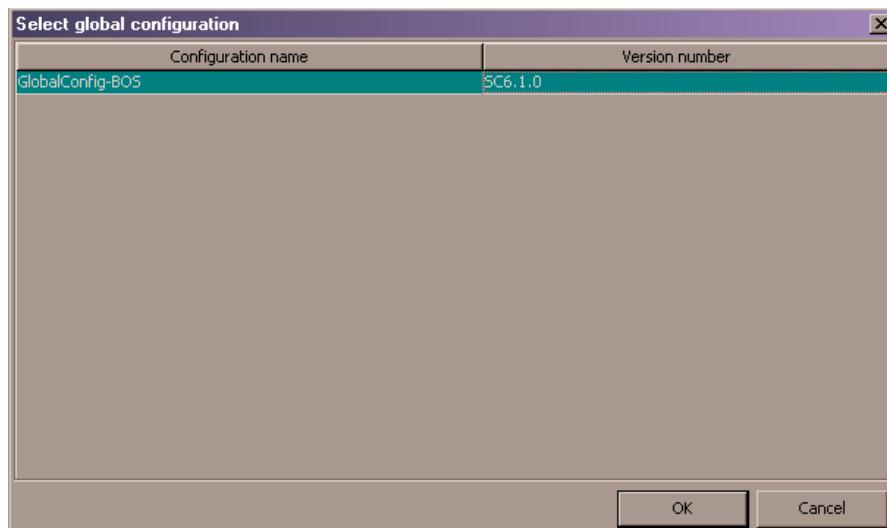
- Refer to "Modifying your Global Configuration" on page 153 for instructions on modifying your global configuration.

Assigning the Global Configuration to the Work Order

Once you have created and modified your global configuration, you assign the global configuration in your work order.

To assign the global configuration in the work order:

- From the Edit work order window, scroll to Work flow and click the Global parameter changes tab.
- Global configuration**—Click  to select your global configuration. The Select global configuration dialog box appears.
- Click the global configuration you want to assign to this work order and click OK.



The **Global configuration** parameter populates with the global configuration and the **Version number** parameter populates with the software version for this global configuration.



- Click **Apply**. An update successfully message appears after your work order is updated.



- Click **OK**. The Work Order Administration window appears.

From here you set the criteria for multiple-instance elements that you want to change when you execute your work order.

Setting Criteria for Element Instances in Work Orders

You have to set the criteria for the multiple-instance elements you modified in your work order. Since some configuration elements occur more than once, you use the **Set Criteria** parameter to indicate which multiple-instance elements you want the changes applied to when you execute your work order.

Setting criteria means selecting which instances of a configuration record type the modifications should be applied to on your targeted devices. For example, if you modify a parameter for a session agent, you set the criteria to indicate which session agents within this targeted device you want to modify when your work order is executed.

By enabling the **Apply changes to all instances** parameter, you can set the criteria for all instances of a multiple element at once.

Note: **Set Criteria** is disabled for all parameters pertaining to Access Control, Local Policy, and Static Flow. For those configuration elements, only changes exactly as specified by instance in the global configuration are supported.

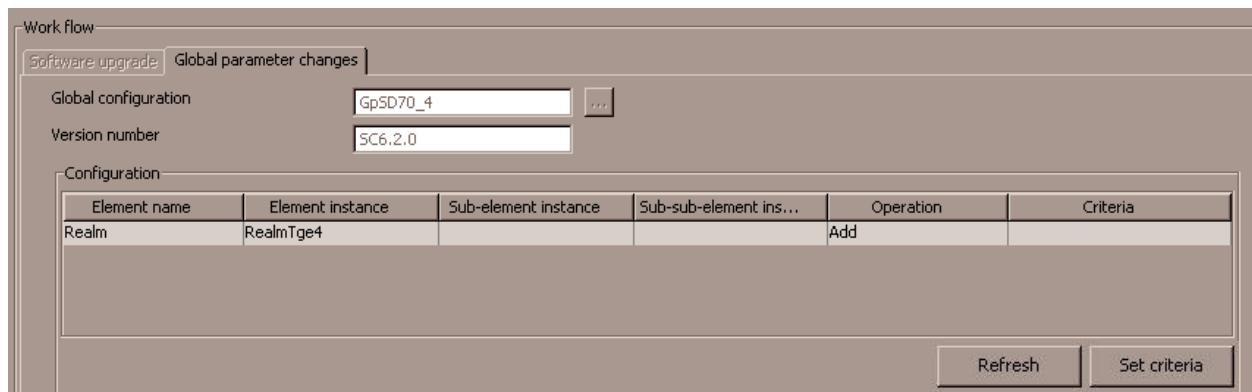
The criteria syntax you enter must follow one of these rules:

- Exactly match the specified instance. The instance is specified by using whatever “key” attribute values are appropriate for that type of configuration element. For example, in the case of a session agent the key is “hostname”.
- Match any one of the specified multiple instances: The input string can have multiple instances separated by a semicolon (;), for example, 1.1.1.1;12.12.12.12;jk.acmepacket.com.

Set criteria is **disabled** for system-wide elements since there is only one instance for a system-wide element and no criteria is needed.

To set the criteria for an element in the work flow configuration:

1. From the Edit work order window, scroll to Work flow.
2. Click the Global parameter changes tab.
3. Click the Element name you want to set criteria for in the Configuration table.



4. Click **Set criteria**. The Set criteria dialog box appears.

- Click **Add**. The Add criteria dialog box appears. (For this example, the primary key is "ID". The Add criteria text field references Realm:id.) The element instance is dynamic and changes depending on the type of element instance you are setting criteria for.

Note: The Add criteria dialog box will automatically prompt you for all attributes that make up the primary key for the selected type of configuration element.

- Enter the specific criteria needed. In this example, a realm ID is added.

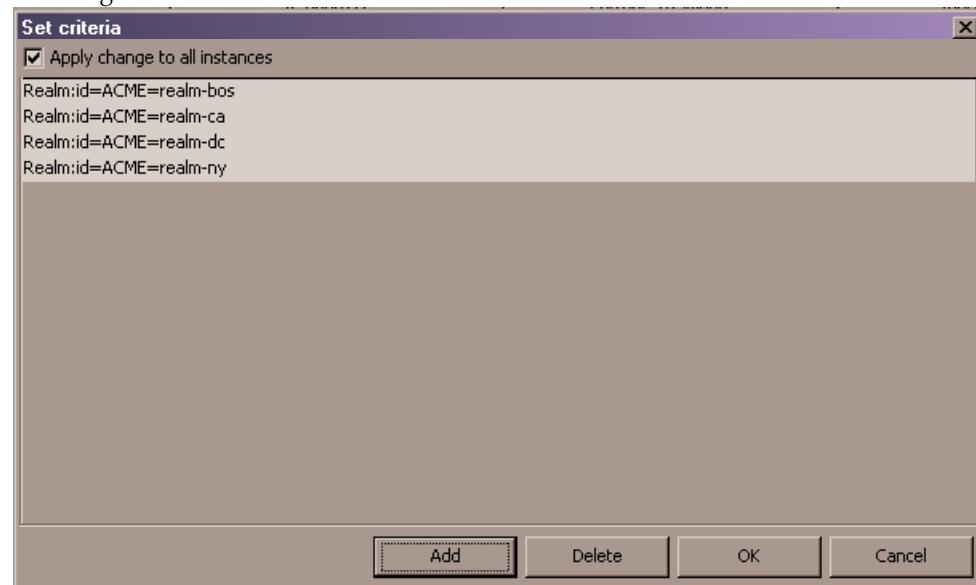


Note: You must know which values are considered valid for the particular attribute you are setting criteria for.

- Click OK. The criteria is added to the Set criteria table.
- Apply changes to all instance**—Click the checkbox to apply the criteria to all instances of this multiple element.



Note: There is some extra information in the string (=ACME). It can be ignored.



- Click OK. The criteria is added to the Criteria column of the Configuration table.

10. To set multiple criteria instances, repeat steps 5 through 9.

The screenshot shows the 'Global parameter changes' tab selected in a 'Work flow' interface. At the top, there are fields for 'Global configuration' (set to 'k-config') and 'Version number' (set to 'SC6.1.0'). Below this is a 'Configuration' table:

| Element name | Element instance | Sub-element inst... | Sub-sub-element... | Operation | Criteria |
|----------------|------------------|---------------------|--------------------|-----------|-------------------------|
| LocalPolicy | LocalPolicy | | | Modify | |
| LocalPolicy | LocalPolicy | | | Modify | |
| SessionAgent | ses-agent1 | | | Add | |
| QosConstraints | k-constraint | | | Add | |
| Realm | home | | | Modify | Realm:id=ACME=realm-... |

At the bottom right are buttons for 'View crit...', 'Refresh', and 'Apply' (which is currently disabled).

11. Click **Apply**. Your work order is updated successfully.



If you click **Apply** when you have not set the criteria instances you will get an error message.



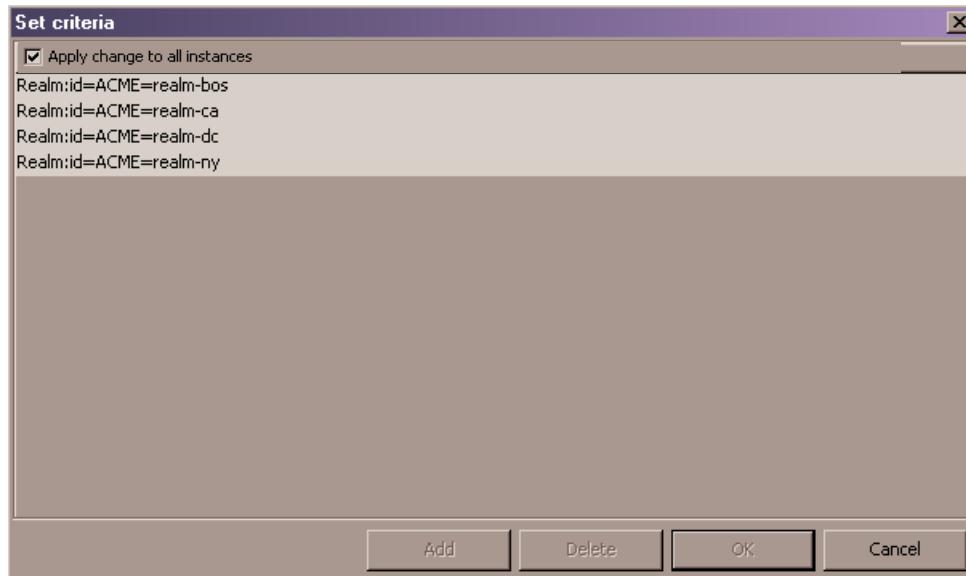
12. Click **OK** to clear the message.

Viewing Set Criteria Details

To view set criteria:

1. From the Edit work order window, click the element you want to view in the Configuration table.
2. Click **View criteria** beneath the configuration table. The criteria for the element you selected appears in the Set criteria window.

Note: There is some extra information in the string (=ACME). It can be ignored.



Apply Configuration Changes

Once you complete the mandatory and optional steps for creating your work order, you ready to apply your configuration changes made in your work order.

To apply the configuration to your work order:

- From the Edit work order window, click **Apply**.

A success message dialog box appears when you have successfully configured your work order.



- Click **OK**. Your work order status changes to NotScheduled.

Executing Work Order

Once your work order is created and your configuration applied, you are ready to execute your work order. You perform this step if you are manually executing your work order. Otherwise, your work order will execute at the date and time you set.

To manually execute your work order:

- Refer to "Executing a Work Order on Demand" on page 146 for more information to perform this procedure.

Committing Work Order

Once your work order is executed, you must commit your work order to unlock all targeted devices associated with your work order.

To commit your work order and unlock all targeted devices associated with your work order:

1. Refer to "Universal Procedure for Committing a Work Order" on page 148 for information to perform this procedure.

Performing a Software Upgrade and Global Parameter Changes

To perform a software upgrade and global parameter changes, you perform a combination of the previous procedures.

Creating Global Configuration Group

To create a global configuration group:

1. Refer to "Creating a Global Configuration Group" on page 149 for instructions on creating your global configuration group.

Creating Global Configuration

You can create a global configuration by copying an existing Net-Net SBC. Your copy will contain all of the configuration values of the Net-Net SBC you copied. Or, you can create a global configuration by using Net-Net SBC default parameter values. This Net-Net SBC does not contain additional customized configurations.

From an Existing Net-Net SBC

To create a global configuration from an existing Net-Net SBC:

1. Refer to "Creating a Global Configuration from an Existing Net-Net SBC" on page 150 for instructions about creating your global configuration from an existing Net-Net SBC.

Using Net-Net SBC Default Values

To create a global configuration using default Net-Net SBC parameter values:

1. Refer to "Creating a Global Configuration Using Net-Net SBC Default Values" on page 151 for instructions on creating a global configuration using Net-Net SBC default values.

Creating the Work Order

You create your work order after creating your global configuration group and your global configuration. The modifications you made to your global configuration are linked to your work order and are applied to the targeted devices you assign to the work order. First, you can configure the universal parameters portion of your work order.

Configuring Universal Parameters

To configure the universal parameters for your work order:

1. Refer to "Configuring Universal Parameters" on page 138 for instructions on configuring the universal parameters for your work order.

Configuring Software Upgrade Portion

To create the software upgrade portion of your work order:

1. Refer to "Creating a Software Upgrade Work Order" on page 132 for instructions on creating the software upgrade portion of your work order.

Configuring Target Software Image

To configure the target software image:

1. Refer to "Configuring Target Software Image for Software Upgrades" on page 134 for instructions on configuring the target software image for this work order.

Configuring Optional Upgrade Parameters**To configure optional software upgrade parameters:**

1. Refer to "Configuring Optional Software Upgrade Parameters" on page 134 for instructions on configuring the following optional parameters:
 - Pause and unlock after loading software image.
 - Optional break points.
 - Optional call shedding.

Configuring Global Parameter Changes Portion**To create the global parameter changes portion of your work order:**

1. Refer to "Creating a Global Parameter Changes Work Order" on page 154 for instructions on creating the global parameter changes portion of your work order.

Assigning Global Configuration to the Work Order**To assign the global configuration in the work order:**

1. Refer to "Assigning the Global Configuration to the Work Order" on page 156 for instructions on assigning the global configuration to your work order.

Modifying Global Configuration**To modify your global configuration:**

1. Refer to "Modifying your Global Configuration" on page 153 for instructions on modifying your global configuration to suit your needs for this work order.

Setting Criteria for Element Instances

You have to set the criteria for the multiple-instance elements you modified in your work order. Since some configuration elements occur more than once, you use the **Set Criteria** parameter to indicate which multiple-instance elements you want the changes applied to when you execute your work order.

To set the criteria for multiple-instance elements:

1. Refer to "Setting Criteria for Element Instances in Work Orders" on page 157 for instructions on setting criteria for multiple-instance elements.

Viewing Criteria Details**To view details of the criteria you set:**

1. Refer to "Viewing Set Criteria Details" on page 159 for instructions on viewing criteria set for multiple-instance elements.

Applying Configuration Changes

Once you complete the mandatory and optional steps above you are ready to apply your configuration changes made in your work order.

To apply the configuration to your work order:

1. Refer to "Apply Configuration Changes" on page 160 for instructions on applying the configuration changes you made to your work order.

Resuming the Work Order After the Software Upgrade

The work order pauses after the software upgrade for each targeted device. At this point, you must resume the work order in order to begin the global parameter changes portion of the work order.

To resume a paused work order following the software upgrade to a targeted device:

1. Refer to "Resuming a Paused Work Order" on page 165 for instructions on resuming a paused work order.

Executing your Work Order

Once you apply your changes to your work order, you are ready to execute. You perform this step if you are manually executing your work order. Otherwise, your work order will execute at the date and time you set.

To manually execute your work order:

1. Refer to "Executing a Work Order on Demand" on page 146 for instructions on manually executing your work order.

Committing your Work Order

Once your work order is executed, you must commit your work order to unlock all targeted devices associated with your work order.

To commit your work order and unlock all targeted devices associated with your work order:

1. Refer to "Universal Procedure for Committing a Work Order" on page 148 for information to perform this procedure.

Universal Pausing, Copying, and Editing Copies of Work Orders

The following three sections contain procedures universal to all three types of work orders. You refer to these sections when you want to:

- Pause and resume a work order.
- Copy an existing work order.
- Edit a copy of an existing work order

About Pausing a Work Order

When performing a combined software upgrade and global parameter changes, once the software upgrade portion of the work order has successfully processed, the work order pauses. The work order Status and the device task Status is paused. You must resume the work order to execute the global parameter changes portion of the work order.

Work order in paused status:

| Work Order Administration | | | | | |
|---------------------------|-----------------------|-----------------------------------|-------------------|---------|---------------------|
| Work Orders | | Software Image Archive Management | | | |
| Work orders | | | | | |
| Name | Type | Device count | Target SW version | Status | Start time |
| SW_GlobalParam-BOS | SW Upgrade+GP Changes | 2 | nnSC610m4p4.gz | Aborted | 2010-06-02 11:08:01 |
| SW_GlobalParam-BOS-c | SW Upgrade+GP Changes | 2 | nnSC620p1.xz | Failed | 2010-06-02 11:45:28 |
| SW_GlobalParam-BOS-c2 | SW Upgrade+GP Changes | 2 | nnSC610m5.xz | Paused | 2010-06-02 11:52:22 |

Logs Refresh Create Pause Resume Report View Edit Abort Commit

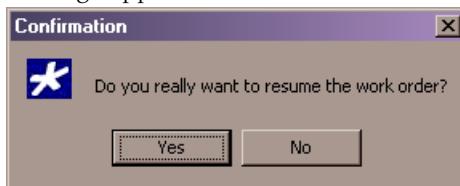
Device task in paused status:

| Device tasks | | | | | | | |
|--------------|---------------|--------------------|---------|----------|---------------------|---------------------|--|
| Name | IP address | Current SW version | Status | Progress | Start time | End time | |
| sd180 | 172.30.80.180 | SC6.1.0 | Success | 12/12 | 2010-06-02 11:47:48 | 2010-06-02 11:52:22 | |
| sd181 | 172.30.80.181 | SC6.1.0 | Paused | 7/12 | 2010-06-02 11:52:22 | 2010-06-02 11:52:22 | |

Resuming a Paused Work Order

To resume a paused work order:

1. From the Work Order Administration window, click the Work Orders tab.
2. Click the work order you want to resume and click **Resume**. A confirmation message appears.



3. Click **Yes**.
4. Click **Refresh** to confirm the status changed from paused to running.

A success status appears when the work order completes successfully.

Creating a Copy of an Existing Work Order

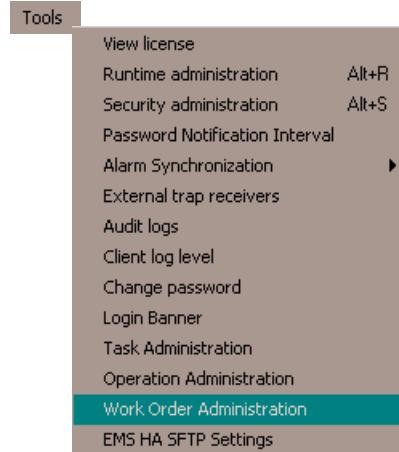
You can reuse an existing work order by making a copy of it and modifying it according to your new configuration needs. For example, if you want to apply the configuration changes in an existing work order called SW_GlobalParam-BOS, but you want to upgrade to a different software version, you can copy this work order and change the software version.

The targeted devices linked to the original work order are copied as well.

Note: You must make the necessary changes to the work order copy. The copy will not execute if it is exactly the same as the original work order. Changing the work order name is not considered a change. You must either change the software version or make at least one parameter change, or change the targeted device list.

To create a copy of an existing work order:

1. Click the Tools menu in the top menu bar and click Work Order Administration.



The Work Order Administration window appears.

2. Click the Work Orders tab.
3. Click the work order you want to copy in the Work orders table.
4. Click **Copy**. The Copy work order dialog box appears.
5. **Name of new work order**—Enter the name for this work order copy.



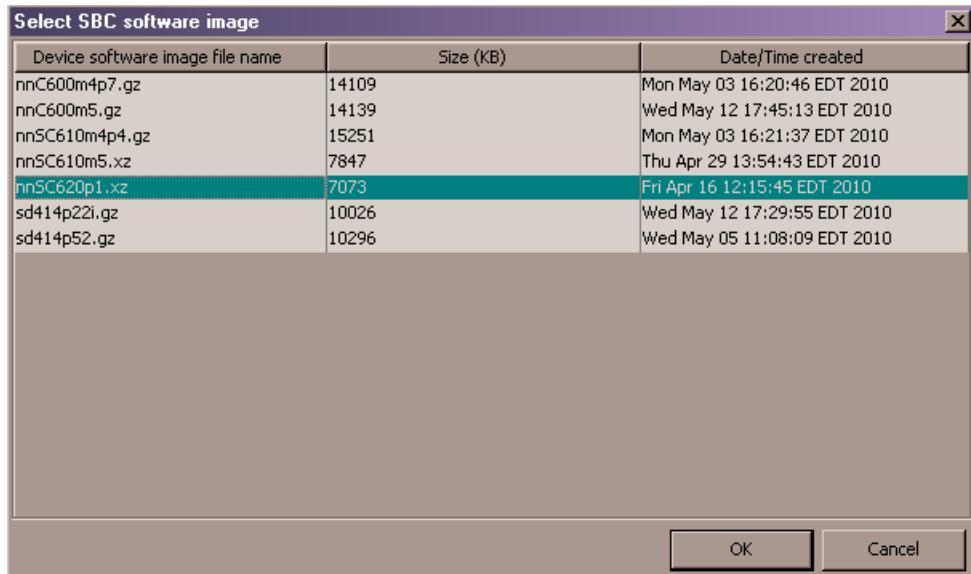
6. Click **OK**. The copy of the work order appears in the Work orders table in the Work Order Administration window. You are ready to edit this work order copy.

Editing a Copy of a Work Order

Once you make a copy of an existing work order, you can edit this copy for specific configuration needs.

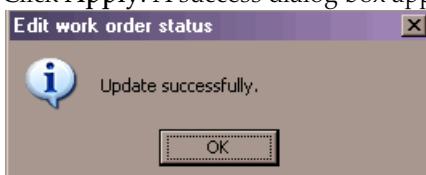
To edit a copy of a work order:

1. From the Work Order Administration window, click the Work Orders tab.
2. Click the copy of the work order you want to edit in the Work orders table and click **Edit**. The Edit work order window appears.
3. Make the changes you want to apply to this work order copy. For example, update the target software image by clicking  next to **Target software image**. The Select SBC software image dialog box appears.
4. Click the software image you want to apply and click **OK**.



The **Target software image** parameter is updated with the software version.

5. Click **Apply**. A success dialog box appears.



6. Click **OK**. Your work order copy is updated and you are ready to execute.

You must make at least one change to a work order copy or you will not be able to execute the work order. You will get the following error message:



7. Click **OK** to clear the message and modify the work order.

Global Configuration Modification Report

The global configuration modification report displays the global parameter changes scheduled for the targeted devices, and is based on the Net-Net SBC's inactive copy of the configuration. You can view the global configuration modification report from a work order table by clicking **Report**. This report allows you to preview the changes before the device tasks execute and the targeted devices are changed. You can make further adjustments in the work order configuration.

Note: For work orders that include both a software upgrade followed by global parameter changes, the report will generate after the software upgrade portion of the work order is completed.

View global parameter change work order report

| Devices | |
|---------|--------------|
| Name | IP address |
| sd70 | 172.30.80.70 |

Configuration modification

| Filter by element | | Parameters | | | |
|----------------------|------------------|----------------------|--------------------------|------------------|-----------|
| Name | Element instance | Sub-element instance | Sub-sub-element instance | Old value | New value |
| SDSystem->sysContact | N/A | N/A | N/A | TonyGPTTestSwGp2 | GP Tester |

Elements

| Name | Element instance | Sub-element instance | Sub-sub-element instance | Operation |
|--------------|------------------|----------------------|--------------------------|-----------|
| SessionAgent | tge-sa | N/A | N/A | Add |

About the Global Configuration Modification Data

The global configuration modification report is broken into three tables:

- Devices—Displays all targeted devices for this work order
- Parameters—Displays the old values and new values configured for this parameter
- Elements—Displays all newly-added and newly-deleted elements for this work order report

Device Table

When you select a device in the device table, the parameters table and the elements table automatically update to reflect the configuration changes for just that device. This is helpful for previewing the specific change(s) for any one device within your work order.

| Data | Description |
|------------|---|
| Name | Name of the targeted device, which can be a standalone device or an HA pair. |
| IP address | Net-Net SBC management IP address. For HA pairs, the IP addresses for each targeted device is listed. |

You can filter the data displayed in the Parameters and Elements tables with the **Filter by element** parameter. If you pick All in the drop down list the tables show all parameters and all elements for this work order. If you pick a specific element in the drop down list, you will get information pertaining to this element only.

Parameters Table

| Data | Description |
|--------------------------|---|
| Name | Net-Net EMS parameter name. |
| Element instance | String value of the key for a top-level element instance, for example, local policy. |
| Sub-element instance | String value of the key for a sub-element instance, for example, local policy attribute. |
| Sub-sub element instance | String value of the key for a sub-sub-element instance, for example, local policy media profiles. |
| Old value | Old parameter value configured for this parameter. |
| New value | New parameter value configured for this parameter. |

Elements Table

| Data | Description |
|----------------------|--|
| Name | Net-Net EMS element name. |
| Element instance | String value of the key for a top-level element instance, for example, local policy. |
| Sub-element instance | String value of the key for a sub-element instance, for example, local policy attribute. |

| Data | Description |
|--------------------------|---|
| Sub-sub element instance | String value of the key for a sub-sub-element instance, for example, local policy media profiles. |
| Operation | Operation performed on this element: <ul style="list-style-type: none">• Modify: Attributes in the element were changed in this global configuration.• Add: This element was added to this global configuration.• Delete: This element was deleted from this global configuration. |

Work Order Processing States and User Actions Matrices

Depending on the Net-Net EMS internal processing state of your work order, there are some actions you can perform during these states and some you cannot. The internal processing state is associated with the predefined process flow for each of the three work order types. The actions in the work order table and the device task table are dynamically enabled or disabled based on the state of the selected work order, or on a device task within the work order. The matrices below chart the various work order states and the actions you can or cannot perform when the work order is in a particular state. A warning dialog box will appear if you attempt an action that is not allowed during a state. Below are two matrices, one for work orders and one for device tasks.

Matrix for Work Order States and Actions

The matrix below details work order states and the actions you can perform during one of these states.

| States Below: | Action: Edit | Action: Delete | Action: Copy | Action: Commit | Action: Abort | Action: Start | Action: Restart | Action: Resume | Action: Pause |
|-----------------------------|--------------|----------------|--------------|----------------|---------------|---------------|-----------------|----------------|---------------|
| Partially-Configured | Yes | Yes | Yes | No | No | No | No | No | No |
| NotScheduled | Yes | Yes | Yes | No | No | Yes | No | No | No |
| Scheduled | No | No | Yes | No | Yes | Yes | No | No | No |
| WaitStarting | No | No | No | No | Yes | Yes | No | No | No |
| Running | No | No | No | No | Yes | No | No | No | Yes |
| Paused | No | No | No | No | Yes | No | No | Yes | No |
| Success | No | No | Yes | Yes | Yes | No | No | No | No |
| Failed | No | No | Yes | Yes | Yes | No | No | No | No |
| Committed | No | Yes | Yes | No | No | No | No | No | No |
| CommitFailed | No | No | Yes | Yes | No | No | No | No | No |
| Aborted | No | Yes | Yes | Yes | No | No | No | No | No |
| AbortFailed | No | No | Yes | Yes | Yes | No | No | No | No |
| PreloadPaused | No | No | No | No | Yes | No | No | Yes | No |
| Preloading | No | No | No | No | No | No | No | No | No |
| PreloadFailed | No | No | Yes | No | No | No | No | No | No |
| ResourceLocking | No | No | No | No | No | No | No | No | No |
| ResourceLockFailed | No | Yes | Yes | No | No | No | Yes | No | No |

Matrix for Device Task States and Actions

The matrix below details device task states and the actions you can perform during one of these states.

| States Below: | Action: Pause | Action: Resume | Action: Abort | Action: Submit | Action: Resubmit |
|-----------------------|------------------|-------------------|------------------|-------------------|---------------------|
| Ready | No | No | No | No | No |
| ResetToReady | No | No | No | No | Yes |
| Running | Yes | No | Yes | No | No |
| Paused | No | Yes | Yes | No | No |
| Success | No | No | Yes | No | No |
| Failed | No | No | Yes | No | No |
| Rolledback | No | No | No | No | Yes |
| RollbackFailed | No | No | Yes | No | No |
| PreloadPaused | No | Yes | Yes | No | No |
| Preloading | No | No | No | No | No |
| PreloadFailed | No | No | No | Yes | Yes |

Work Order Logs

You can view the work order log while the work order is running, or you can view the log for a particular targeted device in the work order. The log includes details for global parameter changes made, or software upgrades performed. The following operations are recorded in the logs:

- Global parameter changes, including addition, modification, and deletion.
- Software archive and software upgrade.
- Work order actions, including pause, start/resume, abort/rollback, and commit.
- Work order task actions, including pause, resume, abort/rollback, and resubmit.

To view work order log data, click Logs beneath the Work order table. A work order log appears.

The screenshot shows a window titled "WorkOrder logs for HAGPTest80". The main area contains a log of events:

```
[06/24/2010 10:55:41]:Process req:WorkOrderStart, user:admin, from:10.0.201.255.....
[06/24/2010 10:55:41]:Start the work order.
[06/24/2010 10:55:41]:Reserving all necessary resources by WO:HAGPTest80
[06/24/2010 10:55:41]:Reserving the active device - sd220_sd221
[06/24/2010 10:55:41]:Reserving the inactive configuration for device sd220_sd221
[06/24/2010 10:55:41]:Successfully reserved all necessary resources.
[06/24/2010 10:55:41]:gp updating for device task - sd220_sd221
[06/24/2010 10:56:57]:gp update return with Success
[06/24/2010 10:56:57]:End work order execution, now its state is: Success
[06/24/2010 10:57:33]:Process req:WorkOrderCommit, user:admin, from:10.0.201.255.....
[06/24/2010 10:57:33]:Commit the work order.
[06/24/2010 10:57:33]:Committing GP update for the device task - sd220_sd221
[06/24/2010 10:57:33]:GP update committed return with Success
[06/24/2010 10:57:33]:Releasing all reserved resources by WO:HAGPTest80
[06/24/2010 10:57:33]:Releasing the active device - sd220_sd221
[06/24/2010 10:57:34]:Releasing the inactive configuration for device sd220_sd221
[06/24/2010 10:57:34]:Released all reserved resources.
[06/24/2010 10:57:34]:End work order execution, now its state is: Committed
```

At the bottom of the window are three buttons: Refresh, Export, and Close.

With the three buttons at the bottom of the report you can:

- **Refresh**—Refreshes stale log data.
- **Export**—Exports the log data to a network file.
- **Close**—Closes the log.

To view log data for a device in this work order, click the device you want to view in the Device tasks table and click **Logs**. A work flow log appears for this device only.

The screenshot shows a window titled "Workflow logs for SW_GlobalParam-BOS_172.30.80.181". The window contains a large text area displaying log entries from a software upgrade process. The log entries are timestamped and show various steps such as cleaning working data, checking available space, pushing images via sftp, and performing rollbacks. The log ends with a successful rollback completion. At the bottom of the window, there are three buttons: "Refresh", "Export", and "Close".

```
SW Upgrade[06/02/2010 10:39:47]:Update workflow=000000456 target=172.30.80.181 starting at step 0 breakpo
SW Upgrade[06/02/2010 10:39:48]:Cleaning working data for workflow=000000456 target=172.30.80.181 isRollba
SW Upgrade[06/02/2010 10:39:48]:Checking available space at 172.30.80.181
SW Upgrade[06/02/2010 10:39:48]:SBC 172.30.80.181 does not support space available table
SW Upgrade[06/02/2010 10:39:48]:Exception: null
SW Upgrade[06/02/2010 10:39:48]:Archiving current image /opt/ACMEPacket/devices/softwareImages/nnC600m5.0
SW Upgrade[06/02/2010 10:39:48]:The rollback image already exists in the archive. No need to archive it
SW Upgrade[06/02/2010 10:39:48]:Pushing image nnSC610m4p4.gz to 172.30.80.181 using sftp
SW Upgrade[06/02/2010 10:39:49]:Pushing image to 172.30.80.181
SW Upgrade[06/02/2010 10:40:33]:Successfully pushed 172.30.80.181
SW Upgrade[06/02/2010 10:40:33]:File /boot/nnSC610m4p4.gz and file /opt/ACMEPacket/devices/softwareImage
SW Upgrade[06/02/2010 10:40:33]:Rolling back workflow=000000456 target=172.30.80.181
SW Upgrade[06/02/2010 10:40:33]:Cleaning working data for workflow=000000456 target=172.30.80.181 isRollba
SW Upgrade[06/02/2010 10:40:33]:Rollback for this device doesn't need to do anything
SW Upgrade[06/02/2010 10:40:33]:Rollback completed successfully
SW Upgrade[06/02/2010 10:46:10]:Cleaning working data for workflow=000000456 target=172.30.80.181 isRollba
SW Upgrade[06/02/2010 10:46:10]:Update workflow=000000456 target=172.30.80.181 starting at step 0 breakpo
SW Upgrade[06/02/2010 10:46:10]:Cleaning working data for workflow=000000456 target=172.30.80.181 isRollba
SW Upgrade[06/02/2010 10:46:10]:Checking available space at 172.30.80.181
SW Upgrade[06/02/2010 10:46:10]:SBC 172.30.80.181 does not support space available table
SW Upgrade[06/02/2010 10:46:11]:Exception: null
SW Upgrade[06/02/2010 10:46:11]:Archiving current image /opt/ACMEPacket/devices/softwareImages/nnC600m5.0
SW Upgrade[06/02/2010 10:46:11]:The rollback image already exists in the archive. No need to archive it
SW Upgrade[06/02/2010 10:46:11]:Pushing image nnSC610m4p4.gz to 172.30.80.181 using sftp
SW Upgrade[06/02/2010 10:46:11]:Pushing image to 172.30.80.181
```

Below is an example of a log for a failed global parameter changes work order and the subsequent rollback.

Workflow logs for dddd_172.30.80.151 X

Global Parameter Updates

```
Update for work order:dddd target:172.30.80.151. Started @ 06/17/2010 23:53:12
Cleaning working data for work order:dddd target:sd151 isRollBack flag:false
Copying inactive config for work order:dddd target:sd151. Started @ 06/17/2010 23:53:12
Copy inactive config successfull for sd151 @ 06/17/2010 23:53:14
Retrieving Node Status for work order:dddd target:sd151
Active IP is 172.30.80.151
Retrieving saved configuration for work order:dddd target:sd151 using sftp
Exception from SFTP: Session.connect: java.io.IOException: End of IO Stream Read
Update failed @ 06/17/2010 23:53:14
```

Global Parameter Rollback

```
Rolling back for work order:dddd target:172.30.80.151. Started @ 06/17/2010 23:53:14
Cleaning working data for work order:dddd target:sd151 isRollBack flag:true
Retrieving Node Status for work order:dddd target:sd151
Active IP is 172.30.80.151
Rollback action begining step:3
Restoring Inactive Copy at EMS work order:dddd target:sd151. Started @ 06/17/2010 23:53:14
Restoring Inactive copy successfull... @ 06/17/2010 23:53:15
Rollback completed successfully @ 06/17/2010 23:53:15
```

Refresh Export Close

Overview

This chapter explains how to view the audit log. The audit log provides information about the changes made to the copies of Net-Net SBCs using the Net-Net EMS. The audit log contains audit trails. Each audit trail contains information about an activity performed on the Net-Net SBC copy when using the Net-Net EMS. Audit trails enable you to view all operations that have been performed, the time they were performed, whether they were successful, and who performed them.

About the Information Logged

Information is logged for the following operations:

- Adding domains
- Discovering Net-Net SBCs
- Copying Net-Net SBCs for edit
- Creating an offline copy
- Creating Net-Net SBC HA pairs
- Creating Net-Net SBC HA pairs from offline configuration
- Creating standalone Net-Net SBCs from offline configuration
- Saving edits to a Net-Net SBC
- Deleting objects
- Rediscovering Net-Net SBCs
- Rebooting
- Switching HA pair roles
- Saving configurations
- Activating configurations
- Saving and activating configurations
- Rebooting and activating configurations

About the Audit Trail Information

Audit trails include the following information:

- User who performed the operation
- What operation was performed by the user
- When the operation was performed by the user
- Whether the operation performed by the user was successful or failed

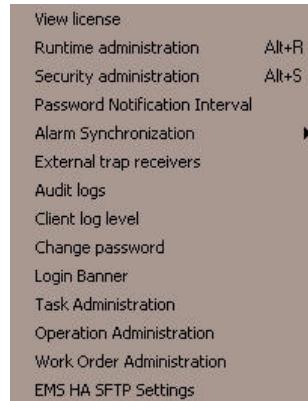
Viewing Audit Logs

This section explains how to view audit log's audit trail data. All users can access the Audit logs from the Tool menu, located in the Net-Net EMS toolbar. If you have the appropriate privileges, you can also access audit trail information from the Security Administration window. See *Security Administration* for details.

Accessing Audit Logs

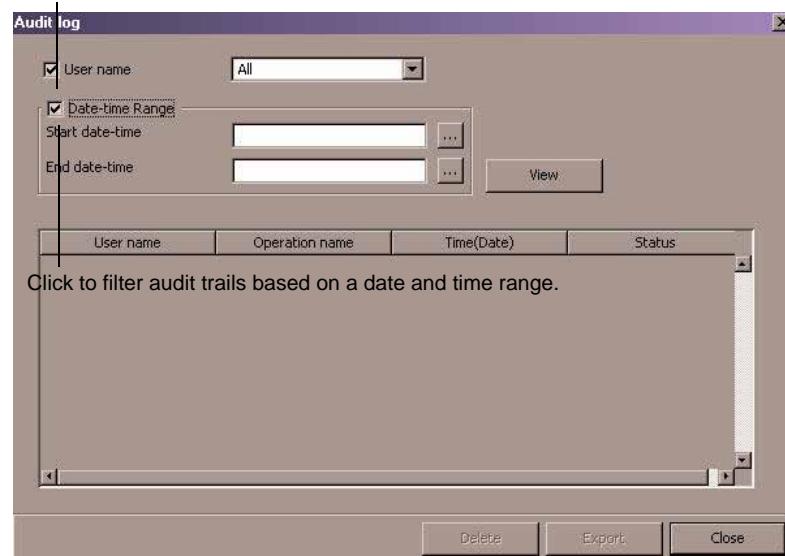
To access audit logs:

- From the Tool menu, choose **Audit logs**. For example:



The Audit log window appears:

Click to filter audit trails based on user name.



From here you can choose the criteria you want to apply to the display of data. You can display audit trails by the following:

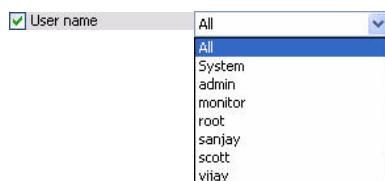
- user name
- date-time range
- user name and date-time range

If you do not choose the date-time range criterion, Net-Net EMS still limits the time to one day (24 hours). The 24 hours counts from the time you click View back 24 hours.

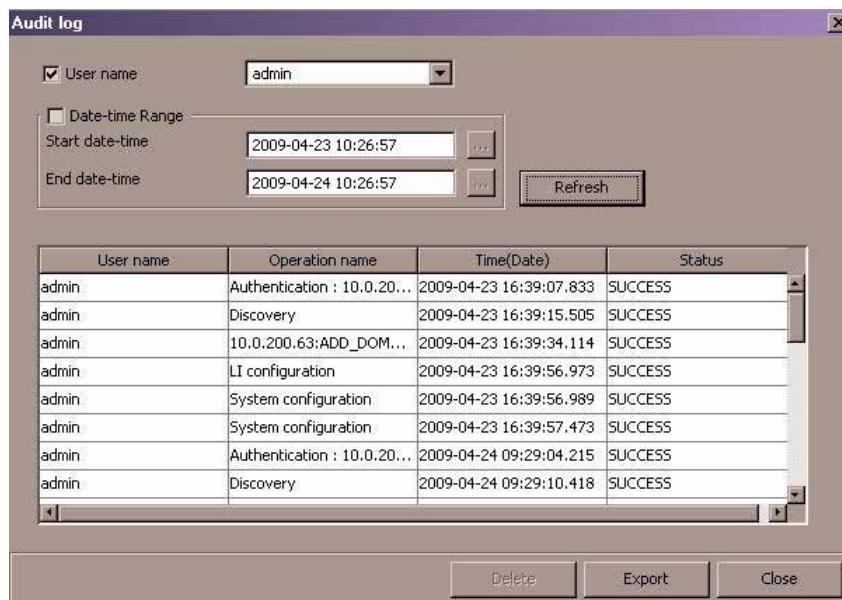
Displaying Audit Trails by User Name

To display audit trails by user name:

1. **User name**—Click the checkbox.
2. Click the down arrow next to the textbox to display the list of all users configured for this Net-Net SBC.



3. Click the user name to select it.
4. Click **View** to display the data. The Audit log window appears and the View button toggles to the Refresh button. For example, the following data is displayed for the user named admin:



From here you can delete one or more audit trails displayed in the Log window and save the data to the file. See *Deleting Audit Trails* and *Saving Data* for details.

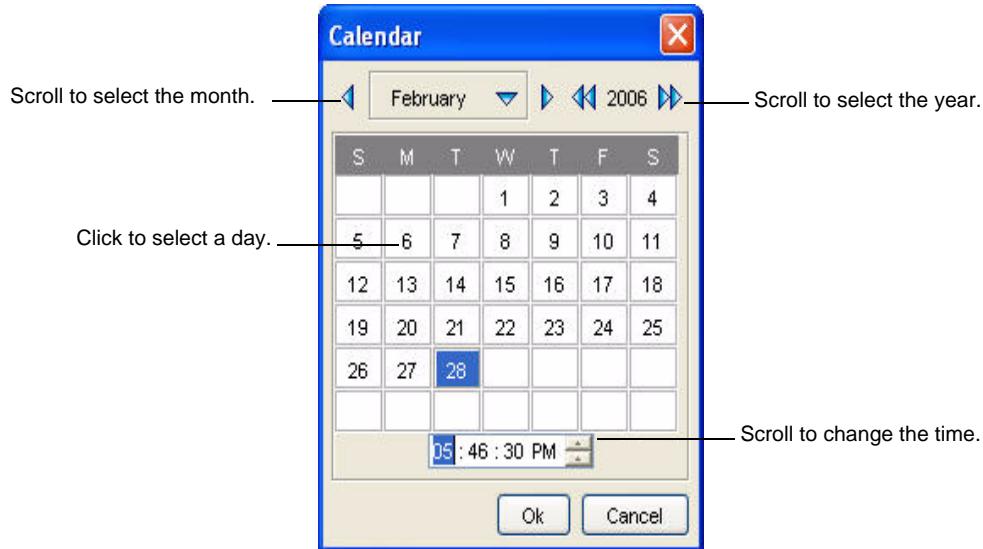
5. Click **Close** to exit the window.

Displaying Audit Trails by Date-Time Range

1. **Date-time Range**—Click the checkbox. The **Start date-time** and **End date-time** options are activated.



2. For the **Start date-time** and **End-date time**, click  to access the Calendar:



3. Choose the month and the year by using the arrows to scroll to the needed options.
4. Choose the day by clicking the appropriate cell.
5. Choose the time by scrolling up or down in the time textbox.
6. Click **OK** to exit the Calendar and apply the values.
7. Click **View** to display the data. The Audit log window appears and the View button toggles to the Refresh button:

| User name | Operation name | Time(Date) | Status |
|-----------|-----------------------------|-------------------------|---------|
| admin | Authentication : 10.0.20... | 2009-04-23 16:39:07.833 | SUCCESS |
| admin | Discovery | 2009-04-23 16:39:15.505 | SUCCESS |
| admin | 10.0.200.63:ADD_DOM... | 2009-04-23 16:39:34.114 | SUCCESS |
| admin | LI configuration | 2009-04-23 16:39:56.973 | SUCCESS |
| admin | System configuration | 2009-04-23 16:39:56.989 | SUCCESS |
| admin | System configuration | 2009-04-23 16:39:57.473 | SUCCESS |
| admin | Authentication : 10.0.20... | 2009-04-24 09:29:04.215 | SUCCESS |
| admin | Discovery | 2009-04-24 09:29:10.418 | SUCCESS |

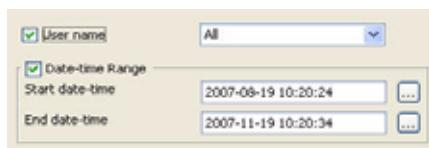
From here you can delete one or more audit trails displayed in the Log window and export and save the data to the file. See *Deleting Audit Trails* and *Saving Data* for details.

8. Click **Close** to exit the window.

Display Audit Trails by User Name and Date-Time Range

To display audit trails by user name and date-time range:

1. **User name**—Click the checkbox and choose the appropriate value.
2. **Date-time Range**—Click the checkbox and choose the appropriate values for **Start date-time** and **End date-time**.



3. Click **View** to display data. The Audit log window appears and the View button toggles to the Refresh button:

| User name | Operation name | Time(Date) | Status |
|-----------|-----------------------------|-------------------------|---------|
| admin | Authentication : 10.0.20... | 2009-04-23 16:39:07.833 | SUCCESS |
| admin | Discovery | 2009-04-23 16:39:15.505 | SUCCESS |
| admin | 10.0.200.63:ADD_DOM... | 2009-04-23 16:39:34.114 | SUCCESS |
| admin | LI configuration | 2009-04-23 16:39:56.973 | SUCCESS |
| admin | System configuration | 2009-04-23 16:39:56.989 | SUCCESS |
| admin | System configuration | 2009-04-23 16:39:57.473 | SUCCESS |
| admin | Authentication : 10.0.20... | 2009-04-24 09:29:04.215 | SUCCESS |
| admin | Discovery | 2009-04-24 09:29:10.418 | SUCCESS |

From here you can delete one or more audit trails displayed in the Log window and save and export the data to the file. See *Deleting Audit Trails* and *Saving Data* for details.

4. Click **Close** to exit the window.

About the Audit Trail Data

The following table defines the audit trail data displayed by Net-Net EMS:

| Data | Description |
|----------------|--|
| User name | Name of the user associated with this audit trail. For example: <ul style="list-style-type: none">• admin• system• monitor |
| Operation name | Description of the operation performed. The operation description can include the following information: <ul style="list-style-type: none">• IP address of the origin of the request. For example, Authentication: 10.0.200.40• Type of operation. For example, user authentication, user logout, adding new objects (OBJ_ADD), Net-Net SBC rediscovery and so on |
| Time(Date) | Date and time the operation occurred |
| Status | Final status of the operation. Values are: <ul style="list-style-type: none">• SUCCESS• FAILED |

Refreshing Audit Trail Data

You can update the audit trail data currently displayed in the Audit log window.

To refresh the data:

1. With audit trail data displayed in the Audit log window, click Refresh. The data currently displayed is updated.

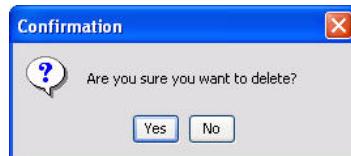
Deleting Audit Trails

The Admin user can delete one or more audit trails displayed in the Log window.

To delete audit trails:

1. Click the row of the audit trail(s) you want to delete. You can select multiple contiguous rows by pressing Shift+click or multiple non-contiguous rows by pressing Ctrl+click.
2. Click Delete.

A confirmation message appears:



3. Click Yes to delete the audit trail(s).

Saving Data

You can save the data displayed on each screen to a text file in comma separated format.

To save data to a file:

1. With the data displayed, click **Save**.
A Save window appears.
2. Enter a name for the file and choose the location where you want to save the file.
3. Click **Save**.

Introduction

Historical data recording (HDR) refers to a group of management features that let you configure the Net-Net SBC to collect statistics about system operation and function, and then send those records to designated servers. System statistics, defined in detail below, are saved to a comma-separated value (CSV) file, which are then sent to the designated server(s).

Information types are grouped so that you can refer to a set of statistics by simply invoking their group name. Within each group, there are several metrics available.

Configuring Net-Net EMS for HDR Collection

You enable HDR by first turning on the system's collection function, then choosing the records you want to capture, and finally setting up server(s) to which you want records sent.

The main collect configuration (found within the main system configuration) allows you to create global settings that:

- Turn the HDR function on and off
- Set the sample rate in seconds, or the time between sample individual collections
- Set the time in seconds in between individual pushes to designated servers (configured in the push receiver configuration accessed via the collect configuration)
- Set the time you want the collect to start and stop; time is entered in year, month, day, hours, minutes, and seconds

You also configure setting for each group of data you want to collect, and the push receiver (server) to which you want data sent.

For complete details about configuring Net-Net EMS for HDR collection, see *Configuring HDR in the Net-Net EMS Decomposed SBC Essentials Guide*.

Group Record Types

In the group-name parameter for the group-settings configuration, you can enter any one of the groups record type defined in the following table. You specify the collection object, and then all metrics for these groups are sent.

| Collection Object | Metrics Included |
|---|---|
| General system statistics (system) | <ul style="list-style-type: none"> • CPU utilization • Memory utilization • Health score • Redundancy state • Current signaling sessions • Current signaling session rate (CPS) • CAM utilization media • CAM utilization ARP • I2C bus state • License capacity |
| Interface statistics (interface) | <ul style="list-style-type: none"> • Interface index • Name/description • Type • MTU • Speed • Physical address • Administrative status • Operational state • In last change • In octets • In unicast packets • In non-unicast packets • In discards • Out errors • Out octets • Out unicast packets • Out non-unicast packets • Out discards • Errors |
| Combined session agent statistics (session-agent) | <ul style="list-style-type: none"> • Hostname • System name • Status • Inbound active sessions • Inbound session rate (CPS) • Outbound active sessions • Outbound session rate (CPS) • Inbound sessions admitted • Inbound sessions not admitted • Inbound concurrent sessions high • Inbound average session rate (CPS) • Outbound sessions admitted • Outbound sessions not admitted • Outbound concurrent sessions high • Outbound average session rate (CPS) • Max burst rate (in and out) (CPS) • Total seizures • Total answered sessions • Answer/seizure ratio • Average one-way signaling latency (ms) • Maximum one-way signaling latency (ms) |

| Collection Object | Metrics Included |
|--|---|
| Session realm statistics (session-realm) | <ul style="list-style-type: none"> • Realm name • Inbound active sessions • Inbound session rate (CPS) • Outbound active sessions • Outbound session rate (CPS) • Inbound sessions admitted • Inbound sessions not admitted • Inbound concurrent sessions high • Inbound average session rate (CPS) • Outbound sessions admitted • Outbound sessions not admitted • Outbound concurrent sessions high • Outbound average session rate (CPS) • Max burst rate (in and out) (CPS) • Total seizures • Total answered sessions • Answer/seizure ratio • Average one-way signaling latency (ms) • Maximum one-way signaling latency (ms) • Average QoS Rfactor (0-93) • MaximumQoS Rfactor (0-93) • Current QoS major exceeded • Total QoS major exceeded • Current QoS critical exceeded • Total QoS critical exceeded |
| Environmental voltage statistics (voltage) | <ul style="list-style-type: none"> • Voltage type • Description • Current voltage (mv) |
| Environmental fan statistics (fan) | <ul style="list-style-type: none"> • Fan type • Description • Speed |
| Environmental temperature statistics (temperature) | <ul style="list-style-type: none"> • Type • Description • Value (Celsius) |
| SIP status statistics (sip-sessions) | <ul style="list-style-type: none"> • Sessions • Subscriptions • Dialogs • Call ID map • Rejections • ReInvites • Media sessions • Media pending • Client transaction • Server transaction • Response contexts • Saved contexts • Sockets • Requests dropped • DNS transactions • DNS sockets • DNS results • Session rate • Load rate |

| Collection Object | Metrics Included |
|---|--|
| SIP error/event statistics (sip-errors) | <ul style="list-style-type: none"> • SDP offer errors • SDP answer errors • Drop media errors • Transaction errors • Media expiration events • Early media expirations • Early media drops • Expired sessions • Multiple OK drops • Multiple OK terminations • Media failure drops • Non-AXK 2XX drops • Invalid requests |
| SIP policy/routing (sip-policy) | <ul style="list-style-type: none"> • Local policy lookups • Local policy hits • Local policy misses • Local policy drops • Agent group hits • Agent groups misses • No routes found • Missing dialog • Inbound SA constraints • Outbound SA constraints • Inbound REG SA constraints • Outbound REG SA constraints • Requests challenged • Challenge found • Challenge not found • Challenge dropped |
| SIP server transaction (sip-server) | <ul style="list-style-type: none"> • All states • Initial • Trying • Proceeding • Cancelled • Established • Completed • Confirmed • Terminated |
| SIP client transactions (sip-client) | <ul style="list-style-type: none"> • All states • Initial • Trying • Calling • Proceeding • Cancelled • EarlyMedia • Completed • SetMedia • Established • Terminated |
| SIP ACL status (sip-ACL-status) | <ul style="list-style-type: none"> • Total entries • Trusted • Blocked |
| SIP ACL operations (sip-ACL-oper) | <ul style="list-style-type: none"> • ACL requests • Bad messages • Promotions • Demotions |

| Collection Object | Metrics Included |
|---------------------------------------|---|
| SIP session status (sip-status) | <ul style="list-style-type: none"> • Sessions initial • Sessions early • Sessions established • Sessions terminated • Dialogs early • Dialogs confirmed • Dialogs terminated |
| MGCP task state (mgcp-state) | <ul style="list-style-type: none"> • MGCP sessions • CA endpoints • GW endpoints • Media sessions • Client transactions • Server transactions • Pending MBCD • MGCP ALGs |
| MGCP transactions (mgcp-trans) | <ul style="list-style-type: none"> • Requests received • Responses sent • Duplicates received • Requests sent • Responses received • Retransmissions sent |
| MGCP media events (mgcp-media-events) | <ul style="list-style-type: none"> • Calling SDP errors • Called SDP errors • Drop media errors • Transaction errors • Media expiration events • Early media expiration • Expiration media drops |
| MGCP ACL status (mgcp-ACL) | <ul style="list-style-type: none"> • Total entries • Trusted • Blocked |
| ACL operation (mgcp-oper) | <ul style="list-style-type: none"> • ACL requests • Bad messages • Promotions • Demotions |
| H.323 statistics (h323-stats) | <ul style="list-style-type: none"> • Incoming calls • Outgoing calls • Connected calls • Incoming channels • Outgoing channels • Contexts • Queued messages • TPKT channels • UDP channels |

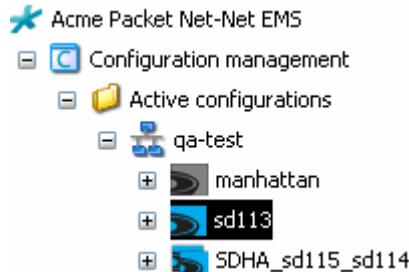
Configuring HDR Reporting Operations

You configure the HDR reporting operations to start and stop collection, to generate reports, and to purge HDR data from a Net-Net SBC.

Accessing HDR Operations

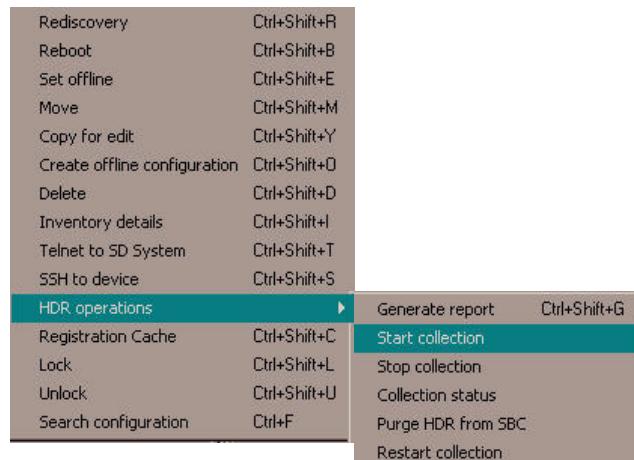
To access HDR operations:

1. In the Active configurations area, right click a Net-Net SBC.



A list of options appears.

2. Scroll over HDR operations to open submenu.



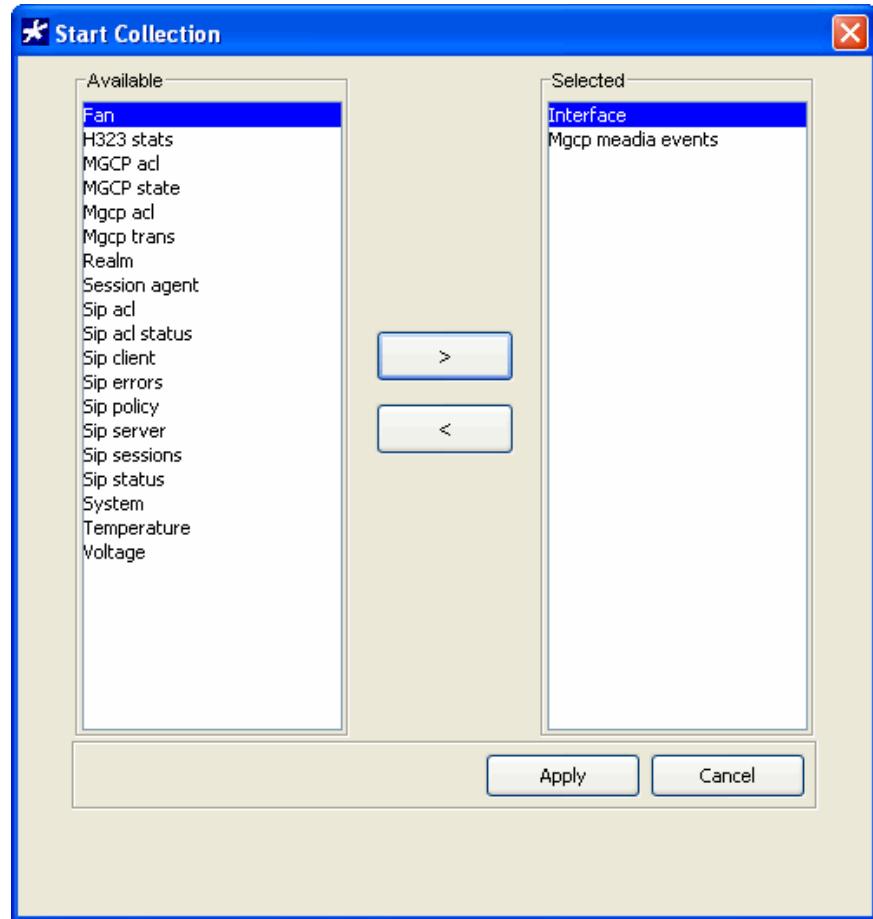
3. Click to choose the operation you want from submenu list.

Starting Data Collection

To start data collection:

1. Click Start collection from the HDR operation submenu list.
2. The Start Collection window appears.
3. Click the collection group for which you want to start collection in the Available list.

4. Click >>> to move the collection group to the Selected list.



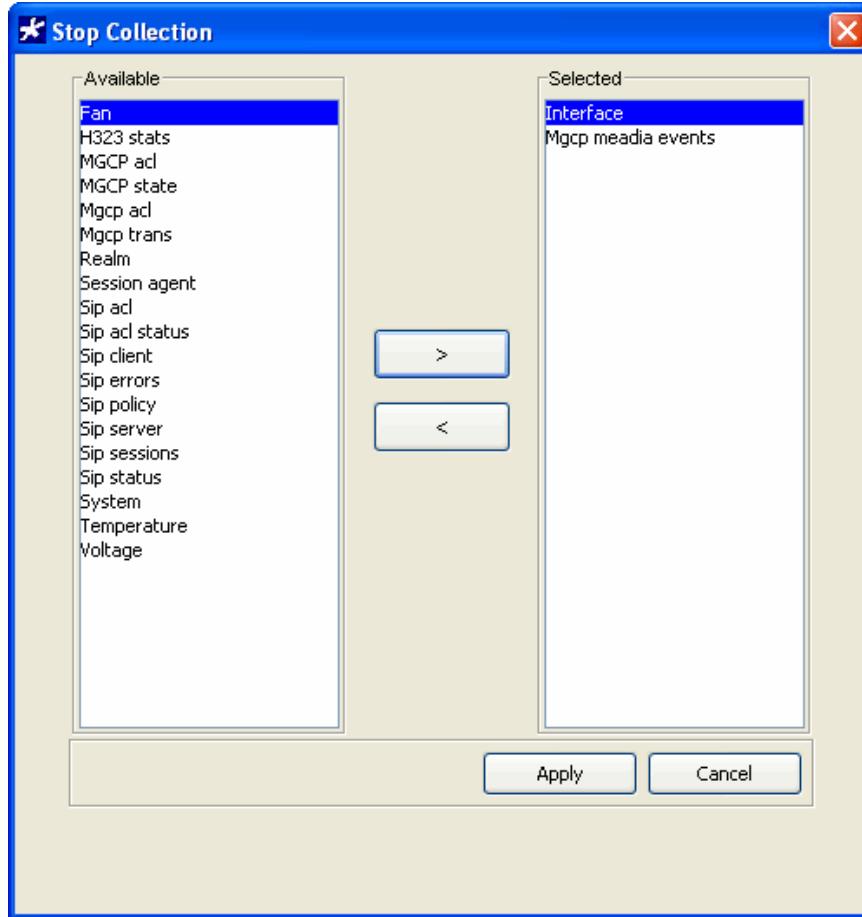
5. Repeat steps 3 and 4 for each collection group for which you want to start collection.
6. Click **Apply**. A Start collection is successful message appears.
7. Click **OK** to clear the message.

Stopping Data Collection

To stop collection:

1. Click Stop collection from the HDR operation submenu list.
2. The Stop Collection window appears.
3. Click the collection group for which you want to stop collection in the Available list.

- Click to move the collection group to the Selected list.

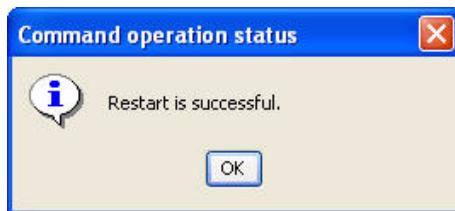


- Repeat steps 3 and 4 for each collection group for which you want to stop collection.
- Click Apply. A Stop collection is successful message appears.
- Click OK to clear the message.

Restarting Collection

To restart collection:

- Choose Restart collection from the Choose HDR operation drop-down list. A message appears that the restart is in progress.
When the restart concludes a message appears stating restart is successful.

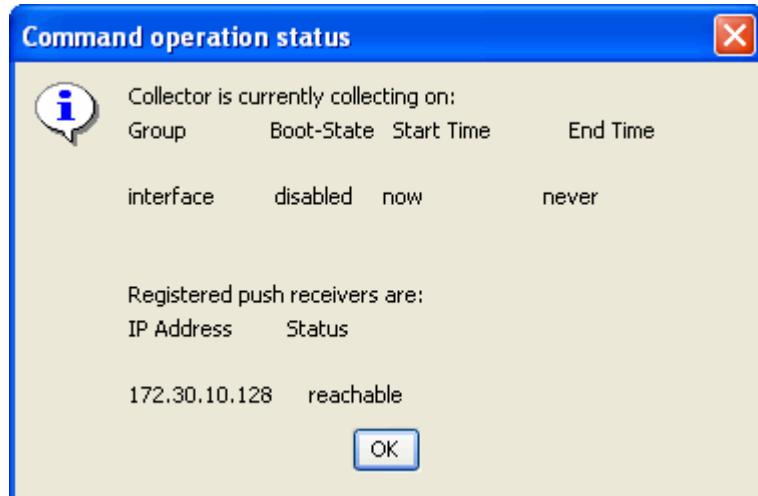


- Click OK to close the dialog box.

Checking Collection Status

To check the status of the collection:

1. Click Collection status from the Choose HDR operation submenu list.
2. A message appears. Then the Command operation status window appears indicating the current collection status.



3. Click OK to close the status window.

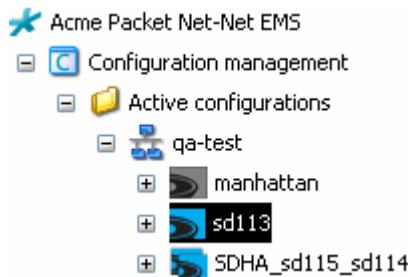
Generating Reports

You can generate HDR data reports by choosing the HDR operations option in the right-click menu and then selecting your report criteria and report style.

Accessing the Report Generation Operation

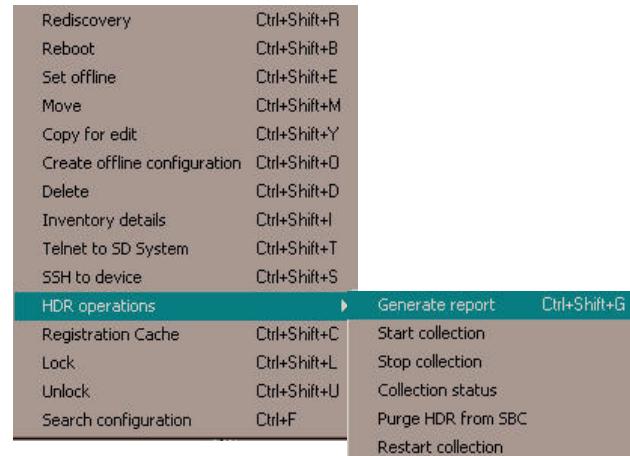
To access the report generation operation:

1. In the Active configurations area, right click a Net-Net SBC.



A list of options appears.

2. Scroll over HDR operations to open a submenu.



3. Click Generate report from submenu list. The Report generation window appears.

Choosing Reporting Criteria

The process of generating the different reports is the same. You choose:

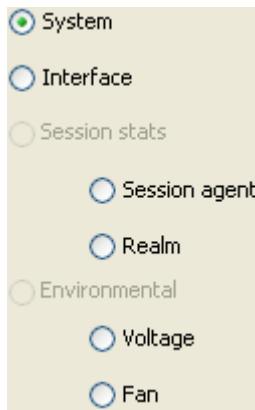
- Group on which you want to report
- Type of report you want to generate
- Start and end date and time of the reporting period
- Data you want to report on

If generating an interface report, you need to choose the interface instance.

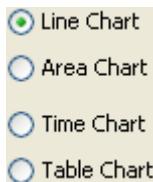
The following instructions show how to generate a line chart for system data. You use the same procedure for generating each type of report.

To generate system reports:

- Groups—Click System.

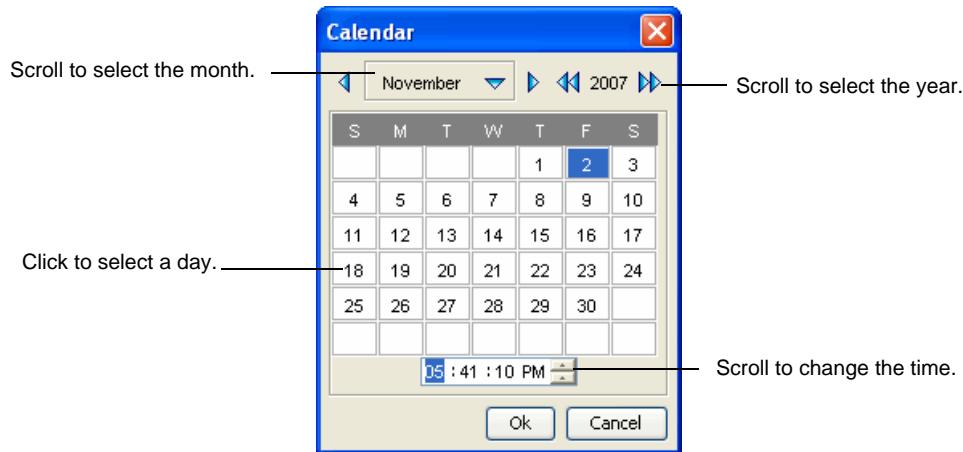


- Report Style—Click the type of report you want. For example:



- Start date time—Click the button with the three dots to access a calendar. Choose the exact date and time (for your local timezone) you want the reporting period to start.
- End date time—Click the button with the three dots to access a calendar. Choose the exact date and time (for your local timezone) you want the reporting period to end.

The Calendar appears:

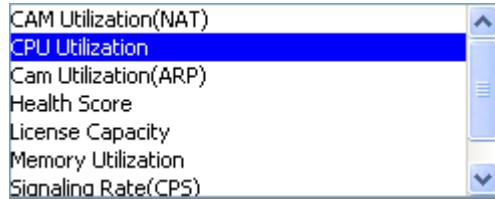


- Choose the month, and the year, for the date by scrolling to the month and year you need.
- Choose the day by clicking the appropriate cell.
- Choose the time by scrolling up or down in the time textbox.

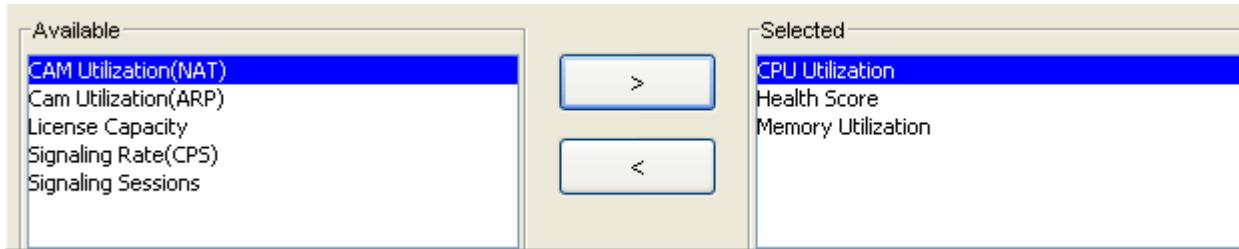
- Click OK to close the Calendar. The start and end dates and time for the reporting period appear in the Date/Time area.

| | | |
|-----------------|---------------------|------------------------------------|
| Start date-time | 2006-11-05 18:50:12 | <input type="button" value="..."/> |
| End date-time | 2007-11-05 18:46:52 | <input type="button" value="..."/> |

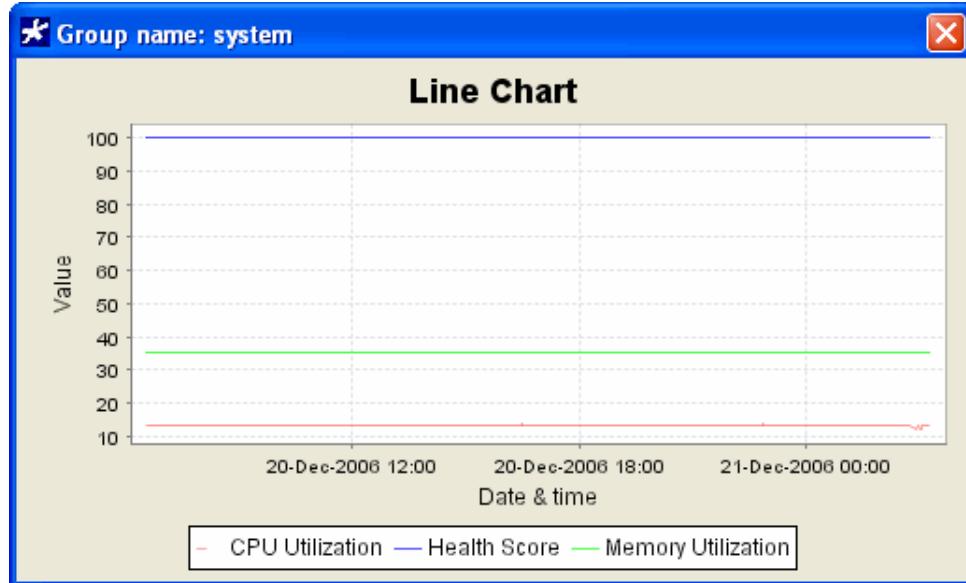
- Choose the data upon which you want to report from the Available list.



- Click to move the data to the Selected list.
- Repeat steps 6 and 7 to choose the data upon which to report. For example:



- Click Apply. The report you configured appears.



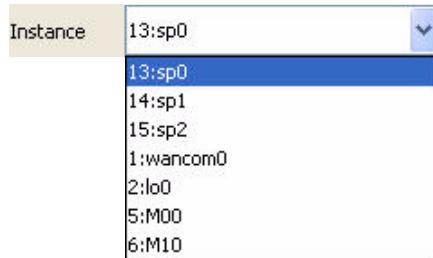
You can change the report type for this data by checking a different type and clicking **Apply** again.

Choose an Interface Instance

If you are generating a report on an interface, you need to choose the interface instance. When you choose Interface in the Groups section and enter the start and end date and time, the Instance parameter and Lookup button are activated in the Report Period section.

To choose the interface instance:

1. Click **Lookup**. The Instance parameter is populated with a list of instances.
2. Choose an instance from the Instance drop-down list.



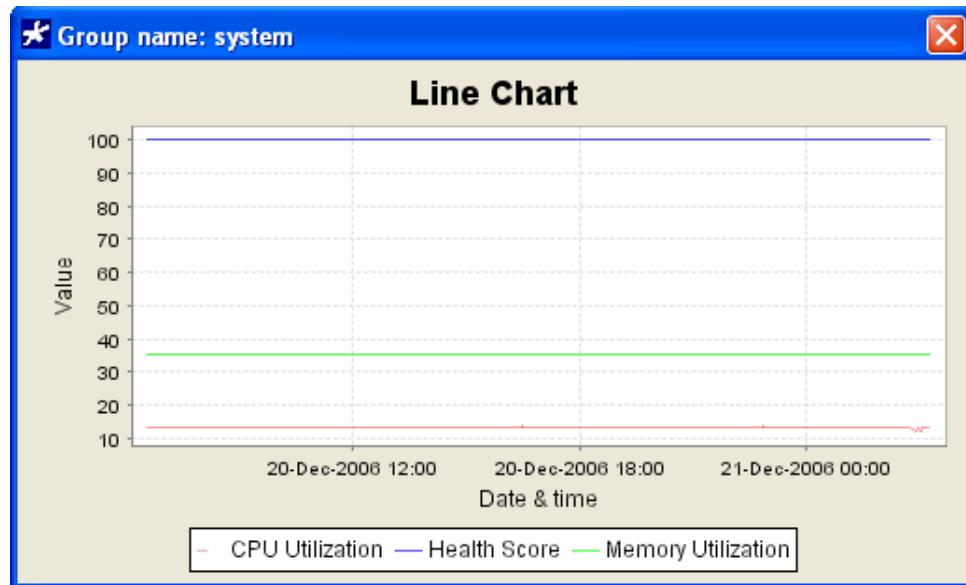
3. Continue to configure the remaining reporting criteria.
4. Click **Apply** to generate the report.

Examples of Report Styles

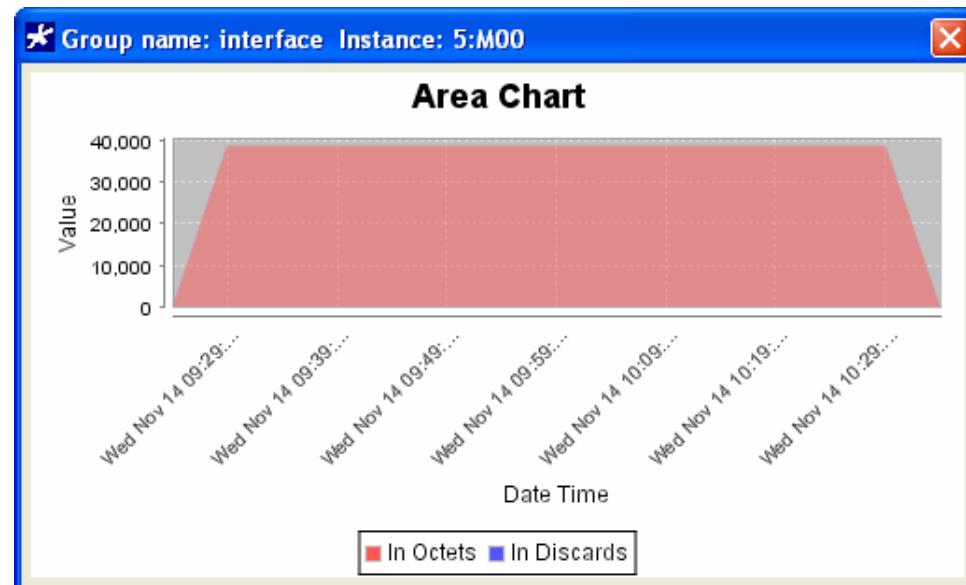
You can generate four different types of reports (charts):

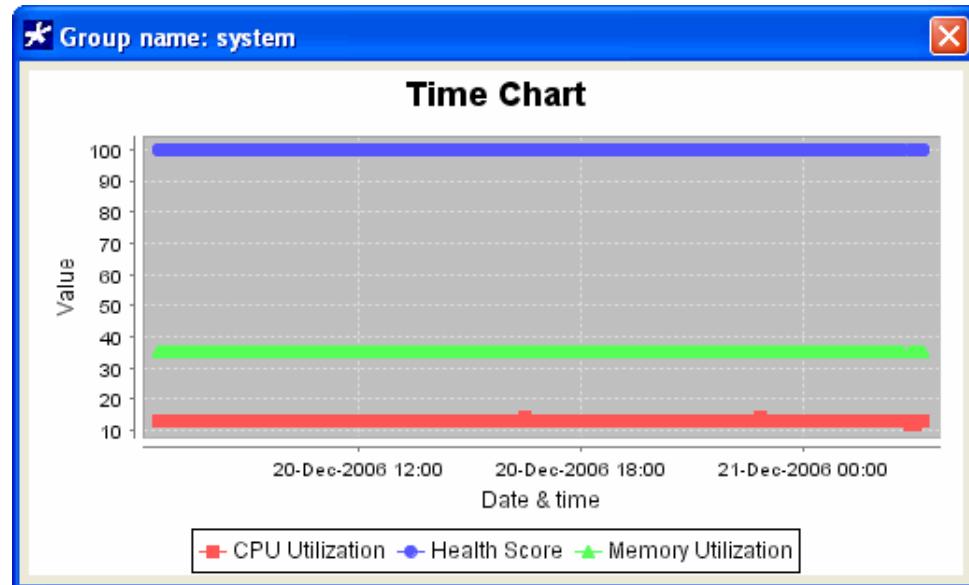
- Line
- Area
- Time
- Table

Line Chart



Area Chart



Time Chart**Table Chart**

Group name: system

| Date Time | CPU Utilization | Health Score | Memory Utilization |
|----------------------|-----------------|--------------|--------------------|
| Wed Dec 20 06:36:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:37:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:38:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:39:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:40:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:41:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:42:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:43:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:44:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:45:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:46:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:47:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:48:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:49:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:50:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:51:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:52:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:53:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:54:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:55:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:56:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:57:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:58:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 06:59:... | 13.0 | 100.0 | 35.0 |
| Wed Dec 20 07:00:... | 13.0 | 100.0 | 35.0 |

Introduction

This chapter describes the Net-Net EMS inventory management component. Each time Net-Net EMS does a discovery or rediscovery of a Net-Net SBC system, the inventory information for that system is retrieved and stored in the database. The results of each new discovery/rediscovery overwrites the existing inventory contents of the database.

Inventory data is maintained for all the nodes and Net-Net SBCs present in the Active configuration area. If a device is deleted from Active configuration, its inventory data is deleted from the database.

Inventory Data Collected

Inventory information is collected on the following Net-Net SBC components:

- hardware components and versions
- software components, which includes software images (current image and other loaded images - includes version) and configuration files (current file and other loaded files)
- software license key

Accessing Inventory Information

This section explains how to access the Inventory management information.

Accessing Inventory Data

You can use the following methods to access inventory information:

- Right-click a specific Net-Net SBC listed under Active configuration and select Inventory details. The Inventory window only displays the details for that Net-Net SBC. (You cannot choose another from the Inventory window.)
- Choose Inventory details from the Inventory option located in the menu bar across the top of the Net-Net EMS screen. You then choose the Net-Net SBC for which you want to view data from the Inventory window. (You can make different choices while in the Inventory window.)

Accessing Data for a Specific Net-Net SBC

To access inventory management information:

- Under the **Active configuration** category, right-click the name of the Net-Net SBC for which you want to view inventory data. A list of options appears:

| | |
|------------------------------|--------------|
| Rediscovery | Ctrl+Shift+R |
| Reboot | Ctrl+Shift+B |
| Set offline | Ctrl+Shift+E |
| Copy for edit | Ctrl+Shift+Y |
| Create offline configuration | Ctrl+Shift+O |
| Create global configuration | Ctrl+Shift+G |
| Delete | Ctrl+Shift+D |
| Inventory details | Ctrl+Shift+I |
| Telnet to SD System | Ctrl+Shift+T |
| SSH to device | Ctrl+Shift+S |
| HDR operations | ▶ |
| Registration Cache | Ctrl+Shift+C |
| Lock | Ctrl+Shift+L |
| Unlock | Ctrl+Shift+U |
| Search configuration | Ctrl+F |
| Configuration inventory | Ctrl+N |
| Synchronize Alarms | Ctrl+A |
| Display config version | Ctrl+W |

- Click **Inventory details** to select it. The Inventory window opens, with data for the specific Net-Net SBC displayed:

The screenshot shows the 'Inventory' window with the title bar 'Inventory'. At the top, there are dropdown menus for 'Type' (set to 'Standalone'), 'Name' (empty), and 'SD system' (set to '172.30.80.100'). Below the menu bar is a toolbar with three tabs: 'Hardware' (selected), 'Software', and 'License'. The main area is a grid table with the following columns: Index, Description, Vendor type, Container id, Class, Parent rel pos, Name, Hardware rev, and Software. The data in the table is as follows:

| Index | Description | Vendor type | Container id | Class | Parent rel pos | Name | Hardware rev | Software |
|-------|------------------|-----------------|--------------|-------------|----------------|------------------|--------------|----------|
| 1 | Assy, Session | .1.3.6.1.4.1... | 0 | chassis | 0 | Session Director | 3 | |
| 2 | Power supply | .1.3.6.1.4.1... | 1 | container | 1 | Power Tray A | | |
| 3 | Assy, 150 ... | .1.3.6.1.4.1... | 2 | powerSupply | 1 | Power Supply | | |
| 4 | Power supply | .1.3.6.1.4.1... | 1 | container | 2 | Power Tray B | | |
| 5 | Assy, 150 ... | .1.3.6.1.4.1... | 4 | powerSupply | 1 | Power Supply | | |
| 6 | Fan tray | .1.3.6.1.4.1... | 1 | container | 3 | Fan Tray | | |
| 7 | Assy, 3-fan ... | .1.3.6.1.4.1... | 6 | fan | 1 | 3-Fan 40x20 | | |
| 8 | PHY slot 0 | .1.3.6.1.4.1... | 1 | container | 4 | PHY Slot 0 | | |
| 9 | Assy, 4 Port ... | .1.3.6.1.4.1... | 8 | module | 1 | Fast Ethernet | 3 | |
| 10 | Assy, 10/10 ... | .1.3.6.1.4.1... | 9 | port | 1 | FEP port 00 | 3 | |
| 11 | Assy, 10/10 ... | .1.3.6.1.4.1... | 9 | port | 2 | FEP port 01 | 3 | |
| 12 | Assy, 10/10 ... | .1.3.6.1.4.1... | 9 | port | 3 | FEP port 02 | 3 | |
| 13 | Assy, 10/10 ... | .1.3.6.1.4.1... | 9 | port | 4 | FEP port 03 | 3 | |
| 14 | PHY slot 1 | .1.3.6.1.4.1... | 1 | container | 5 | PHY Slot 1 | | |
| 15 | Assy, 4 Port ... | .1.3.6.1.4.1... | 14 | module | 1 | Fast Ethernet | 3 | |
| 16 | Assy, 10/10 ... | .1.3.6.1.4.1... | 15 | port | 1 | FEP port 10 | 3 | |
| 17 | Assy, 10/10 ... | .1.3.6.1.4.1... | 15 | port | 2 | FEP port 11 | 3 | |

At the bottom of the window are buttons for 'Refresh', 'Export', and 'OK'.

From here you can navigate through the different categories of inventory data by clicking the Hardware, Software, or License tab. You can export and save the displayed data to a text file. See the following sections for details.

Note: You cannot select a different Net-Net SBC from the Inventory window. See *Accessing Data for All Discovered Net-Net SBCs* for information about choosing from among multiple systems.

No Available Data

An error message appears when there is no Inventory data for a Net-Net SBC, which can occur if the Net-Net SBC is not properly configured for SNMP or if the discovery process was interrupted.

- **Standalone:** Clear the error message and choose a different system under the Active configuration area
- **HA pair:** Clear the error message. From the Inventory window, click the down arrow next to SD system and choose the other Net-Net SBC in the pair. If no data is available for it, close the Inventory window and select another HA pair from under the Active configuration area.

Accessing Data for All Discovered Net-Net SBCs

You can access the Inventory window once, then choose the different standalone Net-Net SBCs, or Net-Net SBC pairs, for which you want to view inventory data.

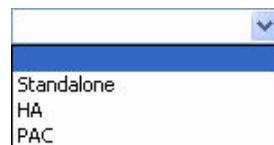
To view inventory data for all discovered systems:

- From the Inventory toolbar option, choose **Inventory details**:



The Inventory window appears.

- In the Inventory window, click the down arrow next to the **Type** textbox to display the type of Net-Net SBCs. For example:



Note: The PAC option is not supported in this release of Net-Net EMS.

- Choose either **standalone** or **HA** from the list. See the instructions in the following sections for more details.

Viewing Standalone Data

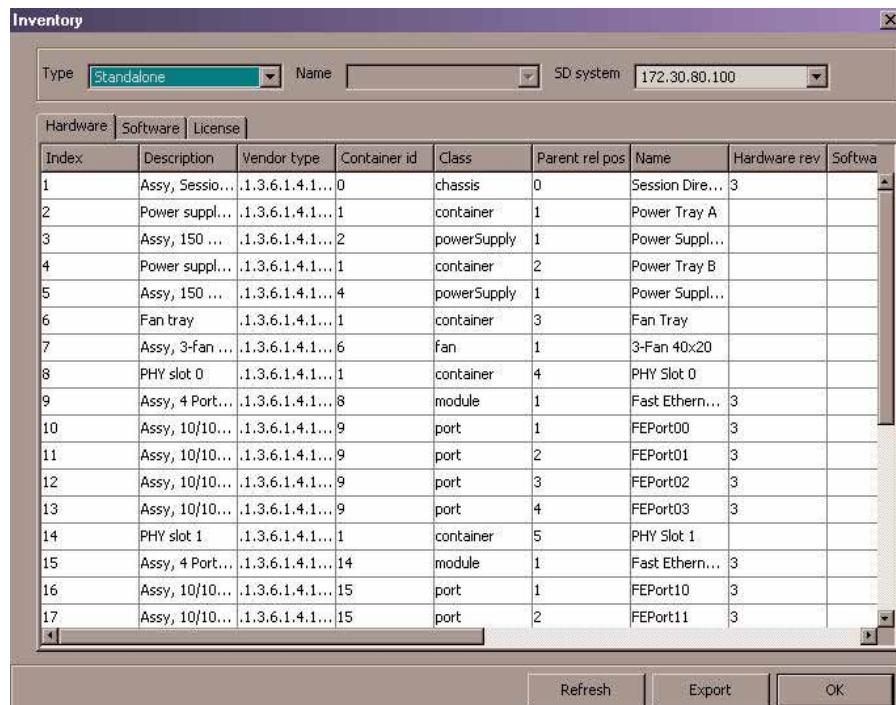
To view standalone data:

- From the Type dropdown list, click **standalone**.
- Click the down arrow next to the **SD system** textbox to display all currently discovered standalone systems. For example:



- Click the name of the system for which you want to view data.

- The Inventory window appears with data displayed. By default, the hardware data for the Net-Net system you chose is displayed (if any data is available). For example:



The screenshot shows the 'Inventory' window with the following details:

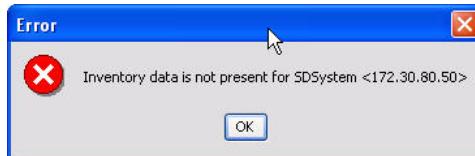
- Type:** Standalone
- Name:** SD system
- IP Address:** 172.30.80.100
- Hardware Tab:** Selected
- Software Tab:** Unselected
- License Tab:** Unselected
- Table Headers:** Index, Description, Vendor type, Container id, Class, Parent rel pos, Name, Hardware rev, Software
- Data Rows:** 17 rows of hardware components, including chassis, power supplies, fans, and ports.
- Buttons at the bottom:** Refresh, Export, OK

From here you can chose the category of information you want to view. You can export and save the inventory data to a file.

Note: If Net-Net EMS displays an error message instead of data, proceed to the next section.

No Data is Available

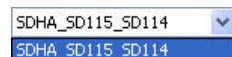
If no inventory data is available for the chosen Net-Net SBC, the following error message appears:



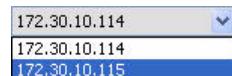
- Click **OK** to clear the error message.
- Choose a different Net-Net SBC from the **SD system** list or exit the Inventory window.

Viewing HA Data**To view HA data:**

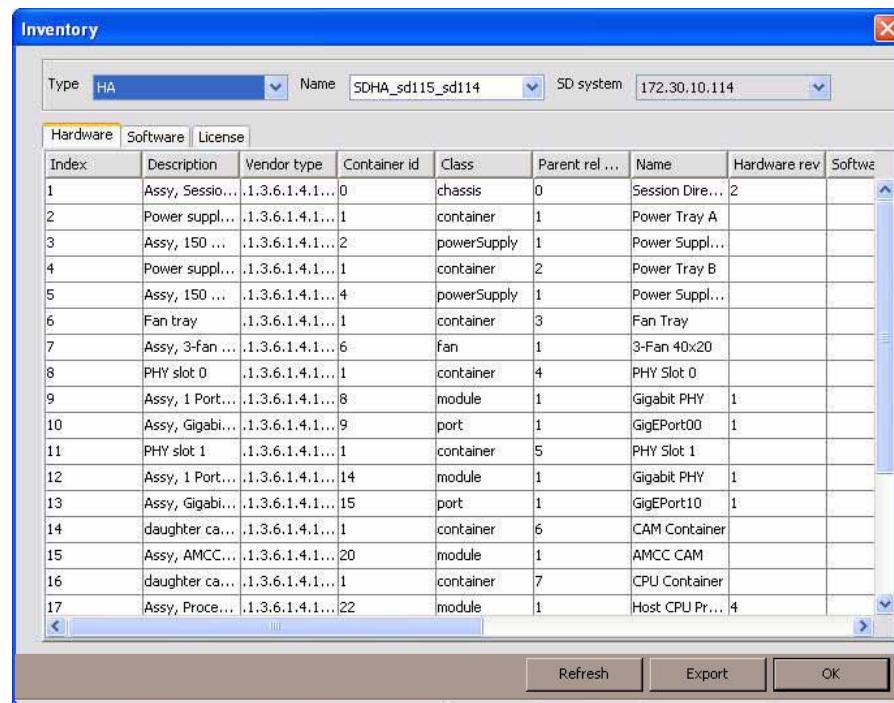
1. From the Type dropdown list, click HA.
2. Click the down arrow next to the Name textbox to display all currently discovered HA pairs. For example:



3. Click the name of the system for which you want to view data.
4. Click the down arrow next to the SD system textbox to display the Net-Net SBCs that belong to that pair. For example:



5. Click the Net-Net SBC for which you want to view inventory data. The Inventory window displays the hardware data for that system by default:

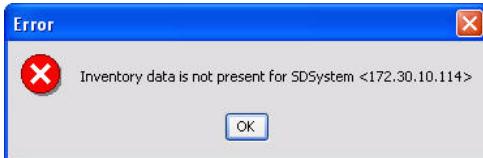


From here you can chose the category of information you want to view. See the following sections for details.

Note: If Net-Net EMS displays an error message instead of data, proceed to the next section.

No Data is Available

If no inventory data is available for the chosen Net-Net SBC, the following error message appears:



1. Click **OK** to clear the error message.
2. Choose the other Net-Net system that belongs to the pair from the **SD system** list, choose a different HA pair from the **Name** list, or exit the Inventory window.

Saving Data

You can save the data displayed on each screen to a text file in comma separated format.

To save data to a file:

1. With the data displayed, click **Save**.
A Save window appears.
2. Enter a name for the file and choose the location where you want to save it.
3. Click **Save**.

Net-Net SBC Configuration Integrity

Net-Net EMS maintains a configuration inventory for each active and inactive Net-Net SBC configuration. This inventory is used to check whether there are discrepancies between the Net-Net SBC's configuration as seen by Net-Net EMS and as seen by the device itself. The record information is retrieved from the Net-Net SBC during each save and discover operation and matched against the information in Net-Net EMS.

Configuration Record Counting

During the discovery phase, Net-Net EMS compares the record count advertised by the Net-Net SBC to the data read by Net-Net EMS. This process confirms that the configuration was correctly discovered from the managed device before being stored in the Net-Net EMS database.

Discovery

If you initiate discovery or rediscovery, Net-Net EMS retrieves the inventory list to obtain the list of objects configured at the Net-Net SBC. Net-Net EMS sets up a list of counters, one for each object in the inventory list. As elements are retrieved, Net-Net EMS increments the corresponding counter. When the discovery or rediscovery finishes, the retrieved counter list is compared to the inventory list. If they do not match, the discovery or rediscovery fails.

When you copy a configuration for edit, the record count is propagated. If elements are added or deleted the corresponding count is updated.

Save

The Net-Net EMS process for saving a configuration involves deleting the current elements at the managed device and re-creating each element stored in the Net-Net EMS database at the managed device, one at a time. After the elements are created, a save command instructs the managed device that the configuration is complete and to save the configuration to persistent storage.

With this feature, Net-Net EMS maintains its own inventory list for an inactive configuration. When that inactive configuration is saved to the Net-Net SBC, the managed device's inventory maintained by the Net-Net SBC is compared to the Net-Net EMS inventory. If they match, the save command is issued.

If the inventories do not match, the Net-Net EMS save fails and an error message appears. Net-Net EMS does not move to the save or the activate configuration phase. The user can perform a manual activate at this point to re-activate the last saved configuration.

Accessing the Configuration Record Count

You can access the record count for a Net-Net SBC configuration and save it to a file.

To check configuration record counts:

1. You can check the record count for an active or inactive configuration by accessing the Configuration inventory right-click option.

For example, under the **Active configuration** category, right-click the name of the Net-Net SBC for which you want to view inventory data. A list of options appears:

| | |
|------------------------------|--------------|
| Rediscovery | Ctrl+Shift+R |
| Reboot | Ctrl+Shift+B |
| Set offline | Ctrl+Shift+E |
| Copy for edit | Ctrl+Shift+Y |
| Create offline configuration | Ctrl+Shift+O |
| Create global configuration | Ctrl+Shift+G |
| Delete | Ctrl+Shift+D |
| Inventory details | Ctrl+Shift+I |
| Telnet to SD System | Ctrl+Shift+T |
| SSH to device | Ctrl+Shift+S |
| HDR operations | ▶ |
| Registration Cache | Ctrl+Shift+C |
| Lock | Ctrl+Shift+L |
| Unlock | Ctrl+Shift+U |
| Search configuration | Ctrl+F |
| Configuration inventory | Ctrl+N |
| Synchronize Alarms | Ctrl+A |
| Display config version | Ctrl+W |

2. Click **configuration inventory** to select it. The Configuration Inventory window appears.

| Object type | Count |
|--------------------|-------|
| h248MgConfig | 0 |
| ipsecGlobalConfig | 0 |
| mediaPolicy | 2 |
| authConfig | 1 |
| staticFlow | 1 |
| phyInterfaceConfig | 3 |
| certRecord | 4 |
| saConfig | 1 |
| sipManipulation | 2 |
| dnsConfig | 1 |
| captureReceiver | 1 |
| steeringPool | 9 |
| classPolicy | 2 |
| H323StackConfig | 2 |
| rphPolicy | 2 |

Refresh Cancel Export

You can review the list of configuration objects and their associated counts. At the bottom of the display, a total count of all records is displayed.

3. *Optional.* Export and save the record count to a file.

Saving Record Counts You can save the data displayed to a text file in comma separated format.

To save data to a file:

1. With the data displayed, click **Save**.
A Save window appears.
2. Enter a name for the file and choose the location where you want to save it.
3. Click **Save**.

Viewing Hardware Information

This section explains the inventory data displayed by the Net-Net EMS for the following hardware components:

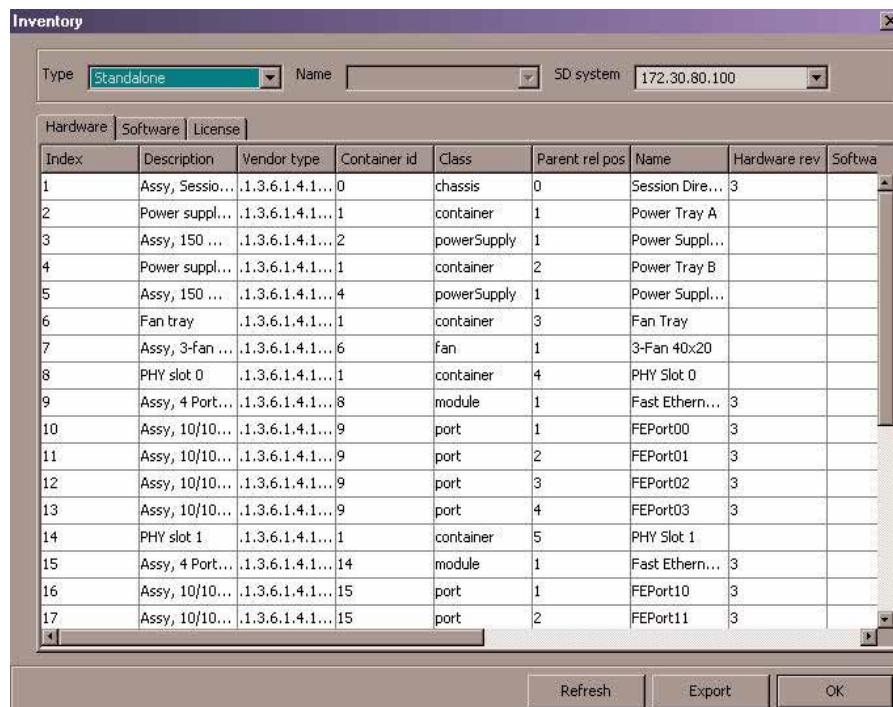
- chassis (main system board)
- CPU
- memory
- network processor
- fans
- packet-processing CAM
- environmental sensors
- network interface
- physical interface cards
- power supplies

Accessing Hardware Data

To access hardware data:

1. In the Inventory window, ensure the Hardware tab is selected.
2. Choose the type of Net-Net SBC by clicking **standalone** or **HA**. The data for your choice appears in the Inventory window. The same information is displayed for either type of Net-Net SBC.

The following example shows the data for a standalone Net-Net SBC:



The screenshot shows the 'Inventory' window with the 'Hardware' tab selected. The 'Type' dropdown is set to 'Standalone'. The table displays 17 rows of hardware components, each with an index number, description, vendor type, container ID, class, parent relative position, name, hardware revision, and software revision. The components include various parts like Session Director, Power Trays, Fan trays, and PHY slots.

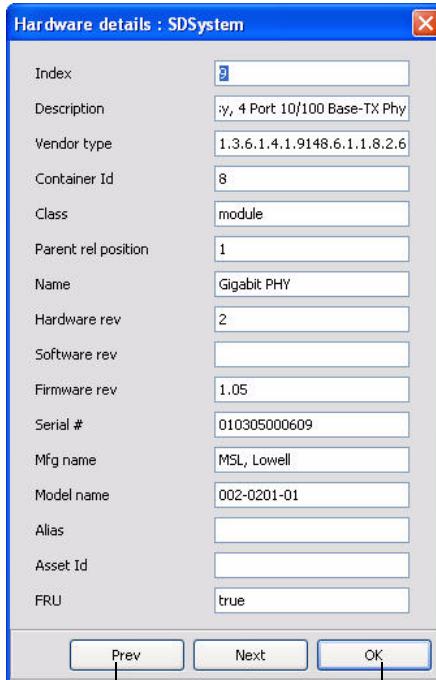
| Index | Description | Vendor type | Container id | Class | Parent rel pos | Name | Hardware rev | Software rev |
|-------|-------------------------|----------------|--------------|-------------|----------------|------------------|--------------|--------------|
| 1 | Assy, Session Director | 1.3.6.1.4.1... | 0 | chassis | 0 | Session Director | 3 | |
| 2 | Power supply | 1.3.6.1.4.1... | 1 | container | 1 | Power Tray A | | |
| 3 | Assy, 150W Power Supply | 1.3.6.1.4.1... | 2 | powerSupply | 1 | Power Supply | | |
| 4 | Power supply | 1.3.6.1.4.1... | 1 | container | 2 | Power Tray B | | |
| 5 | Assy, 150W Power Supply | 1.3.6.1.4.1... | 4 | powerSupply | 1 | Power Supply | | |
| 6 | Fan tray | 1.3.6.1.4.1... | 1 | container | 3 | Fan Tray | | |
| 7 | Assy, 3-fan tray | 1.3.6.1.4.1... | 6 | fan | 1 | 3-Fan 40x20 | | |
| 8 | PHY slot 0 | 1.3.6.1.4.1... | 1 | container | 4 | PHY Slot 0 | | |
| 9 | Assy, 4 Port SFP | 1.3.6.1.4.1... | 8 | module | 1 | Fast Ethernet | 3 | |
| 10 | Assy, 10/10GbE port | 1.3.6.1.4.1... | 9 | port | 1 | FEPort00 | 3 | |
| 11 | Assy, 10/10GbE port | 1.3.6.1.4.1... | 9 | port | 2 | FEPort01 | 3 | |
| 12 | Assy, 10/10GbE port | 1.3.6.1.4.1... | 9 | port | 3 | FEPort02 | 3 | |
| 13 | Assy, 10/10GbE port | 1.3.6.1.4.1... | 9 | port | 4 | FEPort03 | 3 | |
| 14 | PHY slot 1 | 1.3.6.1.4.1... | 1 | container | 5 | PHY Slot 1 | | |
| 15 | Assy, 4 Port SFP | 1.3.6.1.4.1... | 14 | module | 1 | Fast Ethernet | 3 | |
| 16 | Assy, 10/10GbE port | 1.3.6.1.4.1... | 15 | port | 1 | FEPort10 | 3 | |
| 17 | Assy, 10/10GbE port | 1.3.6.1.4.1... | 15 | port | 2 | FEPort11 | 3 | |

The following table defines the data displayed by Net-Net EMS for a standalone Net-Net SBC or for the Net-Net SBCs that belong to an HA pair:

| Data | Description |
|----------------|--|
| Index | Number that represents the physical entity |
| Description | Textual description of the physical entity |
| Vendor type | Vendor-specific hardware type of the physical entity. (This value is different from the definition of MIB-II's sysObjectID.) |
| Container id | Value of the entPhysicalIndex for the physical entity that <i>contains</i> this physical entity |
| Class | Enumerated value that indicates the general hardware type of this physical entity |
| Parent rel pos | Relative position of this <i>child</i> component among all its <i>sibling</i> components |
| Name | Textual name of this physical entity. Name of the component as assigned by the local device |
| Hardware rev | Vendor-specific hardware revision string for the physical entity |
| Software rev | Vendor-specific software revision string for the physical entity |
| Firmware rev | Vendor-specific firmware revision string for the physical entity |
| Serial # | Vendor-specific serial number string for the physical entity |
| Mfg name | Name of the manufacturer of this physical entity |
| Model name | Vendor-specific model name identifier string associated with this physical entity |
| Alias | Alias name for the physical entity as specified by a network manager. It provides a non-volatile <i>handle</i> for the physical entity. |
| Asset ID | User-assigned asset tracking identifier for the physical entity as specified by a network manager. It provides non-volatile storage of this information. |
| FRU | Whether this physical entity is considered a field replace unit (FRU) by the vendor |

Viewing the Details**To view the details:**

1. In the Hardware table, double-click the row of the hardware component for which you want to view details. The Hardware details window appears:



Click to view details for previous entry in the table. Click to view details for the next entry in the table.

2. Click **Prev** and **Next** to scroll forward and backward through all the Hardware table entry details.
3. Click **OK** to close the window.

Viewing Software Information

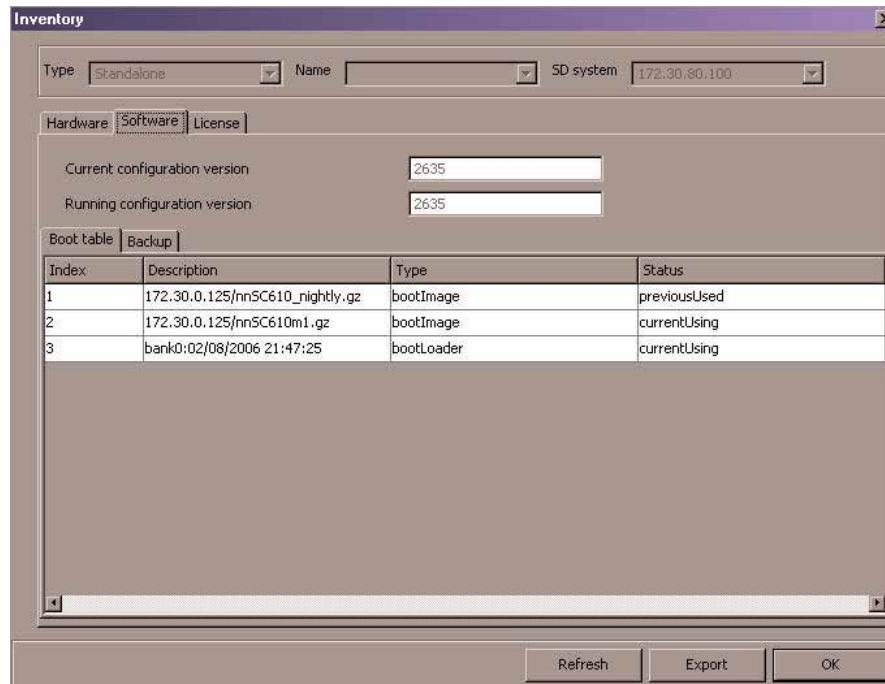
This section explains how to view the inventory data for the following software components:

- Software images: current software image as well as other loaded images, including the version.
- Configuration files: current file as well as other loaded files

Accessing Software Data

To access software data:

1. Select either a standalone Net-Net SBC or an HA pair.
2. In the Inventory window, click the Software tab. By default, the Boot Table software inventory data appears:



About the Configuration Versions

The top section of the screen displays both the current configuration version and the running configuration version.

- Current configuration version: Saved version number of the current configuration
- Running configuration version: Saved version number of the configuration currently running on the Net-Net SBC

About the Boot Table Data

Boot parameters specify what information your Net-Net system uses at boot time when it prepares to run applications. The Net-Net system's boot parameters:

- Determine what software image the Net-Net SBC is using and from where it boots that image: an external device or internal flash memory
- Type of software entity being booted

- Status of that software entity

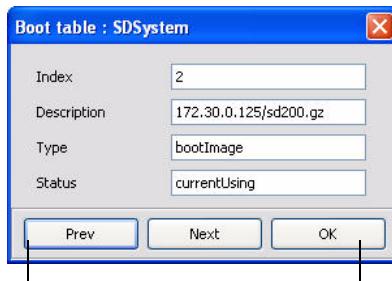
The following table defines the boot table data displayed by Net-Net EMS for a standalone Net-Net SBC or for the Net-Net SBCs that belong to an HA pair:

| Data | Description |
|-------------|--|
| Index | Number that represents the physical entity |
| Description | <p>Textual description that uniquely identifies the software image. Filename, date and time image was built, or other unique identifier can be used. For example:</p> <ul style="list-style-type: none"> • <i>host address/image name</i> (boot image) 10.0.1.12/sd121p3.gz • <i>boot from flash0/image name</i> (boot image) /tfss0/sd121p3.gz • <i>bank0:date time</i> (boot loader) bank0:06/13/2005 10:58:25 |
| Type | Software entity type. Values are: <ul style="list-style-type: none"> • bootImage • bootLoader |
| Status | Software entity status. Values are: <ul style="list-style-type: none"> • previousUsed • currentUsing |

Viewing Boot Table Details

You can view the details of a software component.

1. In the Boot Table display, double-click the row of a specific software component. The Boot table details window appears:



Click to view details for previous entry in the table.

Click to view details for the next entry in the table.

2. Click **Prev** and **Next** to scroll forward and backward through all the Boot table entry details.
3. Click **OK** to close the window.

Viewing Backup Information

The Net-Net SBC can save an existing configuration into a single backup file. Backups are created as gzipped tar files in a .tar.gz format. They are stored in the `/code/bkups` directory on the Net-Net SBC.

To view backup data:

1. In the Software display, click the Backup tab. The table of backup files appears:

| Backup | |
|--------|------------------------|
| Index | Name |
| 1 | gx-cfg-detroit |
| 2 | gx-cfg-det-wsmp.tar.gz |
| 3 | gx-detroit-lab.tar.gz |
| 4 | 1024vlans-cfg.tar.gz |
| 5 | pat-hnt |

Viewing Details**To view details:**

1. In the table, double-click the name of a specific backup file. The Backup table detail window appears:



Click to view details for previous entry in the table. Click to view details for the next entry.

2. Click **Prev** and **Next** to scroll forward and backward through all the Backup table entry details.
3. Click **OK** to close the window.

Viewing License Information

This section explains how to view inventory data for the licenses. All components of the Net-Net system software are licensed by Acme Packet, Inc. (In order to use these components and deploy their related services in your network, you must have a valid license for each of them.)

Accessing License Data

To access license data:

1. In the Inventory window, click the License tab. The license inventory data appears:



About the Total Capacity

The top section of the screen displays the total capacity for the Net-Net SBC, which comprises the maximum number of simultaneous sessions allowed by a Net-Net system for all combined protocols. If the Net-Net SBC had undergone several license upgrades, the value of each Capacity row adds up to the Total Capacity value.

For example:

Total capacity

About the License Data

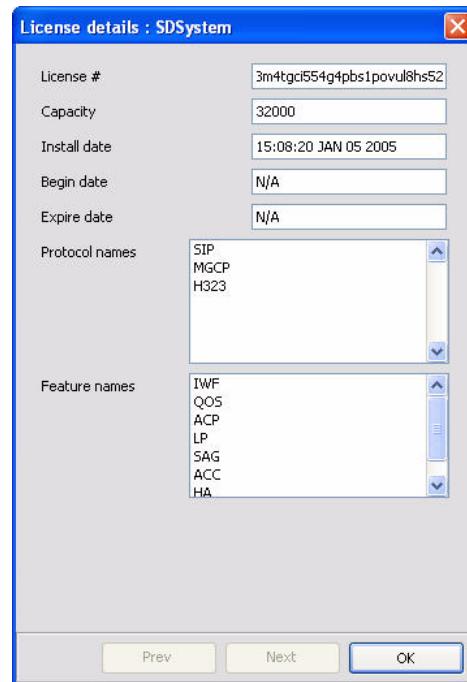
The following table defines the data displayed by Net-Net EMS for a standalone Net-Net SBC or for the Net-Net SBCs that belong to an HA pair:

| Data | Description |
|-----------|--|
| License # | License number |
| Capacity | Maximum number of simultaneous sessions allowed by the Net-Net system for all combined protocols |

| Data | Description |
|----------------|--|
| Install date | Installation time and date in the following format: hh:mm:ss Month Day Year. Displays N/A if a license is not enabled. |
| Begin date | Installation time and date in the following format: hh:mm:ss month day year. Displays N/A if a license is not enabled. |
| Expire date | Expiration time and date in the following format: hh:mm:ss Month Day Year. Displays N/A if a license is not enabled. |
| Protocol names | All protocols licensed for this Net-Net SBC. Values are: <ul style="list-style-type: none"> • SIP • MGCP • H.323 |
| Feature names | All features licensed for this Net-Net SBC. Values are: <ul style="list-style-type: none"> • Interworking (IWF) • Quality of Service (QoS) • Acme Control Protocol (ACP) • Local Policy (LP) • Session Agent Group (SAG) • ACC (allows the Net-Net system to create connections and send CDRs to one or more RADIUS servers) • High Availability (HA) |

Viewing Details**To view details:**

1. In the table, double-click the license row. The License details window appears:



2. Click OK to close the window.

Overview

This chapter contains information about fault management using Net-Net EMS. Fault management involves the following:

- Network event log
- Alarm monitoring and reporting
- System log

The information about events, alarms, and syslog is based on the Acme Packet® standard and proprietary Management Information Bases (MIBs). For more information about the events, alarms, and MIBs, see the *Net-Net MIB Reference Guide*. For information about Net-Net SBC logging, see the *Logs* chapter in the *Net-Net EMS 4000 Configuration Guide*.

About the Relationship of Traps to Events and Alarms

All SNMP traps from nodes managed by Net-Net EMS appear as events in the Network events window. Only a subset of traps are considered to be alarms, which appear in the Alarms window. In general, the Net-Net EMS characterization of alarms matches that of the Net-Net SBC. See the *Net-Net MIB Reference Guide* for more information.

Verifying Net-Net SBC Configuration

You should verify that the Net-Net SBCs for which you want to view fault management information have the following information configured:

- Simple Network Management Protocol (SNMP) communities
- MIB contact
- Trap receivers
- Syslog events

These features are necessary to use Acme Packet's Net-Net EMS to manage Net-Net SBCs. They provide important monitoring and system health information that contribute to a robust deployment of the Net-Net system.

You can also configure the optional syslog server. Syslogs conform to the standard used for logging servers and processes as defined in RFC 3164.

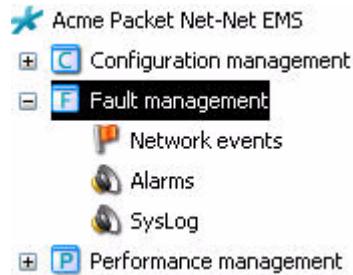
See the *System Configuration* chapter of the *Net-Net EMS 4000 Configuration Guide* for complete information about these parameters.

Accessing Fault Management Information

This section explains how to access the Net-Net SBC fault information displayed by Net-Net EMS.

To access fault management information:

1. In the Navigation tree, click the plus sign (+) next to **Fault management** to expand it. For example:



From here you can choose the type of information you want to view. See the following sections for specific information.

Viewing Event Information

This section explains how to access and view event information. Events are caused by actions that generate one or more of the following:

- Alarms
- Entries in a log file
- SNMP traps

For more information about events, refer to the *Net-Net MIB Reference Guide*.

Event Severity

There are eight severity levels ranging from the highest, Emergency to the lowest severity of Debug.

| syslog Numerical Code | syslog Severity | Acme Packet Log Enumeration |
|----------------------------------|---|--------------------------------------|
| 0 | Emergency (system is unusable) | EMERGENCY (0) |
| 1 | Alert (action must be taken immediately) | CRITICAL (1) |
| 2 | Critical (critical conditions) | MAJOR (2) |
| 3 | Error (error conditions) | MINOR (3) |
| 4 | Warning (warning conditions) | WARNING (4) |
| 5 | Notice (normal but significant condition) | NOTICE (5) |
| 6 | Informational (informational messages) | INFO (6) |
| 7 | Debug (debug level messages) | TRACE (7) DEBUG (8) DETAIL (9) |

Accessing Event Information

To access event information:

1. In the Net-Net EMS navigation tree, click the plus sign (+) to expand **Fault management**.
2. Click **Network events**.

The list of network events appears in the right pane. For example:

Click column headers to change sort order.

Change the number of events on the page. Navigate pages.

Double-click row to view event details.

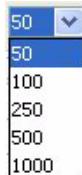
| Server-Time | Severity | Category | Host Name/IP Address | Device time | Failed Resource | SysUpTime | Description | Method |
|---------------------|----------|-----------|----------------------|-------------|-----------------|-----------|------------------------------------|----------|
| 2009-04-10 07:49:39 | Clear | Polling | 172.30.80.100 | | 172.30.80.100 | | Device 172.30.80.100 is reachable. | |
| 2009-04-10 10:24:39 | Clear | Polling | 172.30.80.100 | | 172.30.80.100 | | Device 172.30.80.100 is reachable. | |
| 2009-04-10 07:49:09 | Critical | Discovery | 172.30.80.81 | | 172.30.80.81 | | Failed discovery for 172.30.80.81 | Internal |

Changing Number of Events on the Page

By default, 50 events are shown per page in the Network events view.

To change the number of events displayed:

1. At the top of the Network events window, click the down arrow for **Page Length**. The drop down list of values appears.



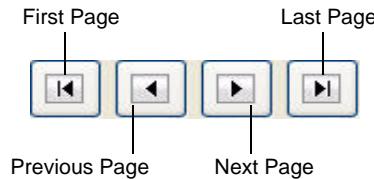
2. Click the number you want to apply.

Navigating Pages

To navigate through multiple pages:

1. Use the navigation arrows located at the top of the Network events window to navigate through multiple pages.

Clicking navigation icons display the desired page, such as the first page, previous page, next page, and the last page of Events list view. For example:



Sorting Events

By default, the events in the Events List View are displayed in the order of precedence based on the Date/Time and Event ID and in descending order. Events are assigned IDs and these are based on the date and time they are generated. Hence these two properties are interrelated. This order can be changed using the **Sorting** option.

To sort events:

1. In the Events List View, click the column header for the column you want to change the sort order.

When you click the column header for the first time, the column is sorted in ascending order. Clicking the same column header again sorts the column in descending order. The up and down arrows in the headers indicate ascending and descending order, respectively.

For example, if you need to sort the events based on its status, click the **Severity** column header. This sorts the events based on its severity and the default order of precedence is Critical, Major, Minor, Warning, Clear, and info. For descending order of the same column, click the **Severity** column header again.

Viewing Event Details

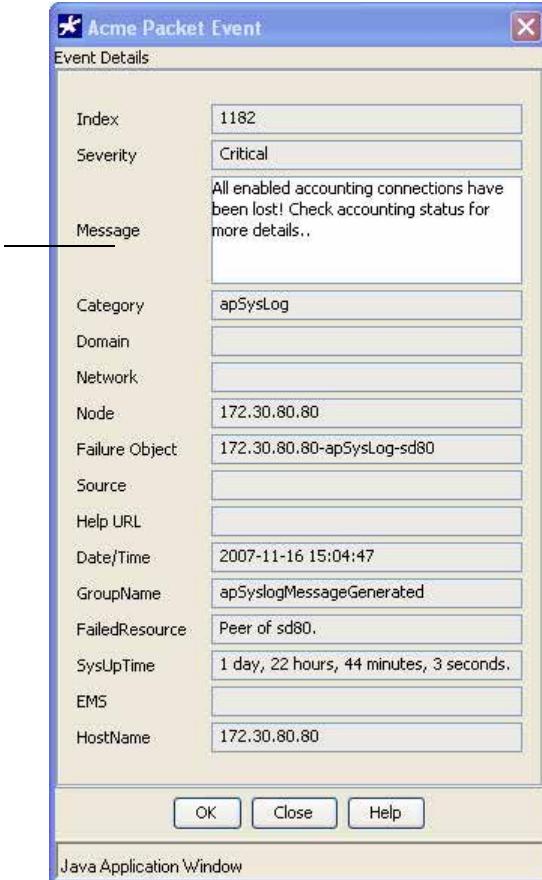
You can access details about the event.

To view event details:

1. Double-click the table row for the event you want to view.

The Event Details dialog box appears. For example:

Review the information



2. Review the information and click OK to close the dialog box.

The following table contains descriptions of the information in the dialog box.

| Event Category | Description |
|----------------|---|
| Index | Unique ID created for the generated event |
| Severity | Severity level of event: <ul style="list-style-type: none"> • Critical • Major • Minor • Clear • Warning • Info |
| Message | Message associated with the event |
| Category | Category to which the event belongs |

| Event Category | Description |
|-----------------|--|
| Domain | Domain-specific information which is based on the physical location, functional categorization, or logical categorization of the source of the event |
| Network | Network to which the event belongs |
| Node | Node to which the event belongs. For example, if the event is for an interface, the node value is specified as the interface parent node. |
| Failure Object | Specific entity in the source that has failed and is primarily responsible for the event |
| Source | Exact source of the event |
| Help URL | URL for locating the help documentation on clicking the Help button in the same dialog box |
| Date/Time | Date and time the event was generated |
| GroupName | Name of the group to which the event belongs |
| Failed Resource | Resource responsible for the event |
| SysUpTime | System's up time in hours, minutes, and seconds |
| EMS | Element Management System |
| HostName | Name of the host from which the alarm was generated |

Viewing Alarm Information

This section explains how to view information about alarms. Alarms play a significant role in determining overall health of the system. For additional information about alarms, see the *Acme Packet MIB Reference Guide*.

About Alarms

An alarm is triggered when a condition or event happens within either the Net-Net system's hardware or software. Alarms contain an alarm code, a severity level, a textual description of the event, and the time the event occurred.

Alarm Categories

The alarms displayed in the Net-Net EMS fall into the following categories:

| Category | Description |
|--------------|--|
| apSysLog | Associated with the proprietary Acme Packet ap-slog.mib, which provides a method of gathering syslog messages generated by the Net-Net system via SNMP |
| apSysMgmt | Associated with the proprietary Acme Packet ap-smgmt.mi, which provides a means of gathering information about the status of the Net-Net system |
| ARP capacity | Percentage of ARP table in CAM utilization. Associated with the apSysMgmtGroup trap. |
| AuthTrap | Associated with the standard authenticationFailure trap. The SNMPv2 agent received a protocol message that was not properly authenticated. |
| ColdStart | Associated with the standard coldStart trap. The SNMPv2 agent is reinitializing itself and its configuration may have been altered. |

| Category | Description |
|-----------------|--|
| CPU | Percentage of CPU utilization. Associated with the apSysMgmtGroupTrap. |
| Cpu load | CPU utilization percentage of application tasks has exceeded the threshold algd-load-limit. |
| Discovery | Discovery status. |
| DoS | Proprietary trap generated by Acme Packet Denial of Service protection |
| Gateway | Status of gateway reachability. Associated with the apSysMgmtGatewayUnreachableTrap trap. |
| EMS-HA | Generated by the Net-Net EMS in a Net-Net EMS failover situation |
| Enhanced DoS | A device exceeded configured thresholds and was denied access by the Net-Net SBC. |
| Fan | Fan unit speed fell below the monitoring level. |
| H323 Stack | Status of H.323 stack. Associated with the apSysMgmtH323InitFail trap. |
| HDR | Server specified becomes unreachable by the system collector. |
| Health | System health percentage. Associated with the apSysMgmtGroupTrap. |
| I2C | The Inter-IC bus (I2C) state changed from normal (1) to not functioning (7). |
| License | Associated with the proprietary Acme Packet ap-license.mib, which provides information about the status of your Net-Net licenses |
| Link | Associated with the standard linkDown and linkUp traps. <ul style="list-style-type: none"> linkDown: The SNMPv2 agent detects that the ifOperStatus object of an interface has transferred from the up state to the down state. The ifOperStatus value indicates the other state. linkUp: The SNMPv2 agent detects that the ifOperStatus object of an interface has transferred from the down state to the up state. The ifOperStatus value indicates the other state. |
| Media bandwidth | Bandwidth allocation failed at a percentage higher or equal to the system's default threshold rate. |
| Media ports | Port allocation failed at a percentage higher or equal to the system's default threshold rate. |
| Media realm | Status of media realm. Associated with the apSysMgmtMediaUnknownRealm trap. |
| Memory | Percentage of memory utilization. Associated with the apSysMgmtGroup trap. |
| Monitor | Associated with the proprietary Acme Packet ap-env-monitor.mib, which gathers information about fan speed, voltage, temperature, and power supply for the Net-Net system. It also sends out traps when status changes occur |
| NAT capacity | Percentage of NAT table (in CAM) utilization. |
| NTP Clock Skew | NTP had to adjust the clock by more than 1000 seconds. |
| NTP server | Specified NTP server became unreachable. |
| NTP service | All configured NTP servers are unreachable. |
| Polling | Generated by the Net-Net EMS to indicate ability to reach the Net-Net SBC. |

| Category | Description |
|------------------------|--|
| Power | Status of power supply. Associated with the apEnvMonStatusChangeNotification trap. |
| Realm Minutes Exceeded | Monthly minutes exceeded for a realm. |
| RADIUS Servers | Status of RADIUS server. |
| Reboot | Proprietary version of the standard coldStart trap |
| Redundancy | State change occurred on either the primary or secondary system in a redundant (HA) pair. |
| Save-config | Error occurred while the system was trying to save the configuration to memory. |
| Session agent | Session agent information that includes hostname, IP address, status, and the reason for the status. Associated with the apSysMgmtStatusChange trap. |
| Single unit redundancy | Status of a slot changed. The varbinds contain the new information for the slot. |
| Surrogate registration | Status of surrogate registration. Associated with the apSysMgmtSurrogateRegFailed trap. |
| Task | Indication of a suspended task. Associated with the apSysMgmtTaskSuspendTrap. |
| Temperature | System temperature. Associated with the apSysMgmtTempTrap trap. |

Alarm Severities

The following table lists the alarm severities.

| Alarm Severity | Description |
|----------------|--|
| Emergency | Requires immediate attention. If you do not attend to this condition immediately, there could be physical, permanent, and irreparable damage to your Net-Net system. |
| Critical | Requires attention as soon as it is noted. If you do not attend to this condition immediately, there may be physical, permanent, and irreparable damage to your Net-Net system. |
| Major | Functionality has been seriously compromised. As a result, this situation might cause loss of functionality, hanging applications, and dropped packets. If you do not attend to this situation, your Net-Net system will suffer no physical harm, but it will cease to function. |
| Minor | Functionality has been impaired to a certain degree. As a result, you might experience compromised functionality. There will be no physical harm to your Net-Net system. However, you should attend to this type of alarm as soon as possible in order to keep your Net-Net system operating properly. |
| Warning | Some irregularities in performance. This condition describes situations that are noteworthy, however, you should attend to this condition in order to keep your Net-Net system operating properly. For example, this type of alarm might indicate the Net-Net system is running low on bandwidth and you may need to contact your Acme Packet customer support representative to arrange for an upgrade. |

Default Alarm Severity Color Codes

The severity levels for the alarms are color coded with the following defaults. (You can change the defaults, see *Configuring Severity Color-Coding*.)

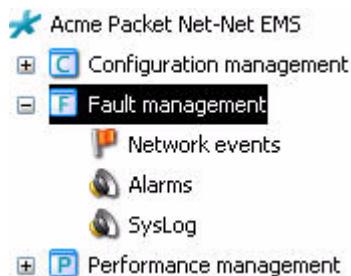
- red- emergency
- red - critical
- gold - major
- yellow - minor
- blue - warning
- green -clear

Remapping Alarm Severities

You can override the default severity levels for alarms.

To remap alarm severities:

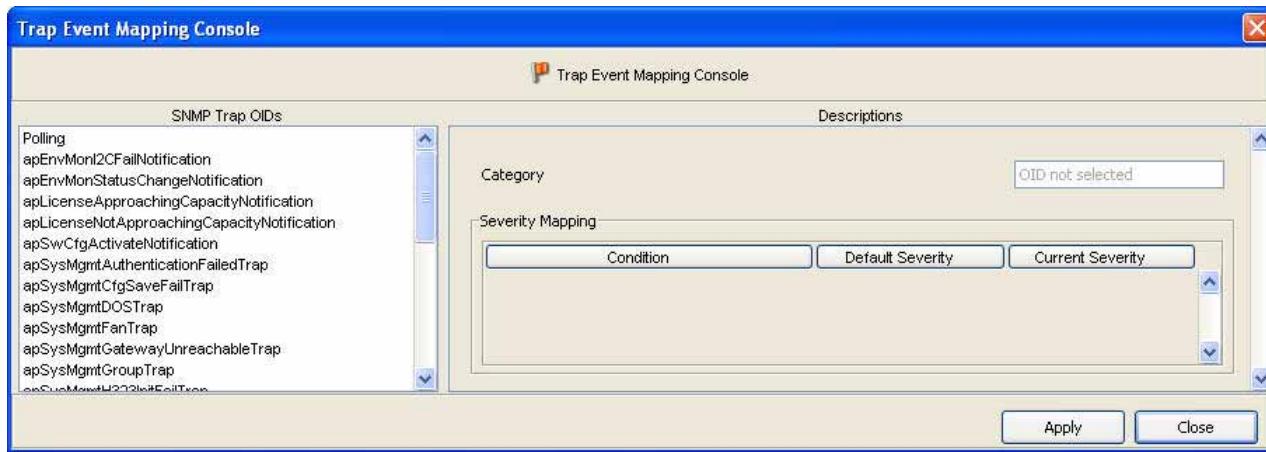
1. In the Navigation tree, click the plus sign (+) next to **Fault management** to expand it. For example:



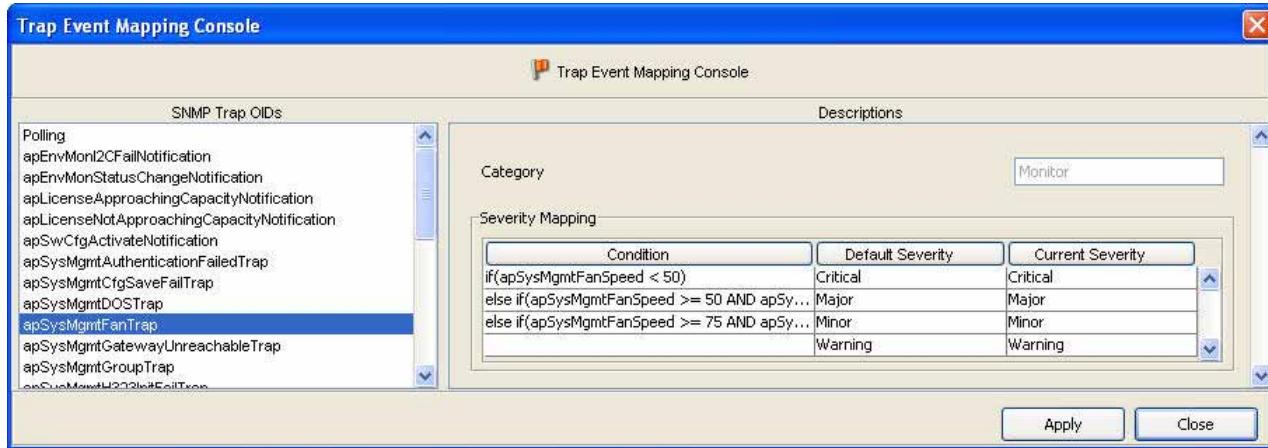
2. Right-click Network events to access the Trap Event Mapping option.



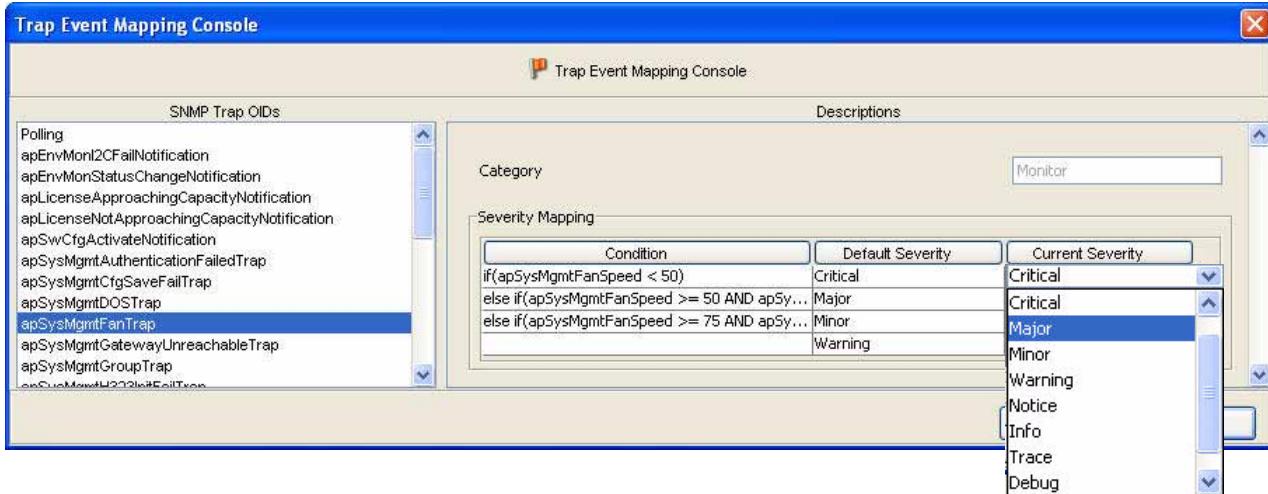
3. Click Trap Event Mapping. The Trap Event Mapping console appears:



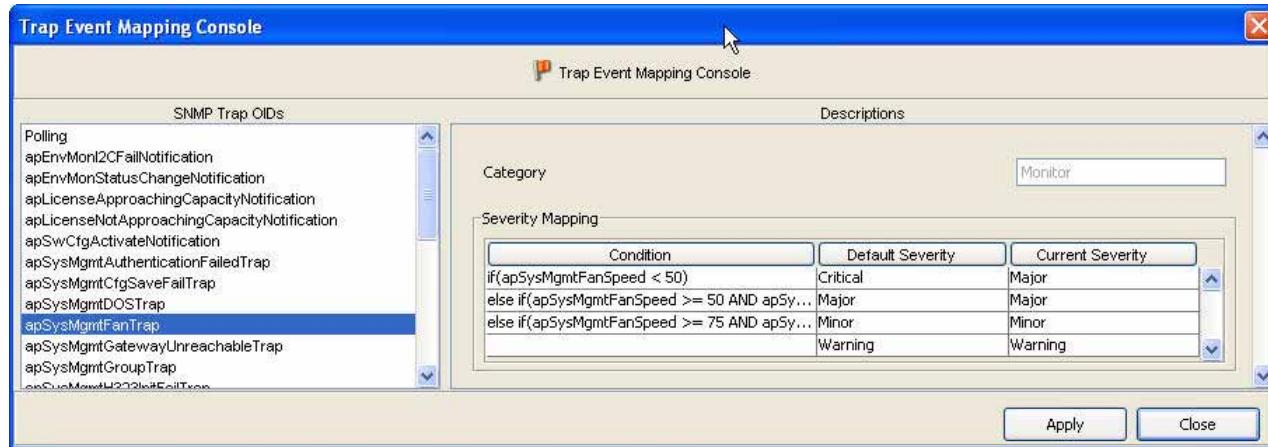
4. Choose the trap event you want to modify in the left pane. The information for that trap event appears in the Severity Mapping area.



5. Click the row of the condition you want to modify in the Current Severity column. A drop-down list of severity levels appears.



6. Click the new severity level in the drop-down list to select it. The new level appears in the Current Severity column.



7. Repeat for each condition you want to modify and click **Apply**. The new value will apply to all subsequent client displays.
 8. Repeat steps for each trap event you want to modify.

Alarm Count by Severity Table

You can access alarm information by using the Alarm count by severity table. (You can also access alarm information by choosing the Alarms option from the Fault Management category. See *Displaying the Alarm View* for details.)

The Alarm count by severity table displays a summary of all alarms generated, by alarm severity and by category. The table appears in the lower left pane of the Net-Net EMS GUI. The summary displays the number of alarms that are generated under various categories and severity levels. This table is automatically refreshed every 30 seconds.

Each row in the Alarm count by severity table corresponds to a specific category of alarms. The number of rows correspond to the number of alarm categories. The last row provides the total number of alarms for each severity level.

For example:

Each alarm severity level is represented by a color-coded column.

| | Critical | Minor | Clear | Alarm count by severity | | | | Category | | | | |
|---|-----------|-------|---------|-------------------------|-----|------|------|----------|----|----|---------------|-------------|
| | Emergency | Major | Warning | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 4 | Task |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | Discovery |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 2 | Temperature |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | H323 Stack |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | Memory |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | apSysLog |
| 0 | 0 | 4 | 0 | 0 | 0 | 0 | 38 | 0 | 42 | 42 | Link | |
| 0 | 0 | 0 | 0 | 0 | 1 | 7 | 0 | 0 | 8 | 8 | CPU | |
| 0 | 0 | 12 | 0 | 0 | 0 | 0 | 0 | 0 | 12 | 12 | ColdStart | |
| 0 | 0 | 2 | 0 | 0 | 0 | 0 | 10 | 0 | 12 | 12 | Health | |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | Media realm | |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 16 | 0 | 17 | 17 | Polling | |
| 0 | 0 | 13 | 0 | 0 | 0 | 0 | 0 | 0 | 13 | 13 | RADIUS Se... | |
| 0 | 0 | 0 | 0 | 0 | 819 | 535 | 1354 | 0 | 0 | 0 | Session agent | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | License | |
| 0 | 7 | 33 | 1 | 821 | 608 | 1470 | 0 | 0 | 0 | 0 | Total | |

Alarm categories listed here, when alarms are present. If no alarm is present, the category does not appear.

The Alarm count is based on the severity. When a new alarm is generated, the count is updated automatically and, if necessary, its category is added to the display.

You can click a table cell to display a list of alarms in the Alarm view, in the right pane. (See *Displaying the Alarm View* for details.) An asterisk appears in the cell to provide a visual cue as to which filter you have applied to the alarm display.

Viewing Alarms by Severity for a Specific Category

To view all alarms by category:

- Click the count corresponding to the specific category of the alarms you want to view.

For example, if you want to view all the Critical alarms for the asSyslog category, click the count in the red column and in the asSyslog row.

Click to view the critical alarms in the apSysLog category.

| Alarm count by severity | | | | | | | Category |
|-------------------------|---|---|---|---|---|---|-----------|
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | CPU |
| 0 | 0 | 0 | 0 | 0 | 2 | 2 | Link |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | ColdStart |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | Polling |
| 0 | 2 | 0 | 0 | 0 | 0 | 2 | apSysLog |
| 0 | 2 | 1 | 0 | 0 | 4 | 7 | Total |

An asterisk appears next to the count to provide a visual cue as to which filter you have applied to the alarm display. The Alarm view appears in the right pane, displaying the two Critical alarms that belong to the asSyslog category. For example:

Viewing All Alarms by Severity

You can view a list of all alarms that belong to a specific severity level.

To view all alarms by severity:

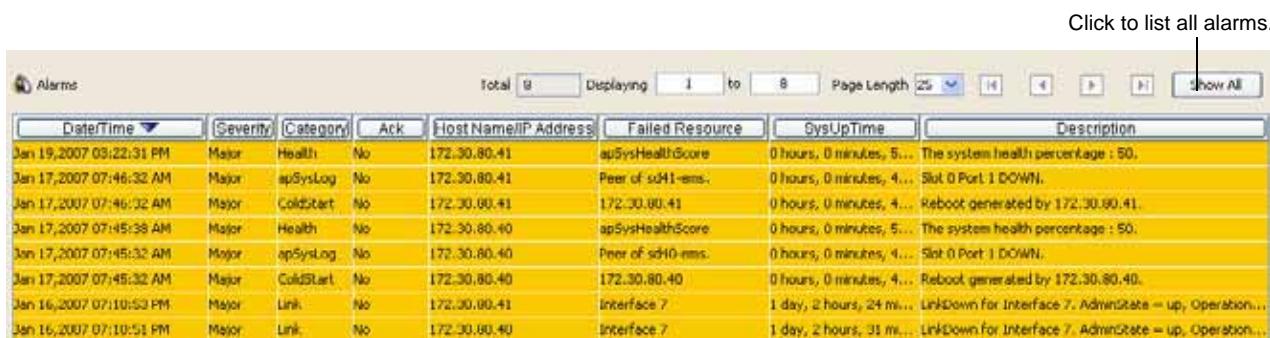
- From the Alarm count by severity table, click the count in the Total row that corresponds to the specific severity of the alarms you want to view.

For example, if you want to view all Major alarms (8 in the following example), click the count in the gold column and in the Totals row.

Click to view all Major alarms.

| Alarm count by severity | | | | | | | Category |
|-------------------------|---|---|---|---|---|---|-----------|
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | CPU |
| 0 | 0 | 0 | 0 | 0 | 2 | 2 | Link |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | ColdStart |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | Polling |
| 0 | 2 | 0 | 0 | 0 | 0 | 2 | apSysLog |
| 0 | 2 | 1 | 0 | 0 | 4 | 7 | Total |

An asterisk appears next to the count to provide a visual cue as to the type of alarms you are viewing. The Alarm view appears in the right pane, displaying all Major alarms. For example:



| Date/Time | Severity | Category | Ack | Host Name/ IP Address | Failed Resource | SysUpTime | Description |
|--------------------------|----------|-----------|-----|-----------------------|---------------------|--------------------------|---|
| Jan 19, 2007 03:22:31 PM | Major | Health | No | 172.30.80.41 | apSysHealthScore | 0 hours, 0 minutes, 5... | The system health percentage : 50. |
| Jan 17, 2007 07:46:32 AM | Major | apSysLog | No | 172.30.80.41 | Peer of sd41-msm... | 0 hours, 0 minutes, 4... | Slot 0 Port 1 DOWN. |
| Jan 17, 2007 07:46:32 AM | Major | ColdStart | No | 172.30.80.41 | 172.30.80.41 | 0 hours, 0 minutes, 4... | Reboot generated by 172.30.80.41. |
| Jan 17, 2007 07:45:38 AM | Major | Health | No | 172.30.80.40 | apSysHealthScore | 0 hours, 0 minutes, 5... | The system health percentage : 50. |
| Jan 17, 2007 07:45:32 AM | Major | apSysLog | No | 172.30.80.40 | Peer of sd40-msm... | 0 hours, 0 minutes, 4... | Slot 0 Port 1 DOWN. |
| Jan 17, 2007 07:45:32 AM | Major | ColdStart | No | 172.30.80.40 | 172.30.80.40 | 0 hours, 0 minutes, 4... | Reboot generated by 172.30.80.40. |
| Jan 16, 2007 07:10:53 PM | Major | Link | No | 172.30.80.41 | Interface 7 | 1 day, 2 hours, 24 mi... | LinkDown for Interface 7, AdminState = up, Operation... |
| Jan 16, 2007 07:10:51 PM | Major | Link | No | 172.30.80.40 | Interface 7 | 1 day, 2 hours, 31 mi... | LinkDown for Interface 7, AdminState = up, Operation... |

- Click Show All to display all alarms or click a different cell in the Alarm count by severity table to display a different set of alarms.

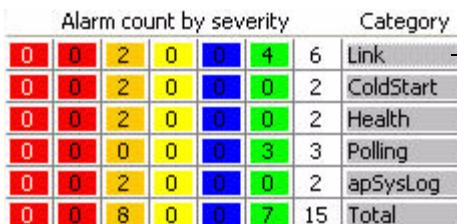
Viewing Alarms by Category

You can view a list of all alarms that belong to a specific severity level.

To view all alarms by severity:

- From the Alarm count by severity table, click the count in the Total row that corresponds to the specific severity of the alarms you want to view.

For example, if you want to view all Monitor alarms, click the Monitor cell in the Category column.



| Alarm count by severity | | | | | | | | Category |
|-------------------------|---|---|---|---|---|----|-----------|----------|
| 0 | 0 | 2 | 0 | 0 | 4 | 6 | Link | |
| 0 | 0 | 2 | 0 | 0 | 0 | 2 | ColdStart | |
| 0 | 0 | 2 | 0 | 0 | 0 | 2 | Health | |
| 0 | 0 | 0 | 0 | 0 | 3 | 3 | Polling | |
| 0 | 0 | 2 | 0 | 0 | 0 | 2 | apSysLog | |
| 0 | 0 | 8 | 0 | 0 | 7 | 15 | Total | |

Click to view all alarms for the Link category.

An asterisk appears next to the count to provide a visual cue as to the type of alarms you are viewing. The Alarm view appears in the right pane, displaying all alarms belonging to the Monitor category. For example:



| Date/Time | Severity | Category | Ack | Host Name/ IP Address | Failed Resource | SysUpTime | Description |
|--------------------------|----------|----------|-----|-----------------------|-----------------|--------------------------|--|
| Jan 17, 2007 08:51:31 AM | Clear | Link | No | 172.30.80.40 | Interface 4 | 1 hours, 6 minutes, 4... | LinkUp for Interface 4, AdminState = up, Operation st... |
| Jan 17, 2007 08:51:31 AM | Clear | Link | No | 172.30.80.40 | Interface 3 | 1 hours, 6 minutes, 4... | LinkUp for Interface 3, AdminState = up, Operation st... |
| Jan 17, 2007 07:44:32 AM | Clear | Link | No | 172.30.80.41 | Interface 4 | 0 hours, 13 minutes, ... | LinkUp for Interface 4, AdminState = up, Operation st... |
| Jan 17, 2007 07:44:32 AM | Clear | Link | No | 172.30.80.41 | Interface 3 | 0 hours, 13 minutes, ... | LinkUp for Interface 3, AdminState = up, Operation st... |
| Jan 16, 2007 07:10:53 PM | Major | Link | No | 172.30.80.41 | Interface 7 | 1 day, 2 hours, 24 mi... | LinkDown for Interface 7, AdminState = up, Operation... |
| Jan 16, 2007 07:10:51 PM | Major | Link | No | 172.30.80.40 | Interface 7 | 1 day, 2 hours, 31 mi... | LinkDown for Interface 7, AdminState = up, Operation... |

Click to list all alarms.

- Click Show All to display all alarms in the right pane or click a different cell in the Alarm count by severity table to display a different set of alarms.

Displaying the Alarm View

The Alarm view is a list of alarms that is displayed in the right pane. You can generate this list of alarms by:

- Clicking **Alarms** under the Fault Management function
- Clicking the **Totals** category in the Alarm count by severity table. You can also change what is displayed in the list of alarms by clicking cells in the alarm severity table.

The following example shows the Alarm view:

| Date/Time | Severity | Category | Ack | HostName/IP Address | Failed Resource | SysUpTime | Description |
|--------------------------|----------|-----------|-----|---------------------|------------------|--------------------------|--|
| Jan 23, 2007 03:13:58 PM | Clear | Polling | No | 172.30.80.40 | 172.30.80.40 | | Device 172.30.80.40 is reachable. |
| Jan 22, 2007 05:53:17 PM | Clear | Polling | No | 172.30.80.41 | 172.30.80.41 | | Device 172.30.80.41 is reachable. |
| Jan 19, 2007 03:22:31 PM | Major | Health | No | 172.30.80.41 | apSysHealthScore | 0 hours, 0 minutes, 5... | The system health percentage : 50. |
| Jan 17, 2007 09:51:21 AM | Clear | Link | No | 172.30.80.40 | Interface 4 | 1 hours, 6 minutes, 4... | LinkUp for Interface 4. AdminState = up, Operation st... |
| Jan 17, 2007 09:51:21 AM | Clear | Link | No | 172.30.80.40 | Interface 3 | 1 hours, 6 minutes, 4... | LinkUp for Interface 3. AdminState = up, Operation st... |
| Jan 17, 2007 07:46:32 AM | Major | apSysLog | No | 172.30.80.41 | Peer of sd41-ems | 0 hours, 0 minutes, 4... | Slot 0 Port 1 DOWN. |
| Jan 17, 2007 07:46:32 AM | Major | ColdStart | No | 172.30.80.41 | 172.30.80.41 | 0 hours, 0 minutes, 4... | Reboot generated by 172.30.80.41. |
| Jan 17, 2007 07:45:38 AM | Major | Health | No | 172.30.80.40 | apSysHealthScore | 0 hours, 0 minutes, 5... | The system health percentage : 50. |
| Jan 17, 2007 07:45:32 AM | Major | apSysLog | No | 172.30.80.40 | Peer of sd40-ems | 0 hours, 0 minutes, 4... | Slot 0 Port 1 DOWN. |
| Jan 17, 2007 07:45:32 AM | Major | ColdStart | No | 172.30.80.40 | 172.30.80.40 | 0 hours, 0 minutes, 4... | Reboot generated by 172.30.80.40. |
| Jan 17, 2007 07:44:32 AM | Clear | Link | No | 172.30.80.41 | Interface 4 | 0 hours, 13 minutes, ... | LinkUp for Interface 4. AdminState = up, Operation st... |
| Jan 17, 2007 07:44:32 AM | Clear | Link | No | 172.30.80.41 | Interface 3 | 0 hours, 13 minutes, ... | LinkUp for Interface 3. AdminState = up, Operation st... |
| Jan 16, 2007 07:10:53 PM | Major | Link | No | 172.30.80.41 | Interface 7 | 1 day, 2 hours, 24 mi... | LinkDown for Interface 7. AdminState = up, Operation... |
| Jan 16, 2007 07:10:51 PM | Major | Link | No | 172.30.80.40 | Interface 7 | 1 day, 2 hours, 31 mi... | LinkDown for Interface 7. AdminState = up, Operation... |
| Jan 16, 2007 12:01:44 PM | Clear | Polling | No | 172.30.80.127 | 172.30.80.127 | | Device 172.30.80.127 is reachable. |

The following table describes the information displayed in the list of alarms.

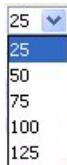
| Options | Description |
|----------------------|--|
| Date-Time | Date and time the alarm was generated |
| Severity | Current alarm severity level |
| Category | Category to which the alarm belongs |
| Ack | Whether an alarm has been acknowledged |
| Host name/IP address | Specific host name or IP address from which this alarm was generated |
| Failed Resource | Resource responsible for the alarm |
| SysUpTime | System's up time in hours, minutes, and seconds |
| Description | Description of the alarm |

Changing Number of Alarms on the Page

By default, 25 alarms are shown per page in the Alarm view.

To change the number of alarms displayed:

- At the top of the Alarms window, click the down arrow for **Page Length**. The drop down list of values appears.



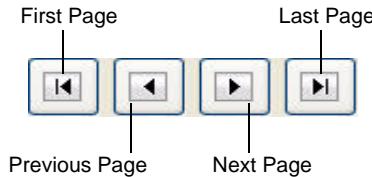
- Click the number you want to apply.

Navigating Pages

To navigate through multiple pages:

- Use the navigation arrows located at the top of the Alarms window to navigate through multiple pages.

Clicking navigation icons display the desired page, such as the first page, previous page, next page, and the last page of Alarms list view. For example



Sorting Alarms

By default, in the Alarms view the alarms are displayed in the order of precedence based on time and in descending order. This order can be changed using the **Sorting** option.

To sort alarms:

- In the Alarms view, click the column header for the column you want to change the sort order.

When you click the column header for the first time, the column is sorted in ascending order. Clicking the same column header again sorts the column in descending order. The up and down arrows in the headers indicate ascending and descending order respectively.

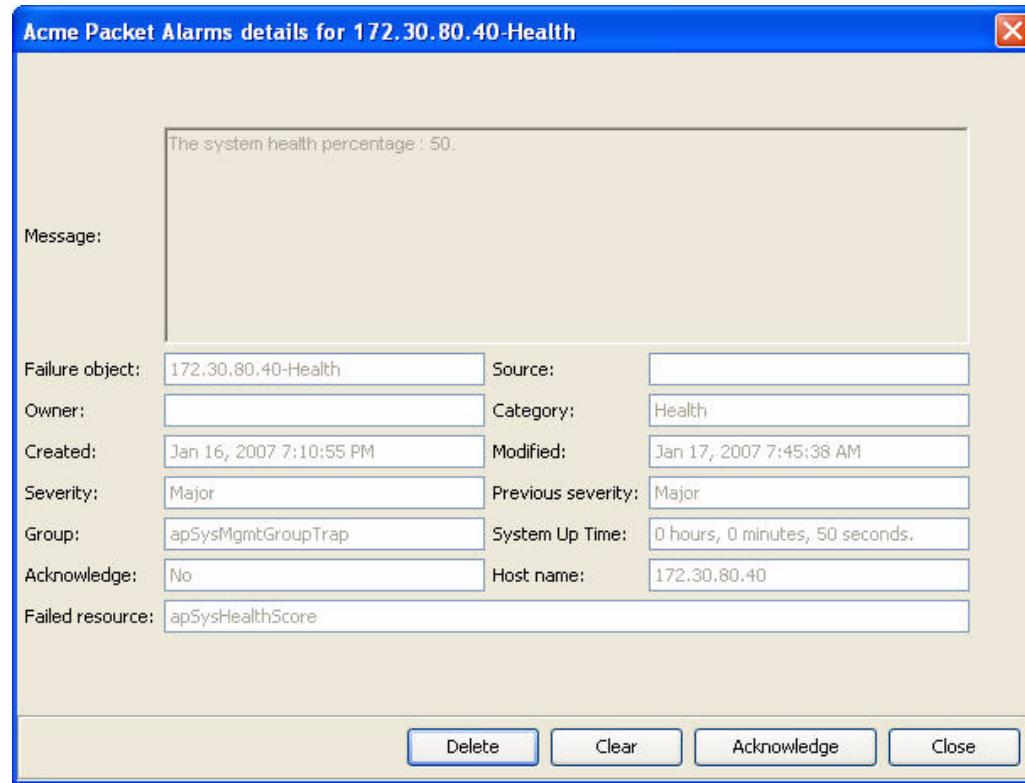
For example, if you need to sort the alarms based on its severity, click the **Severity** column header. This sorts the alarms based on its severity and the default order of precedence is Critical, Major, Minor, Warning, Clear, and info. For descending order of the same column, click the **Severity** column header again.

Viewing Alarm Details

You can view alarm details for a specific alarm.

To view alarm details:

- With the Alarm view displayed, double-click a row in the table to access alarm details. The Alarm details dialog box appears:



The following table describes the information displayed in the Alarm details window.

| Options | Description |
|----------------|---|
| Message | Message associated with the alarm |
| Failure object | Specific entity in the source that has failed and is primarily responsible for the alarm |
| Owner | Owner associated with the alarm |
| Created | Date and time the alarm was created |
| Severity | Current severity of alarm: <ul style="list-style-type: none"> • Emergency • Critical • Major • Minor • Warning • Clear |
| Group | Name of group to which the alarm belongs |

| Options | Description |
|-------------------|--|
| Acknowledge | Acknowledge an alarm. The alarm acknowledgment status is displayed on the Alarm view window. |
| Failed resource | Failed resource that generated the alarm |
| Source | Source of the alarm |
| Category | Category to which the alarm belongs |
| Modified | Date and time the alarm was last modified |
| Previous severity | Previous severity of the alarm |
| System Up Time | Length of time the system has been operational |
| Host name | Name of the host being managed |

Acknowledging Alarms

Users with the appropriate privileges can acknowledge alarms by clicking Acknowledge on the Alarms details window. When you acknowledge an alarm the Acknowledge, Owner, and Modified fields are updated. The Acknowledge button toggles to the Unacknowledge button.

Clearing Alarms

Users with the appropriate privileges can clear alarms by clicking Clear on the Alarms details window. The user is prompted to confirm clearing the alarm and the alarm severity is updated to Clear. If the Severity is Clear, the Clear and Acknowledge buttons are disabled.

Deleting Alarms

Users with the appropriate privileges can delete alarms by clicking Delete in the Alarms details window. The user is prompted to confirm deleting the alarm and the alarm is removed from the Net-Net EMS display and database for all Net-Net EMS users.

Configuring Alarm Email List

Net-Net EMS can trigger automatic e-mail notification when reporting alarms for certain severities. Users with the appropriate privileges can configure alarm e-mail addresses for each severity.

To configure an alarm email list:

1. Right-click Alarms in the Fault management area of the Net-Net EMS navigation pane.
2. Choose Alarm E-mail Console. The console appears.
3. Click the checkboxes of the alarm severities for which you want to attach an email address.
4. Enter up to six email addresses you want to attach to the alarm severity. Separate multiple email addresses with a comma.
5. Click **Apply**.

Using the Audible Alarm System

The Net-Net EMS audible alarm system lets you activate an audible alarm sound that will play when an alert (the trap event associated specifically with an alarm) is received by Net-Net EMS from a Net-Net SBC.

About the Audible Alarm System

The audible alarm system lets you associate sounds with the different alarm severity levels, and set the sound alarm frequency and number of repetitions. The audible alarm system provides the tools necessary for a Net-Net EMS client to interact with the sounding alarms. Once activated, the audible alarm system checks the alarm statistics during each configured cycle, looking for new or modified alarms. Once it detects alarms, it sends them for processing. Finally, it plays the sound wave for a specific alarm severity (if you have configured an alarm sound for that severity level).

Note: A delay of up to 5 seconds can sometimes occur between the time an alarm is updated on the screen and the time the alarm sounds. A discrepancy between the Net-Net EMS client and server system times, can increase the delay. Acme Packet recommends ensuring the system times are the same on both.

How the Audible Alarm System Works

You configure the audible alarm system to choose the alarm severity levels for which you want audible alarms to sound. You then activate the audible alarm system. Alarms detected after activation will cause the configured alarms to sound.

If alarms of different severity levels (for which you configured alarm sounds) are detected, only the alarm with the greater severity will sound. Alarm priorities from highest to lowest are critical, major, minor, warning.

About the Audio Files

The audible alarm system comes with four alarm sound.wav files. Each sound is specific to the severity it represents. You can find these files in the ADVENTNET_HOME/conf directory.

- Audio_Critical.wav: critical severity alarms
- Audio_Major.wav: major severity alarms
- Audio_Minor.wav: minor severity alarms
- Audio_Warning.wav: warning severity alarms

Substituting WAV Files

You can substitute your own .wav files for those supplied with Net-Net EMS.

1. Create an alarm sound wav file. For example, NewCriticalAlarm.wav.
2. In the ADVENTNET_HOME/conf directory, rename the existing Audio_Critical.wav to Original_Audio_Critical.wav to create a backup of the original file.
3. Copy the new wav file to the ADVENTNET_HOME/conf directory and rename it to Audio_Critical.wav.

The new critical alarm sound will now be played after you activate the audible alarm system.

Using the Audible Alarm Console

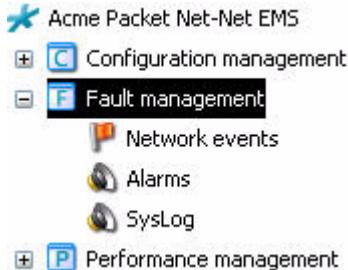
You activate, deactivate, and configure alarm sound characteristics through the Audible Alarm console. The configuration settings are only valid for the current session. When you exit the session, the alarm sound settings revert to the default values.

Note: If a time difference exists between the client and server systems, either the alarms do not sound or are not synchronized with the trap generator.

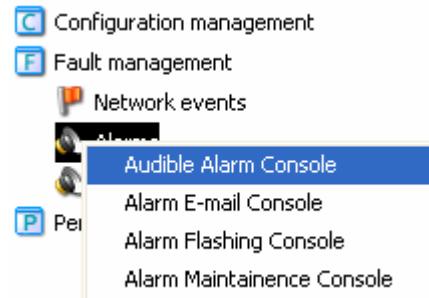
Accessing the Audible Alarm Console

To access the Audible Alarm console:

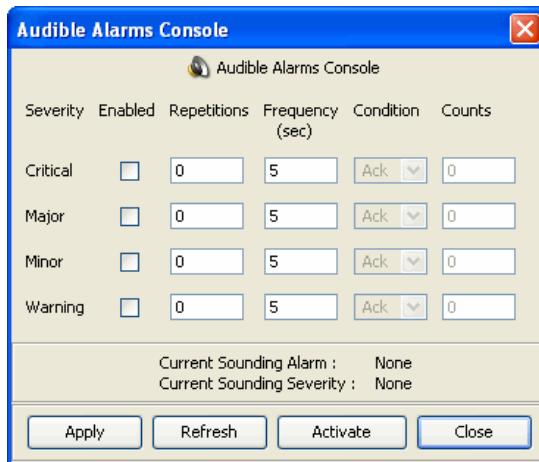
1. In the Navigation tree, click the plus sign (+) next to **Fault management** to expand it. For example:



2. Right-click Alarms to display the Audible Alarm Console option.



3. Click Audible Alarm Console to select it. The Audible Alarm Console appears.



Note: The Condition options are currently not supported.

Configuring Audible Alarms

After you enter your configuration values, you must click **Apply** to apply your configuration and then click **Activate** to active the Audible Audio Alarm console.

Note: Acme Packet recommends setting the frequency to accommodate the sounding time of the alarm .wav file chosen. You want to ensure the alarm sound plays in its entirety. For example, if a .wav file sound runs for 10 seconds, enter a value greater than 10 seconds, so that sound file plays completely.

To configure audible alarms:

1. Click the checkbox in the Enabled column for each alarm severity to which you want to associate an audible alarm.
2. Enter a value that represents the number of times the alarm will sound. Providing a number greater than zero causes the alarm sound to be repeated for the number of repetitions requested. For example, enter the number 10 to cause the severity alarm to sound 10 times and then stop.

The default value of zero (0) means that once a alarm sound starts, it will continue indefinitely until the end user stops it by either deselecting the checkbox and clicking Apply button, or clicking the Deactivate button to stop the audible alarm system.

3. Enter a value in seconds that represents the frequency of the alarm sound and accommodates the sounding time of the alarm .wav file chosen. The default value of 5 seconds means that the alarm sound plays every 5 seconds and the sounding time of the file is less than 5 seconds.

Note: Do not enter a value of 2 seconds or less for frequency.

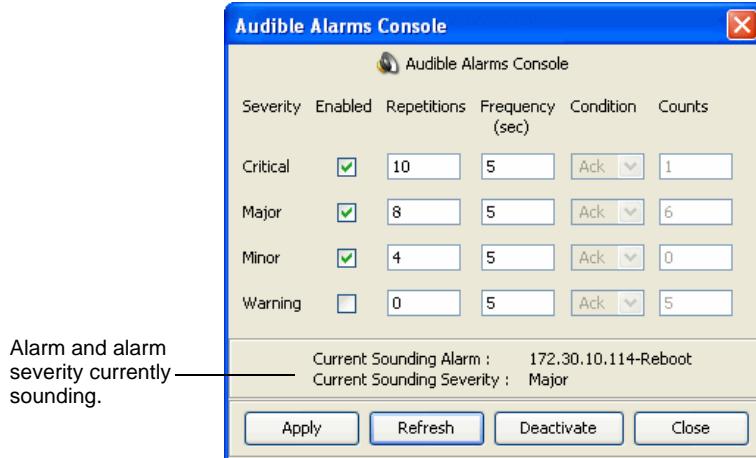
4. Click **Apply** to apply the values you entered.
5. Click **Activate** to start the audible alarm system. The button toggles to Deactivate. The next alarm detected that has been configured for an audible alarm, will cause the audible alarm to sound.

Viewing Alarm Information

You can click **Refresh** to display the most current valid configuration. Use Refresh if the Audible Alarms console has been active for a lengthy period of time to ensure the correct information is displayed.

The Count column displays the total number of alarms for each severity level currently in the system. The Audible Alarm console displays the counts after you activate the audible alarm system.

The console displays the name of the alarm sounding, as well as its severity. This information is not updated until you activate the audible alarm system and an alarm is sounding.



Note: If multiple alarms of the same severity are present and causing the alarm to sound, only one of those alarms is chosen at random and noted in the display.

Clearing the Audible Alarm

To clear the audible alarm:

1. Open the Audible Alarm console.
2. Perform one of the following:
 - Click **Deactivate** (recommended)
 - Deselect the Enabled checkbox for the specific alarm severity and click **Apply**.
3. Click **Close** to exit the console.

Alarm Handling

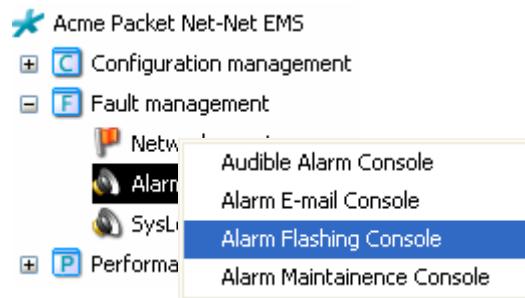
The information Net-Net EMS displays in the alarms table includes the severity level of the alarm (Severity column) and whether the alarm has been acknowledged (Ack column). The severity levels for the alarms are color coded, all Critical alarms are red, Major alarms are gold, and so on. (See *Viewing Alarm Information* in the *Net-Net EMS User Guide* for details about the alarm display.)

You can control the visual display of unacknowledged alarms by configuring alarm flashing based on severity level. Each alarm of the severity level you configure, has its entry in the Severity column continuously change from the assigned severity color to a white background, and back, at a specified interval. The alarm will flash until it is acknowledged, or you configure the flashing to stop.

Configuring Flashing Alarms

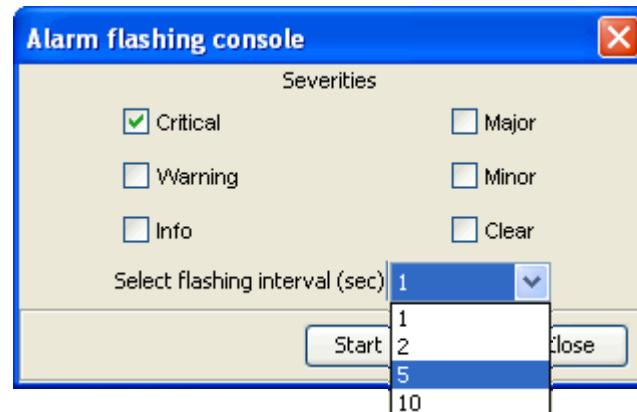
To configure flashing alarms:

1. Click the plus sign (+) next to Fault management in the navigation pane to expand it.
2. Right-click Alarms. A pop-up list of options appears.
3. Click Alarm Flashing Console to choose it.



The Alarm flashing console appears.

4. **Severities**—Choose the severity levels of the alarms you want to flash by clicking the checkboxes. For example, if you want alarms with the severity level of Critical to flash, click the Critical checkbox. You can choose any or all of the severity levels.
5. **Select flashing interval (sec)**—Choose the interval in seconds at which you want the alarms to flash from the drop-down list.



6. Click **Start Flashing**. The button toggles to **Stop Flashing**.
7. Click **Close**. The flashing starts immediately. The background color in the Severity column changes from its assigned color to white and back again for the specified interval. For example, the Critical alarm's red background has changed to white:

| Date/Time | Severity | Category | Ack | Host Name/IP Address | Failed Resource | SysUpTime | |
|--------------------------|----------|--------------|-----|----------------------|--------------------------|--------------------------|----------|
| Mar 27, 2007 04:45:01 PM | Critical | apSysLog | No | 172.30.10.114 | Peer of sd114. | 1 hours, 5 minutes, 4... | All |
| Mar 27, 2007 04:44:58 PM | Critical | apSysLog | No | 172.30.10.115 | Peer of sd115. | 2 hours, 14 minutes, ... | All |
| Mar 27, 2007 03:51:45 PM | Major | Gateway | No | 172.30.10.113 | gateway 4.4.4.4 unrec... | 0 hours, 48 minutes, ... | Gateways |
| Mar 27, 2007 03:43:46 PM | Warning | Session a... | No | 172.30.10.113 | sip-sa2 | 0 hours, 40 minutes, ... | SA |
| Mar 27, 2007 03:43:46 PM | Warning | Session a... | No | 172.30.10.113 | sip-sa1 | 0 hours, 40 minutes, ... | SA |
| Mar 27, 2007 03:43:46 PM | Warning | Session a... | No | 172.30.10.113 | sip-sa | 0 hours, 40 minutes, ... | SA |
| Mar 27, 2007 03:43:32 PM | Warning | CPU | No | 172.30.10.113 | apSysCPUUtil | 0 hours, 40 minutes, ... | The CPU |

Stopping Alarms from Flashing

You can stop the alarm flashing by using the Alarm flashing console or by acknowledging the alarm.

Using the Alarm Flashing Console

1. Access the Alarm flashing console.
2. Click **Stop Flashing**. The button toggles to **Start Flashing**.
3. Click **Close**.

Acknowledging Alarms

Users with the appropriate privileges can acknowledge alarms by clicking **Acknowledge** on the Alarms details window. When you acknowledge an alarm, the Acknowledge, Owner, and Modified fields are updated. The Acknowledge button toggles to the Unacknowledge button. (See *Viewing Alarm Details* in the Fault Management chapter of the *Net-Net EMS 6User Guide* for details.)

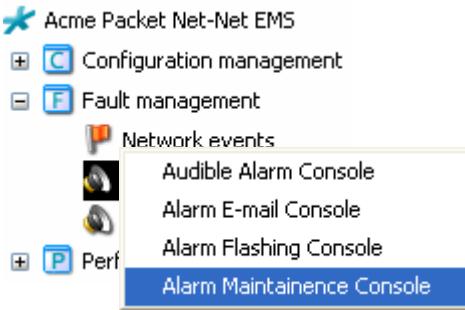
Saving and Deleting Selected Alarms

You can filter selected alarms to choose the ones you want to save or delete. You can select alarms using one, some, or all of the selection criteria. For example, you can select alarms for a specific IP address during a specified date-time range.

Configuring Alarm Selection

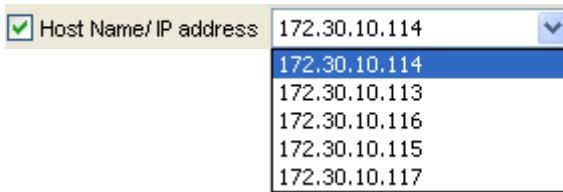
To configure alarm selection:

1. Click the plus sign (+) next to Fault management in the navigation pane to expand it.
2. Right-click Alarms. A pop-up list of options appears.
3. Click Alarm Maintenance Console to choose it.



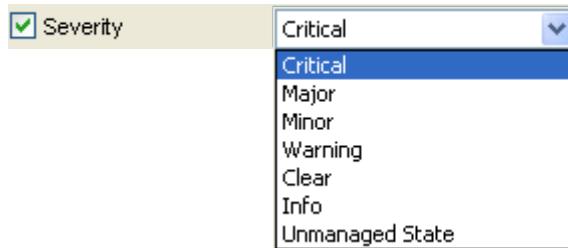
The Alarm maintenance console appears. Choose the alarm filtering method by clicking any or all of the checkboxes.

4. **Host Name/IP address**—Click the checkbox to select alarms based on hostname or IP address. The drop-down list is activated.
5. Choose the hostname or IP address from the drop-down list.

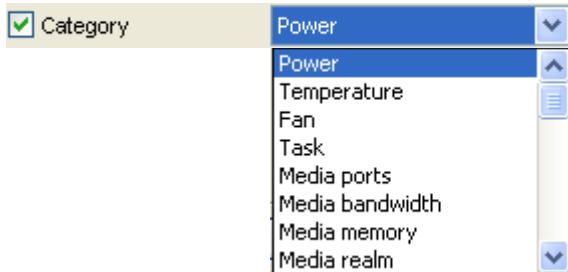


6. **Severity**—Click the checkbox to select alarms based on severity. The drop-down list is activated.

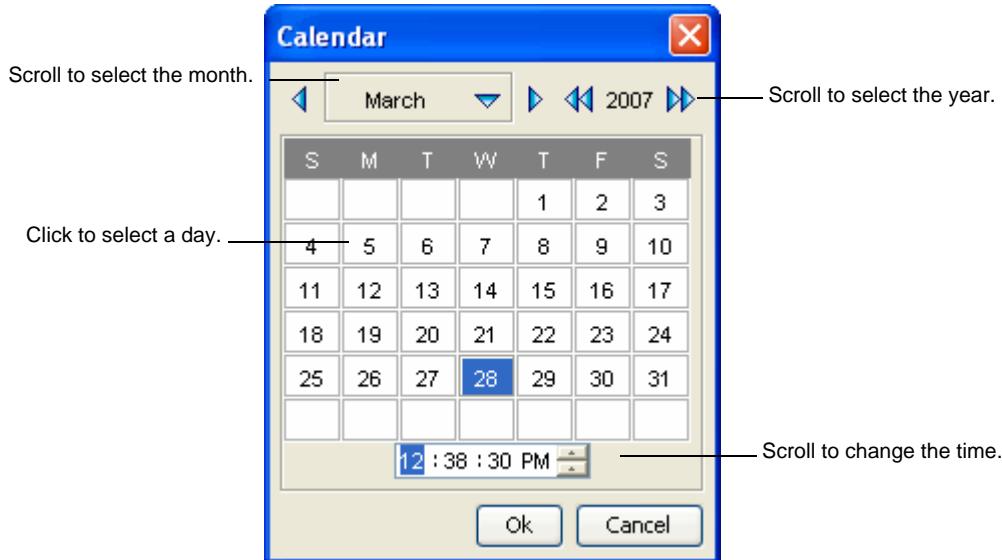
7. Choose the severity level from the drop-down list.



8. **Category**—Click the checkbox to select alarms based on category. The drop-down list is activated.
9. Choose the category from the drop-down list.

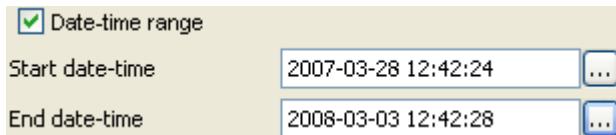


10. **Date-time range**—Click the checkbox to select alarms based on a date-time range. The Start date-time and End date-time textboxes are enabled.
11. **Start date-time, End date-time**—Click to access the Calendar:



12. Choose the month and the year by using the arrows to scroll to the needed options.
13. Choose the day by clicking the appropriate cell.
14. Choose the time by scrolling up or down in the time textbox.

15. Click **OK** to exit the Calendar and apply the values.



You can now save or delete alarms.

Saving Alarms

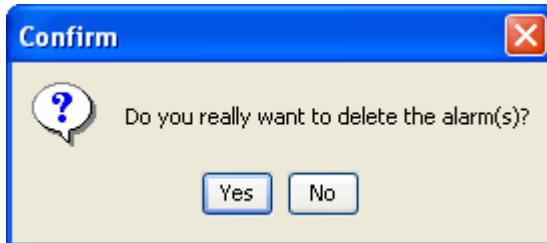
To save alarms:

1. In the Alarm maintenance console, click **Save**. You are prompted to save the alarms text file (.txt). The file name is Alarms-date time.txt. For example:
Alarms-2007-03-28 12-51-54.txt
2. Edit the default file name to change it.
3. Choose the location to which you want to save your alarm file.
4. Save the file.

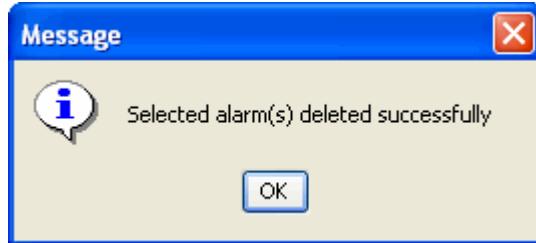
Deleting Alarms

To delete alarms:

1. In the Alarm maintenance console, click **Delete**. A confirmation message appears.



2. Click **Yes** to continue the deletion. A message that alarms were deleted successfully appears.



3. Click **OK**.

The alarms you selected for deletion are removed from the Alarms display.

Synchronizing Alarms

If you have administrator privileges, you can synchronize the alarms displayed by Net-Net EMS with those maintained on those Net-Net SBCs that support alarm synchronization:

- Net-Net SBC 4000 6.1 and later
- Net-Net SBC 3800 6.1.0M1 and later

You usually perform alarm synchronization when you discover a Net-Net SBC or after Net-Net EMS has reconnected after losing access to a Net-Net SBC.

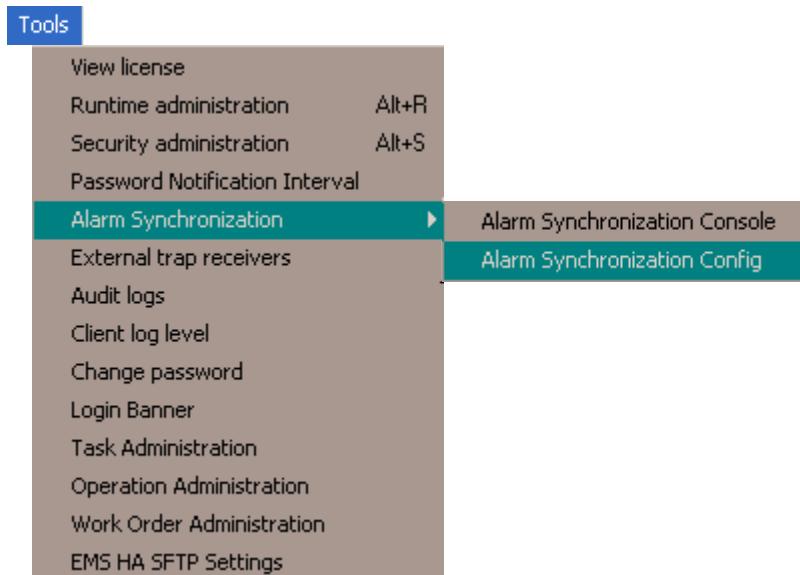
You can synchronize alarms:

- automatically for each Net-Net SBC you discover or reconnect to
- manually for one or more Net-Net SBCs using a console
- manually for one specific Net-Net SBC by accessing a right click option

Configuring Global Automatic Synchronization

To configure global automatic alarm synchronization:

1. Login to Net-Net EMS.
2. From the Tool menu, choose Alarm Synchronization, then Alarm Synchronization Config.



The Alarm Synchronization Configuration window appears.

3. Click the checkbox for one or both of the following:
 - **Enable alarm synchronization upon device discovery**—alarm synchronization occurs when Net-Net SBC is discovered

- **Enable alarm synchronization upon device reconnection**—alarm synchronization occurs when Net-Net SBC and Net-Net EMS regain connectivity



4. Click **OK**.

Synchronizing Alarms Using the Console

The console displays a table listing each Net-Net SBC in your Active configuration area that supports alarm synchronization currently by its IP address. The table also displays:

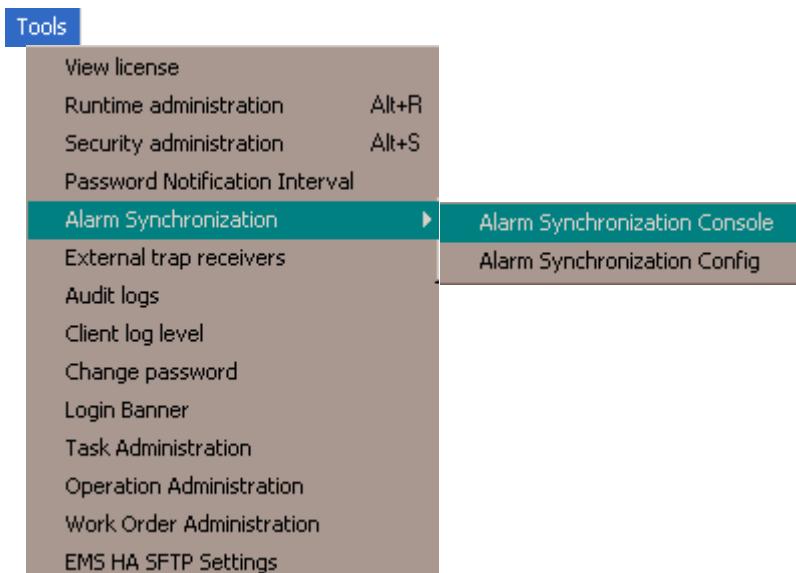
- when the alarm synchronization request was submitted
- time the synchronization started
- time the synchronization ended
- status of the alarm synchronization operation

You access the console and choose the managed device(s) for which you want to synchronize alarms or choose to synchronize alarms for all Net-Net SBCs listed in the table.

Accessing the Console

To access the console:

1. Login to Net-Net EMS.
2. From the Tool menu, choose Alarm Synchronization, then Alarm Synchronization Console



The Alarm Synchronization Console appears. The table displayed lists all managed Net-Net SBCs that support alarm synchronization listed under Active configurations .

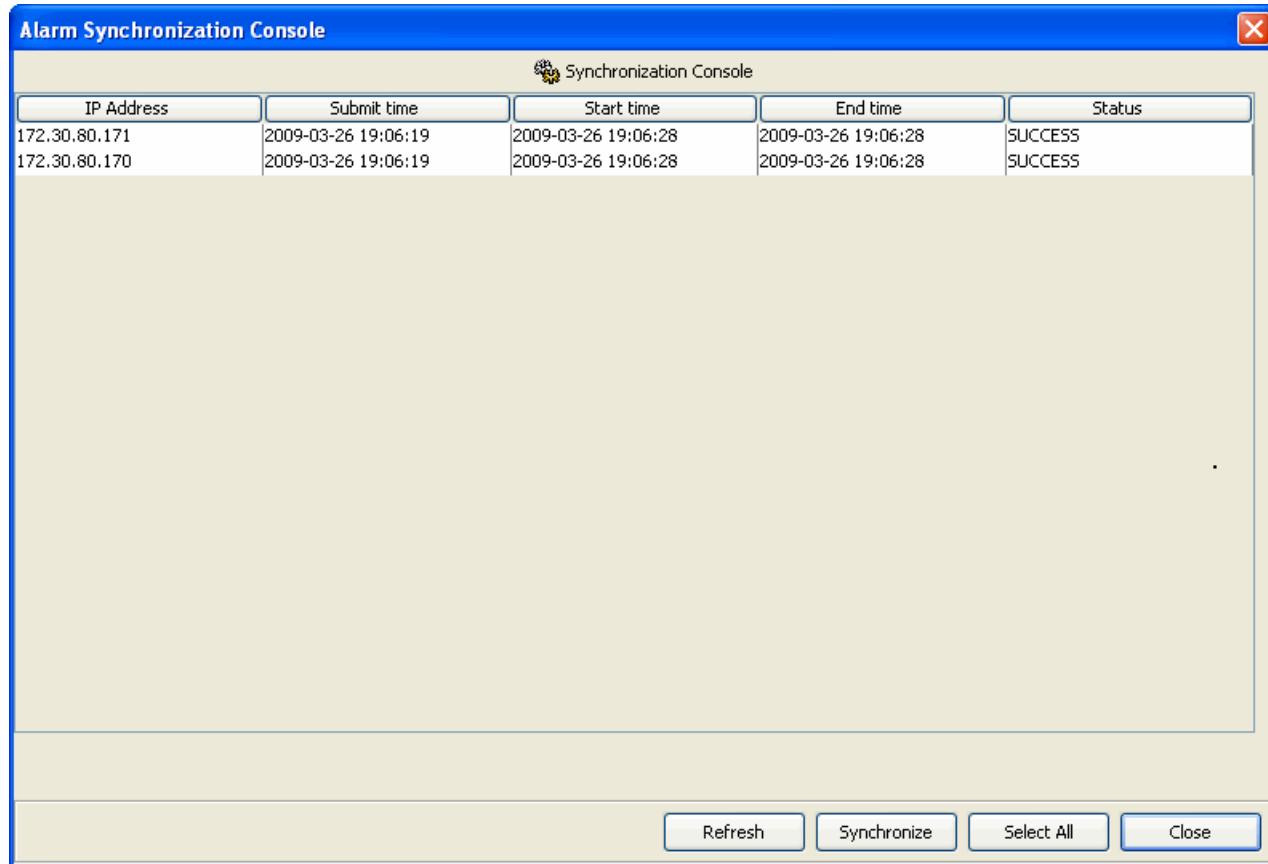
The screenshot shows a Windows application window titled "Alarm Synchronization Console". The window has a blue header bar with the title and a close button. Below the header is a toolbar with icons for Refresh, Synchronize, Select All, and Close. The main area is a table with the following data:

| IP Address | Submit time | Start time | End time | Status |
|---------------|-------------|------------|----------|--------|
| 172.30.80.100 | | | | |
| 172.30.80.70 | | | | |

The information displayed includes:

- IP Address column only displays information: alarm synchronization has not yet been performed on the Net-Net SBCs associated with the addresses
- Submit time and Start time columns display a value but End time column is blank: that Net-Net SBC is currently undergoing alarm synchronization

- All columns display values: alarm synchronization occurred at the time displayed. Any subsequent synchronizations update the information in the table.

**Single Net-Net SBC**

To synchronize alarms for one Net-Net SBC:

1. In the table, click the row for that Net-Net SBC and click **Synchronize**. The synchronize process begins.
2. Click **Refresh**. The columns in the table are populated with data.
3. Click **Close**.

All Net-Net SBCs

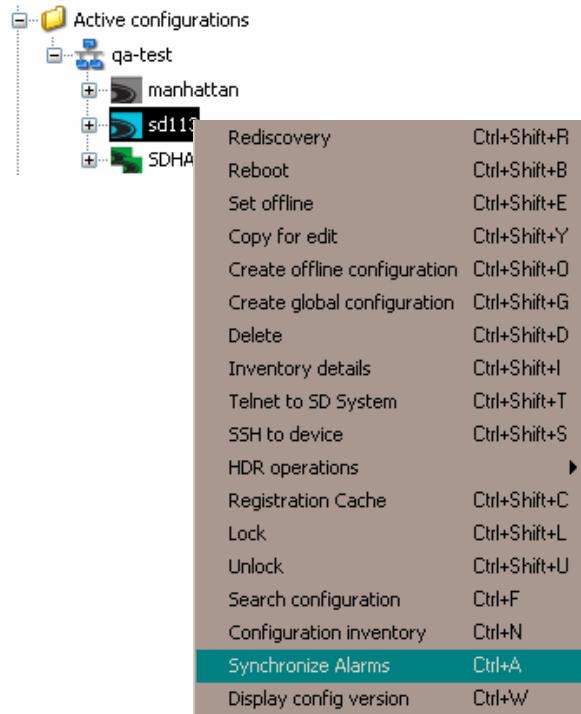
To synchronize alarms for all Net-Net SBCs:

1. Click **Select All**. Each row in the table is highlighted. The synchronize process begins for all Net-Net SBC listed in the table.
2. Click **Refresh**. The columns in the table are populated with data.
3. Click **Close**.

Manually Synchronize Alarms

To manually synchronize alarms:

1. Login to Net-Net EMS.
2. In the navigation pane, right-click the Net-Net SBC for which you want to synchronize alarms. A pop-up list of options appears.
3. Choose the Synchronize Alarms option



A message appears.



4. Click OK. The alarms for that Net-Net SBC are synchronized.

Viewing Syslog Information

This section explains how to view the syslog messages generated for the discovered devices. Each Net-Net SBC generates syslog messages. These message can be stored internally within the device or forwarded to an external entity. If the syslog server's IP address is set to 0.0.0.0, logs are stored internally within the device. If the IP address is set to an EMS server, the logs are saved in the database.

Syslog Message Example

The following example shows one of the possible syslog messages. For more information and additional examples, see the *Net-Net MIB Reference Guide*.

Hardware Monitor Failure Trap Example

The following is an example of an `apsyslogMessageGenerated` trap caused by the failure of the Net-Net system's environmental sensor. This generated a Critical-level alarm.

```
=====PACKET CAPTURED=====
DLC: Ethertype=0800, size=307 bytes
IP: D=[10.0.1.27] S=[10.0.2.233] LEN=273 ID=317
UDP: D=162 S=161 LEN=273
SNMP: ----- Simple Network Management Protocol (version 2) -----
SNMP:
SNMP: SNMP Version = 2
SNMP: Community     = public
SNMP: Command        = SNMPv2-trap
SNMP: Request ID    = 1
SNMP: Error status   = 0 (No error)
SNMP: Error index    = 0
SNMP:
SNMP: Object = {1.3.6.1.2.1.1.3.0} (sysUpTime.0)
SNMP: value  = 5145 hundredths of a second
SNMP:
SNMP: Object = {1.3.6.1.6.3.1.1.4.1.0} (internet.6.3.1.1.4.1.0)
SNMP: value  = {1.3.6.1.4.1.9148.3.1.2.0.1}
SNMP:
SNMP: value  = type
SNMP:
SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.5.1}
(enterprise.9148.3.1.1.2.3.1.5.1)
SNMP: Value = Hardware monitor failure! Unable to monitor fan speed and
temperature!
SNMP:
SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.6.1}
(enterprise.9148.3.1.1.2.3.1.6.1)
SNMP: value  = 50 (time ticks)
SNMP:
ADDR  HEX                                     ASCII
0000: 00 d0 09 6e a0 0c 00 08 25 01 00 70 08 00 45 00 | .D.n ...%..p..E.
0010: 01 25 01 3d 00 00 40 11 60 88 0a 00 02 e9 0a 00 | .%.=..@.^.~...é..
```

```

0020: 01 1b 00 a1 00 a2 01 11 fd 08 30 82 01 05 02 01 | ...j..¢..ý.0,....
0030: 01 04 06 70 75 62 6c 69 63 a7 81 f7 02 01 01 02 | ...public§÷....
0040: 01 00 02 01 00 30 81 eb 30 0e 06 08 2b 06 01 02 | .....0_ë0...+...
0050: 01 01 03 00 43 02 14 19 30 1a 06 0a 2b 06 01 06 | ....C...0...+...
0060: 03 01 01 04 01 00 06 0c 2b 06 01 04 01 c7 3c 03 | .....+....ç<.
0070: 01 02 00 01 30 1d 06 0f 2b 06 01 04 01 c7 3c 03 | .....0...+....ç<.
0080: 01 01 02 03 01 02 01 04 0a 61 63 6d 65 73 79 73 | .....acmesys
0090: 74 65 6d 30 14 06 0f 2b 06 01 04 01 c7 3c 03 01 | tem0...+....ç<..
00a0: 01 02 03 01 03 01 02 01 02 30 17 06 0f 2b 06 01 | .....0...+...
00b0: 04 01 c7 3c 03 01 01 02 03 01 04 01 04 04 74 79 | ..ç<.....ty
00c0: 70 65 30 59 06 0f 2b 06 01 04 01 c7 3c 03 01 01 | pe0Y...+....ç<...
00d0: 02 03 01 05 01 04 46 48 61 72 64 77 61 72 65 20 | .....FHardware
00e0: 6d 6f 6e 69 74 6f 72 20 66 61 69 6c 75 72 65 21 | monitor failure!
00f0: 20 55 6e 61 62 6c 65 20 74 6f 20 6d 6f 6e 69 74 | Unable to monit
0100: 6f 72 20 66 61 6e 20 73 70 65 65 64 20 61 6e 64 | or fan speed and
0110: 20 74 65 6d 70 65 72 61 74 75 72 65 21 30 14 06 | temperature!0..
0120: 0f 2b 06 01 04 01 c7 3c 03 01 01 02 03 01 06 01 | .+....ç<.....
0130: 43 01 32                                         | C.2

=====SAME PACKET RECEIVED BY SNMP TEST TOOL=====

Tue Nov 11 17:09:50 2003  SNMPv2c trap from [10.0.2.233]
    sysUpTime.0 :  (5145) type TimeTicks
    snmpTrapOID.0 : apSyslogMessageGenerated (1.3.6.1.4.1.9148.3.1.2.0.1)
    type ObjectID
        apSyslogHistFrom.1 :  (ACMEPACKET) type DisplayString, indexed by
        apSyslogHistIndex
        apSyslogHistLevel.1 :  (2) type SyslogLevel, indexed by
        apSyslogHistIndex
        apSyslogHistType.1 :  (type) type DisplayString, indexed by
        apSyslogHistIndex
        apSyslogHistContent.1 :  (Hardware monitor failure! Unable to monitor
        fan speed and temperature!) type DisplayString, indexed by
        apSyslogHistIndex
        apSyslogHistTimestamp.1 :  (50) type Timestamp, indexed by
        apSyslogHistIndex

```

Displaying Syslog Messages

By default the syslog message display is started and you can access the syslog message view. You can stop and re-start the syslog message display at any time.

To display the syslog view:

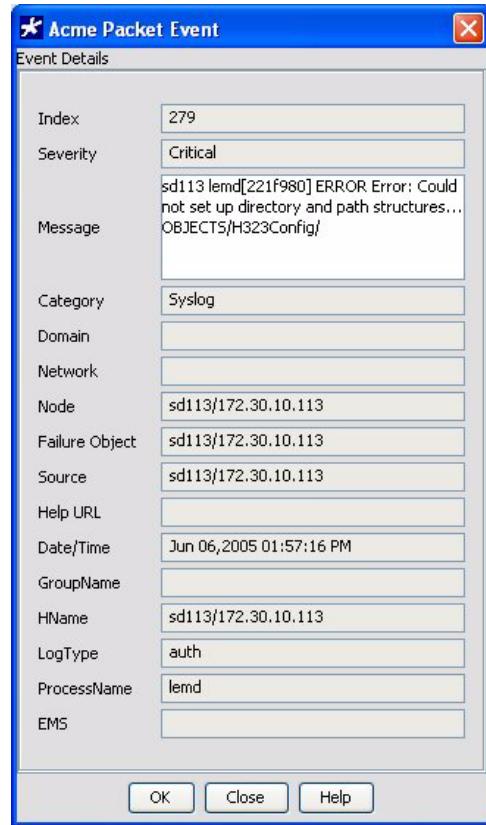
- Under the Fault Management category, click **sysLog**. The syslog view appears in the right pane. For example:

Viewing Details

You can view the details for a syslog message.

To view the syslog details:

1. In the SysLog view, double-click the row of the syslog message you want to view. The Event Details window appears:



2. Review the information and click **OK** to apply the changes and close the dialog box.

The following table contains descriptions of the information contained in the dialog box.

| Event Category | Description |
|-----------------------|--|
| Index | Unique ID created for the generated event |
| Severity | Severity level of event <ul style="list-style-type: none"> • All • Emergency • Critical • Major • Minor • Clear • Warning • Notice • Info • Trace • Debug |
| Message | Message associated with the event |
| Category | Category to which the event belongs |
| Domain | Domain-specific information which is based on the physical location, functional categorization, or logical categorization of the source of the event |
| Network | Network to which the event belongs |
| Node | Node to which the event belongs. For example, if the event is for an interface, the node value is specified as the interface parent node. |
| Failure Object | Specific entity in the source that has failed and is primarily responsible for the event |
| Source | Exact source of the event |
| Help URL | URL for locating the help documentation on clicking the Help button in the same dialog box |
| Date/Time | Date and time the event was generated |
| GroupName | Name of the group to which the event belongs |
| HName | Name of the host from which the alarm was generated |
| Log Type | Type of log |
| ProcessName | Name of the process that generated the log |
| EMS | |

Stopping Syslog Message Display

You can stop the display of syslog messages.

To stop the syslog message display:

- Under Fault Management, right-click **sysLog**. A list of options appears.
- From the list, click **Stop**. The Stop option toggles to Start option and the Confirm message appears:



- Click **Yes** to stop the syslog message display. The disabled successfully message appears.



- Click **OK** to clear the message.

Starting Syslog Message Display

To start the syslog message display:

- Under Fault Management, right-click **sysLog**. A list of options appears.
- From the list, click **Start**. The Start option toggles to Stop option and the Confirm message appears:



- Click **Yes** to start the syslog message display. The enabled successfully message appears.



- Click **OK** to clear the message.

Sorting Syslog Messages

By default, the syslog messages in the Syslog view are displayed in the order of precedence based on the Date/Time and in descending order. This order can be changed using the Sorting option.

To sort events:

1. In the Syslog view, click the column header for the column you want to change the sort order.

When you click the column header for the first time, the column is sorted in ascending order. Clicking the same column header again sorts the column in descending order. The up and down arrows in the headers indicate ascending and descending order respectively.

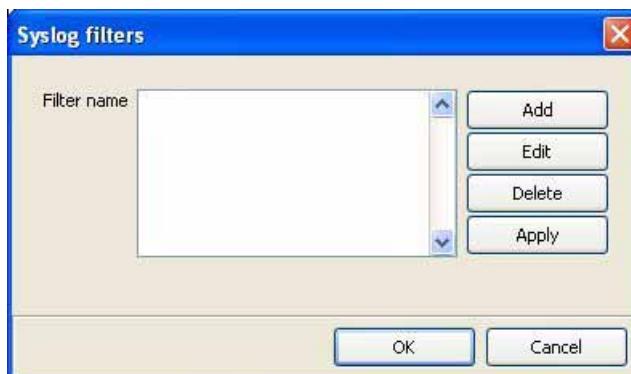
Filtering Syslog Messages

You can create filters to apply to the syslog view to focus on the syslog messages that meet specific criteria. That criteria can be as broad as filtering syslog messages on all severity levels or as narrow as filtering on severity level, date and time range, and process.

Accessing the Syslog Filter Dialog Box

To access the Syslog filters dialog box:

1. Under Fault Management, right-click **syslog**. A list of options appears.
2. Click **syslog filter** to select it. The Syslog filters dialog box appears:



Note: You can also choose **syslog filter** from the Display filter option in the toolbar.

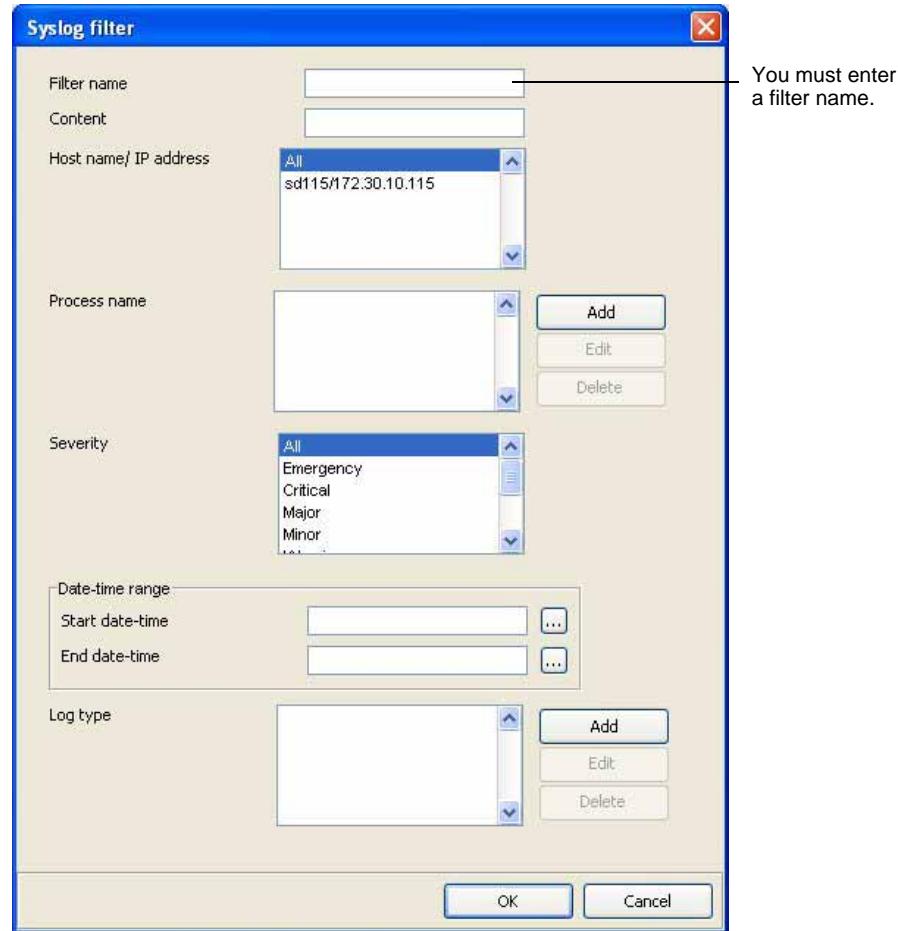
From here you can add or edit, then apply filters, as well as delete filters.

Adding New Syslog Filters

You can add new filters to use to filter the syslog messages.

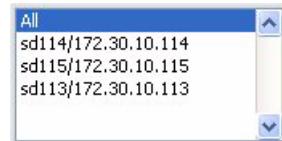
To add syslog filters:

1. Click Add. The Syslog filter dialog box appears:



From here you enter the criteria by which you want to filter the syslog messages. The only required information is a name for the filter. You can create a filter that operates on Content and Process name, or on Severity, or just on Host Name or IP address.

2. **Filter name**—*Required*. Enter a name for the filter. For example, filter1.
3. **Content**—Enter the text of the log message to filter by Content field. All messages that have Content fields that contain this text will be displayed.
4. **Host name/IP address**—Choose one or more host names or IP addresses (or all) from the list. All discovered Net-Net SBCs appear in the list. For example:



You can choose multiple values.

- Use CTRL+click to select multiple non-contiguous values
- Use SHIFT+click to select multiple contiguous values
- Click All to filter on all discovered Net-Net SBCs

All messages generated by the selected host names or IP addresses will be displayed.

5. **Process name**—Enter the name (or names of multiple processes) that generated the log.

- 5a. Click Add. The Process name dialog box appears:



- 5b. Enter the name of the process that generated the log. The following table lists the processes:

| Process | Description |
|-----------|--|
| algd | MGCP processes |
| berpd | Berpd process or the redundancy health process. Used for storing health messages and events and for determining whether a switchover is required. |
| brokerd | Platform-level processes, for example various host tasks related to communicating with the network processors and/or the CAM. Brokerd also forwards messages from the IP fragmenter, which currently takes part in the SIP NAT process, through sysmand to the acmelog (the overall system log). |
| cliTelnet | ACLI Telnet sessions, if your system access method is Telnet |
| console | ACLI console functions |
| h323d | H.323 processes |
| lemd | Local element manager (or local database server) processes, pertains to remote retrievals of and writing of configuration data |
| mbcd | Application flow manager processes, such as the creating, updating, and removing media NAT entries |
| radd | Accounting daemon for RADIUS. It serves as a RADIUS client to the outside world. Also serves as a place to concentrate RADIUS records from various signaling protocol tasks running on the Net-Net SBC. |

| Process | Description |
|---------|---|
| sipd | SIP process; how the Net-Net system's SIP proxy is processing messages |
| sysmand | System manager process, which is currently responsible for writing the system log (acmelog), dispatching commands to other application tasks, and starting the application-level code |

- 5c. Click OK.

The process name is added to the list and the Edit and Delete buttons are activated.

- 5d. Enter another process name following steps 5a through 5c or click Cancel. All process names appear in the list. For example:

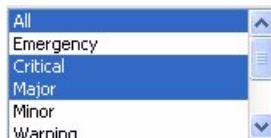


All messages that have the specified process names are displayed.

6. **Severity**—Choose the severity level from the drop-down list. You can choose multiple values.

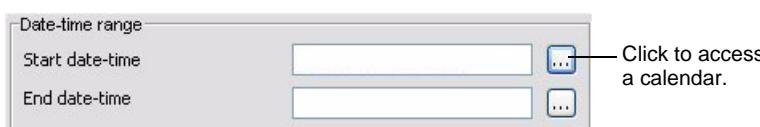
- Use CTRL+click to select multiple non-contiguous values
- Use SHIFT+click to select multiple contiguous values
- Click All to include all severity levels

For example:

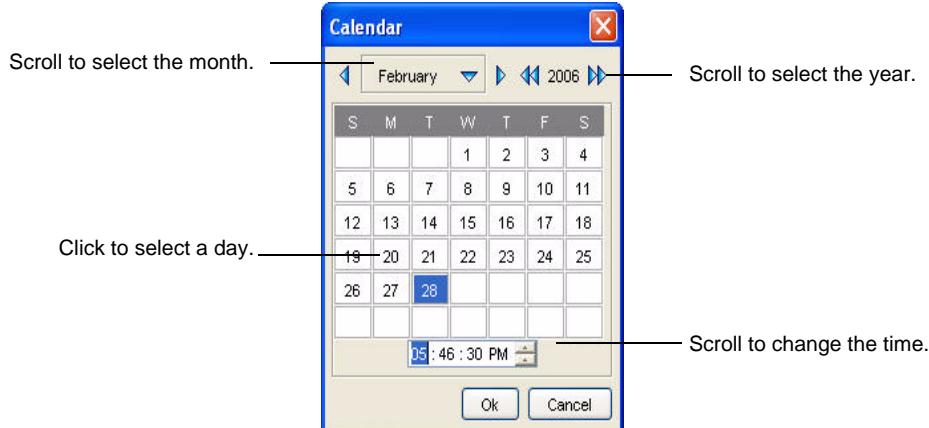


7. **Date-time range**—Enter the start date and time and end date and time.

- 7a. **Start date-time** and **End date-time**—Click the box next to the textboxes to access a calendar. For example:



The Calendar appears:



- 7b. Choose the month, and the year, for the date by scrolling to the month and year you need.
- 7c. Choose the day by clicking the appropriate cell.
- 7d. Choose the time by scrolling up or down in the time textbox.
Only syslog messages within that date-time range will be displayed.
8. **Log type**—Add the log types upon which you want to filter.

- 8a. Click **Add**. The Log type dialog box appears:



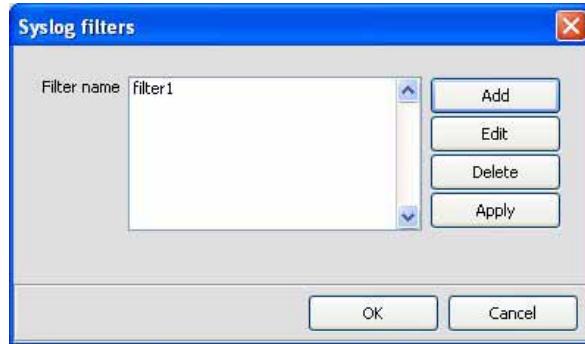
- 8b. Enter the text that identifies the log type.
- 8c. Click **OK**.
The log type is added to the list and the Edit and Delete buttons are activated.
- 8d. Enter another log type following steps 8a through 8c or click **Cancel**. All log types appear in the list. For example:



- 8e. Choose the log types from the list for which you want to filter.
 - Use CTRL+click to select multiple non-contiguous values
 - Use SHIFT+click to select multiple contiguous values
 - Click **all** to include all log types

All messages for those specified log types are displayed.

9. After you enter all filter criteria, click **OK**. The filter name appears in the Syslog filters list:



10. Click the filter name to select it and click **Apply**. The Confirmation screen appears:



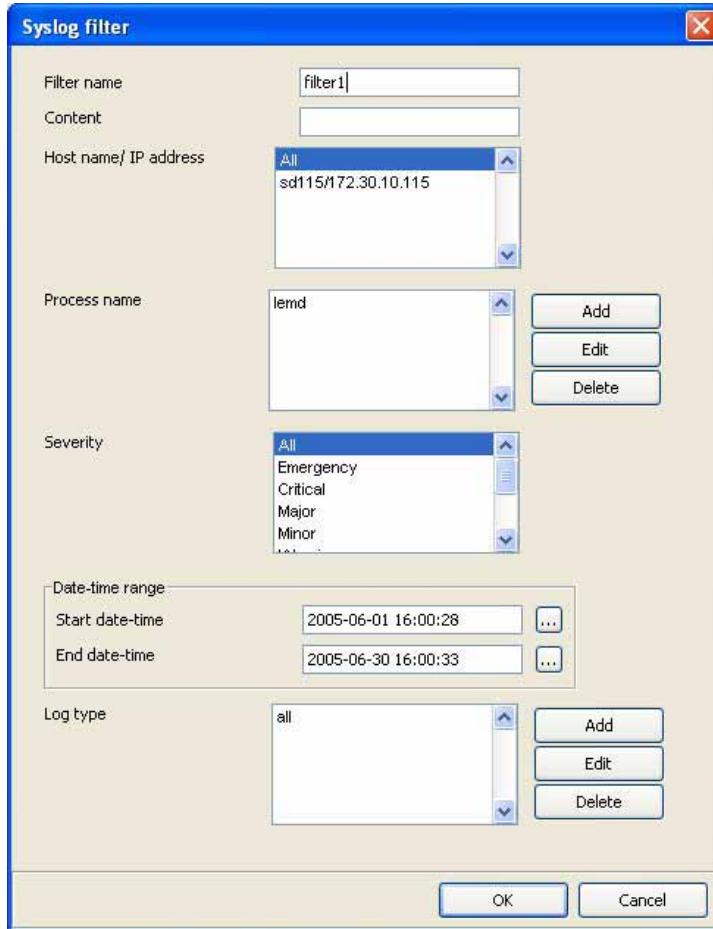
11. Click **Yes** to apply the filter.

Editing Syslog Filters

You can edit an existing filter to change or add filtering criteria.

To edit syslog filters:

1. Click **Edit**. The Syslog filter dialog box appears:

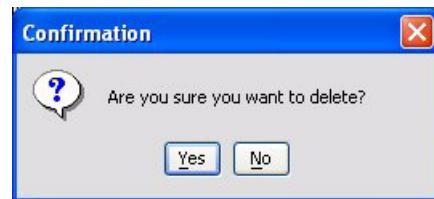


2. Follow the instructions in *Adding New Syslog Filters* to edit or add criteria.

Deleting Filters

To delete filters:

1. In the Syslog filters list, click the name of the filter you want to delete.
2. Click **Delete**. A confirmation message appears:



3. Click **Yes** to delete the file.

Viewing Registration Cache Information

You can use Net-Net EMS to access the registration cache for the SIP, H.323, and MGCP protocols to query and clear entries. You can run an endpoint audit to determine if endpoints are reachable and able to respond to signaling messages.

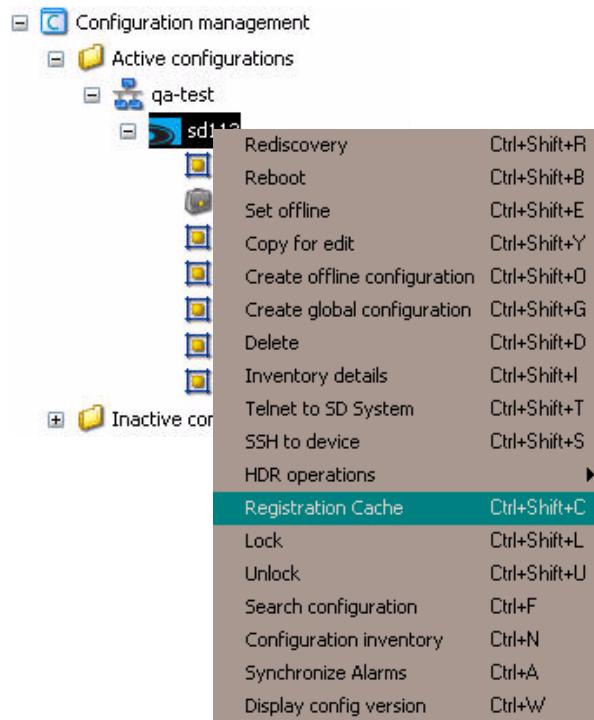
How It Works

You can query and clear entries in each cache using predefined grouping methods among others. You can group cache entries by user (endpoint) or IP address range.

Accessing the Registration Cache

To access the registration cache:

1. In the Active configurations area, right click a Net-Net SBC. A pop-up list of options appears
2. Choose Registration Cache..



The Registration Cache window appears. You can view, audit, and clear registration cache information for SIP, MGCP, and H.323 protocols.

Working with SIP Registration Caches

To display the SIP registration caches:

1. In the Cache Type area, click SIP.



The SIP commands and registration cache table appear. From here you can show, clear, and audit.

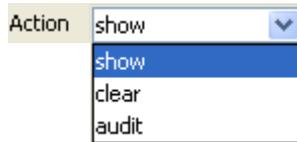
IP Address

Displays the Net-Net SBC's SIP process registration cache for a specified IP address. The IP address value can be a single IP address, a wildcarded IP address value that has an asterisk (*) as its final character, or just the asterisk itself as the wildcard.

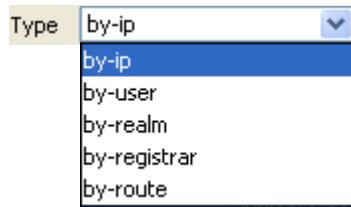
Note: This command is only available if you configure the reg-via-key option in the SIP interface prior to endpoint registration. The reg-via-key option keys all registered endpoints by IP address and username.

To display the SIP process registration cache for an IP address.

1. Action—Choose show from the Action drop-down list.



2. Type—Choose by-ip from the Type drop-down list.



3. Expression—Enter the IP address value or an IP address range in the form n.n.n.n/nn in the Expression textbox. You can use the asterisk as a wildcard.

Expression 111.222.33.*

4. Click **Apply**. The Apply button grays out while Net-Net EMS processes the command. A message is displayed in the Command status textbox once processing completes and the Cache table displays the results (if any).

You can view the known details of the cache table entries. See Viewing Registration Cache Details for step-by-step instructions.

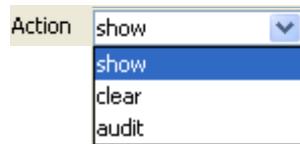
Users

Displays the Net-Net SBC's SIP process registration cache for a specified phone number or for a user name. The <endpoint> portion of the command you enter depends on how the SIP endpoint is registered. For example, an endpoint might be registered as 7815551234@10.0.0.3 or as username@10.0.0.3. The value preceding the at-sign (@) is what you enter for the <endpoint>.

The phone number can be a single number (such as 7815551234) or a single number wildcarded by placing an asterisk (*) (such as 7815551*) at the end of the phone number. The user name can be a single name (such as user), or a single name wildcarded by using an asterisk at the end of the user name (such as us*).

You can prefix the expression with sip: or sips: to specify whether the search for the endpoint should be over the secure connection (TLS) or not.

1. **Action**—Choose show from the Action drop-down list.



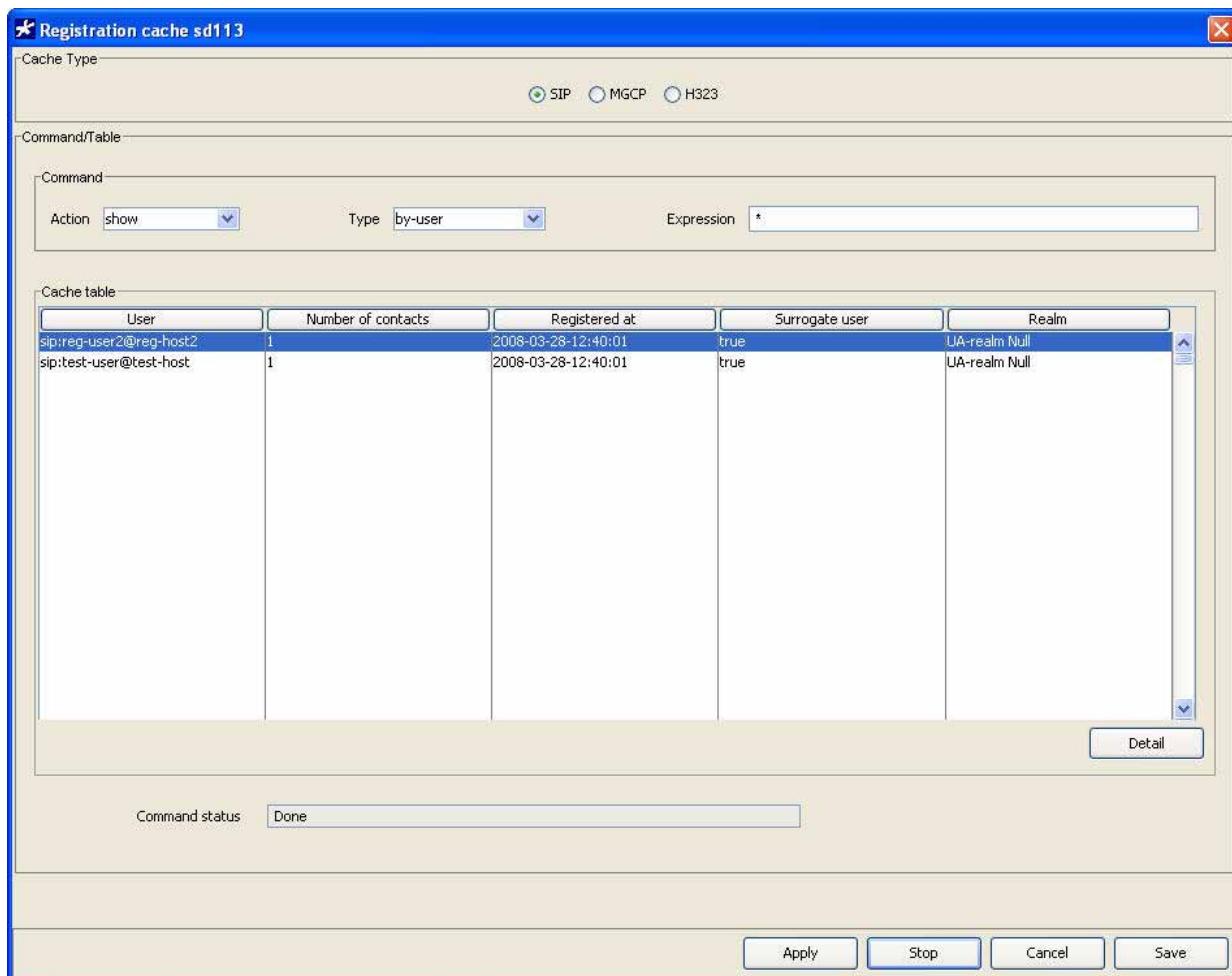
2. **Type**—Choose by-user from the Type drop-down list.



3. **Expression**—Enter the user name or phone number in the Expression textbox. You can use the asterisk as a wildcard.

| | |
|------------|---|
| Expression | * |
|------------|---|

- Click **Apply**. The Apply button grays out while Net-Net EMS processes the command. A message is displayed in the Command status textbox once processing completes and the Cache table displays the results (if any).



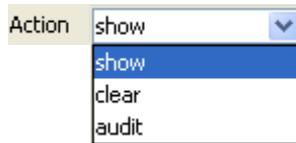
You can view the known details of the cache table entries. See Viewing Registration Cache Details for step-by-step instructions.

Realm

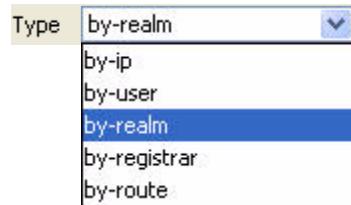
Displays the calls that have registered through a specified ingress realm. The output is sorted alphabetically by the realm name which will be shown first in the output.

To display the SIP process registration cache for a realm:

- Action—Choose show from the Action drop-down list.



2. **Type**—Choose by-realm from the Type drop-down list



3. **Expression**—Enter the name of the realm whose registration cache information you want to view or use the asterisk as a wildcard.

Expression: access

4. Click **Apply**. The Apply button grays out while Net-Net EMS processes the command. A message is displayed in the Command status textbox once processing completes and the Cache table displays the results (if any).

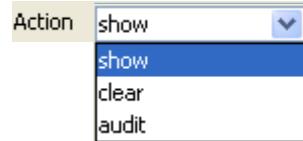
You can view the known details of the cache table entries. See Viewing Registration Cache Details for step-by-step instructions.

Registrar

Displays formation for calls that use a specific registrar.

To display the SIP process registration cache for a registrar:

1. **Action**—Choose show from the Action drop-down list.



2. **Type**—Choose by-register from the Type drop-down list



3. **Expression**—Enter the IP address of the registrar whose registration cache information you want to view or use the asterisk as a wildcard

Expression: 111.222.33.*

4. Click **Apply**. The Apply button grays out while Net-Net EMS processes the command. A message is displayed in the Command status textbox once processing completes and the Cache table displays the results (if any).

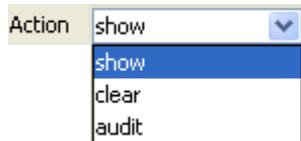
You can view the known details of the cache table entries. See Viewing Registration Cache Details for step-by-step instructions.

Route

Display information for calls by their Internet-routable IP address. This allows you to view the endpoints associated with public addresses.

To display the SIP process registration cache for a route:

1. Action—Choose show from the Action drop-down list.



2. Type—Choose by-route from the Type drop-down list



3. Expression—Enter the IP address whose registration cache information you want to view or use the asterisk as a wildcard

Expression 111.222.33.*

4. Click **Apply**. The Apply button grays out while Net-Net EMS processes the command. A message is displayed in the Command status textbox once processing completes and the Cache table displays the results (if any).

You can view the known details of the cache table entries. See Viewing Registration Cache Details for step-by-step instructions.

Command Status

The Command status textbox displays the commands you issue. For example:

| | |
|----------------|-----------------------------|
| Command status | No matching entires found ! |
|----------------|-----------------------------|

Viewing Registration Cache Details

You can right-click an entry in the Cache table or click a row to select it and then click Detail to access additional details. The Registration cache entry details window appears.

Registration cache entry details

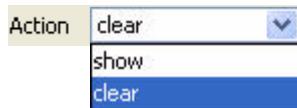
| | |
|---------------------------|-------------------------|
| Protocol | sipd |
| User | sip:test-user@test-host |
| Number of contacts | 1 |
| Surrogate user | true |
| Number of Active sessions | 0 |
| User bandwidth | 0 |
| Lifetime | 2007-09-06-12:05:47 |
| Contact | sip:test-user@test-host |
| Valid | false |
| Challenged | false |
| Lifetime | 2007-09-06-12:05:47 |
| Last registered | 2007-09-06-12:05:47 |
| State | expired |
| UA contact | sip:test-host |
| Transport | none |
| Secure | false |
| UA realm | core |
| SBC contact | sip:7.8.9.10@3.4.5.6 |
| REG realm | acme |

OK

Clearing the SIP Registration Cache

To clear the SIP process registration cache:

- Action—Choose clear from the Action drop-down list.



- Type—Choose all or by-user from the Type drop-down list.



- all**—Clears all SIP registrations in the cache
- by-user**—Clears the Net-Net SBC's SIP process registration cache of a particular phone number or user name

Note: You cannot wildcard values for commands to clear the SIP registration cache.

- Expression—If clearing by user, enter a phone number or a user name.
- Click **Apply**.

Auditing the SIP Registration Cache

To audit the SIP process registration cache:

- Action—Choose audit from the Action drop-down list.
- Type—Choose by-ip or by-user from the drop-down list.
 - by-ip**—Audits a specified IP address in the SIP registration cache.
 - by-user**—Audits a specific user by specifying the user name or phone number in the SIP registration cache.

Note: Note that you cannot wildcard values for commands to audit the SIP registration cache. Expired entries are automatically cleared.

- Expression—Enter an IP address for or phone number or a user name.
- Click **Apply**.

Working with the H.323 Registration Cache

To work with H.323 registration caches:

- In the Cache Type area, click H323.

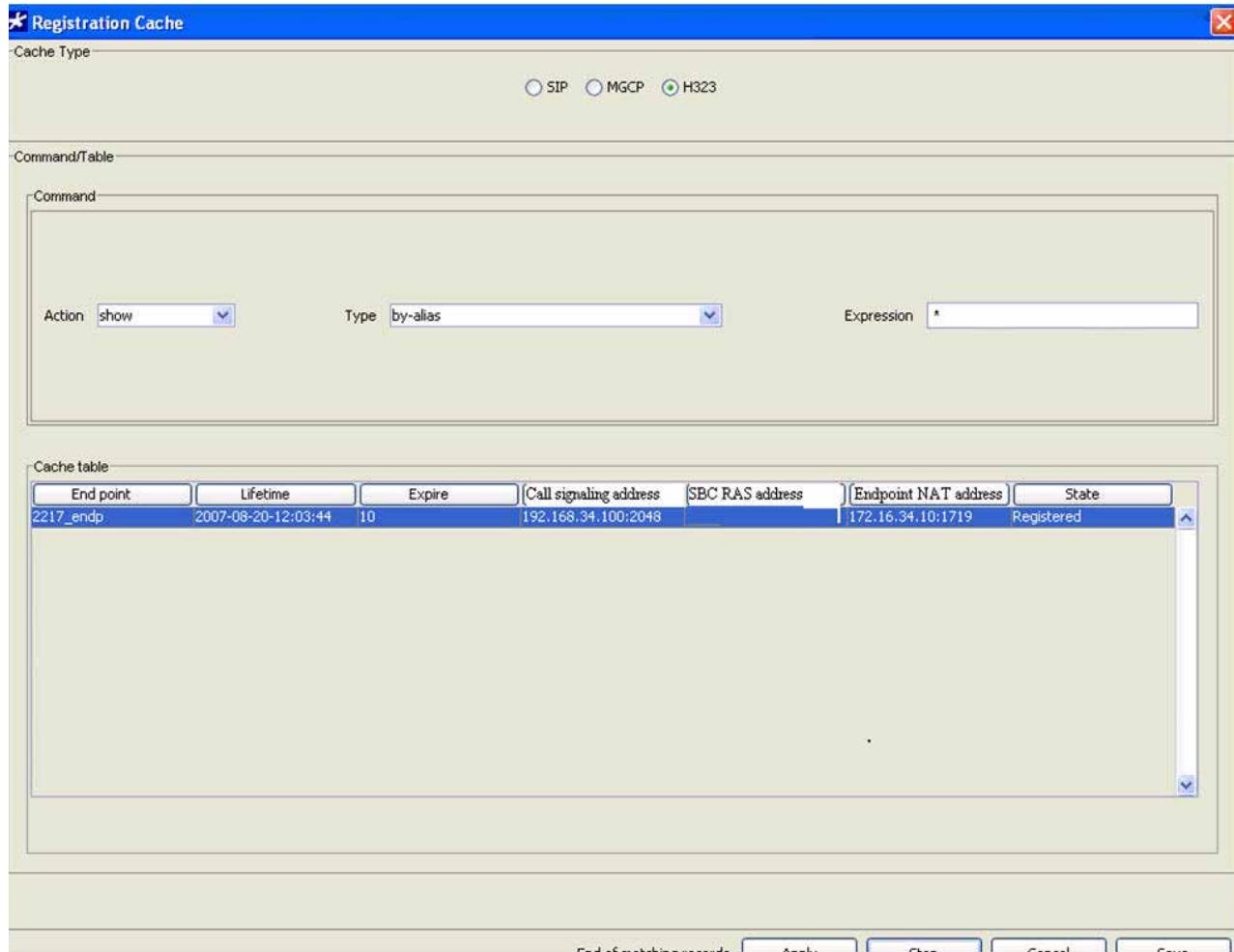
The H.323 commands and registration cache table appear. From here you can show, clear, and audit registration cache entries.

Displaying the H.323 Registration Cache

To display the H.323 cache entries:

- Action—Choose show from the Action drop-down list.
- Type—Choose by-alias from the Type drop-down list to display the H.323 registration cache for a particular alias.

3. **Expression**—Enter use a phone number or terminal identifier. You can wildcard the value by using an asterisk (*) as the final character in the terminalAlias string.
4. Click **Apply**. The Apply button grays out while Net-Net EMS processes the command. A message is displayed in the Command status textbox once processing completes and the Cache table displays the results (if any).



You can view the known details of the cache table entries. See Viewing Registration Cache Details for step-by-step instructions.

Viewing Registration Cache Details

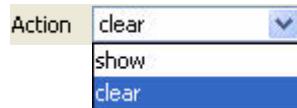
You can right-click an entry in the Cache table or click a row to select it and then click Detail to access additional details. The Registration cache entry details window appears.

Registration cache entry details

| | |
|---|----------------------------|
| Protocol | h323d |
| End point | 2217_endp |
| Lifetime | 1187625824 |
| Expire | 27 |
| Audit results | REACHABLE - [IRQ: Success] |
| Gatekeeper ID | open-gk1 |
| SBC CAS | 192.168.34.100:2048 |
| SBC RAS address | 192.168.34.100:8200 |
| Endpoint NAT address | 172.16.34.10:1719 |
| State | Registered |
| Terminal alias | |
| Alias | h323-ID: fjeleskovic |
| Register | true |
| Terminal alias | |
| Alias | e164: 1234 |
| Register | true |
| Call signalling address | |
| CAS | 172.16.34.10:1720 |
| RAS-Address | |
| RAS (Registration, admission and status) | 172.16.34.10:1719 |
| <input type="button" value="OK"/> <input type="button" value="Raw data"/> | |

Clearing the H.323 Registration Cache**To clear the H.323 process registration cache:**

1. Action—Choose clear from the Action drop-down list.



2. Type—Choose all or by-alias from the Type drop-down list.
3. Expression—If by-alias, enter a phone number or terminal identifier.

Note: You cannot wildcard values to clear the H.323 registration cache.

4. Click Apply.

Auditing the H.323 Registration Cache**To audit the H.323 process registration cache:**

1. Action—Choose audit from the Action drop-down list.
2. Type—Choose by-alias from the drop-down list.
3. Expression—Enter enter a phone number or terminal identifier.
4. Click Apply.

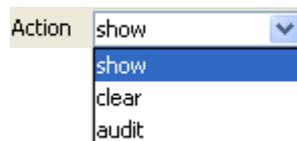
Working with MGCP Registration Caches**Displaying the MGCP Registration Cache****To work with MGCP registration caches:**

1. In the Cache Type area, click MGCP.

The MGCP commands and registration cache table appear. From here you can show, clear, and audit registration cache entries.

To display the MGCP registration cache entries:

1. Action—Choose show from the Action drop-down list.



2. Type—Choose by-endpoint from the Type drop-down list.

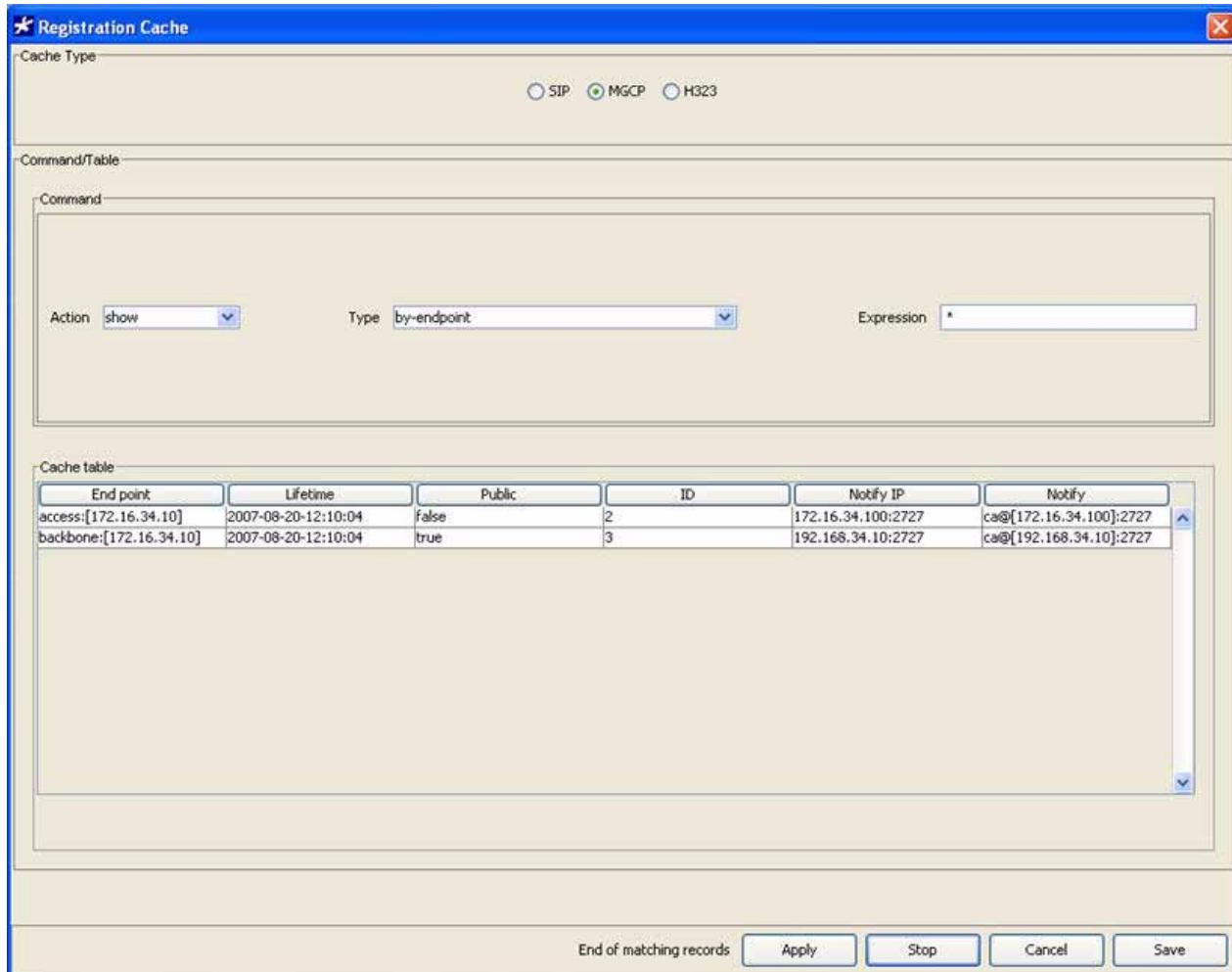
3. Expression—Enter one of the following arguments:

- realm_id:local_name@host
- realm_id:host
- local_name@host
- host

In these arguments, values are defined as follows:

- realm_id—Name of a realm named in the MGCP configured; only complete realm names are accepted; entry must end with a colon (:)
- local_name—Local name of the endpoint; must end with the at-sign (@)

- host—Can be an FQDN, IP address, or IP address enclosed in square brackets ([]); wildcarded by using an asterisk (*) at the end to refer to multiple hosts; using the square brackets for an IP address value is optional
4. Click **Apply**. The Apply button grays out while Net-Net EMS processes the command. A message is displayed in the Command status textbox once processing completes and the Cache table displays the results (if any).



You can view the known details of the cache table entries. See Viewing Registration Cache Details for step-by-step instructions.

Command Status

The Command status textbox displays the commands you issue. For example:



Viewing Registration Cache Details

You can right-click an entry in the Cache table or click a row to select it and then click Detail to access additional details. The Registration cache entry details window appears.

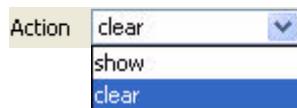
Registration cache entry details

| | |
|---|-------------------------|
| End point | access:[172.16.34.10] |
| Lifetime | 1187626204 |
| Public | false |
| Identifier | 2 |
| Notify IP | 172.16.34.100:2727 |
| Notify | ca@[172.16.34.100]:2727 |
| Auditable | audit |
| SESSION | |
| Identifier | 1 |
| NAT mode | OnlyHost |
| Local name | 172.16.34.10 |
| Local port | 172.16.234.22:15674 |
| Local endpoint | aaln/1 |
| Remote name | |
| Remote port | 192.168.34.100:2427 |
| Notify port | 0.0.0.0:0 |
| Remote endpoint | aaln/1@172.16.34.10 |
| Audit name | aaln/1@172.16.34.10 |
| Lookup call agent | backbone:[172.16.34.10] |
| Lookup gateway | access:[172.16.34.10] |
| <input type="button" value="OK"/> <input type="button" value="Raw data"/> | |

Clearing the MGCP Registration Cache

To clear the MGCP process registration cache:

- Action—Choose clear from the Action drop-down list.



- Type—Choose all or by-endpoint from the Type drop-down list.
 - all**—Clears all MGCP registrations in the registration cache.
 - by-endpoint**—Clears the MGCP registration cache of a particular endpoint. You enter this command with one of the following arguments:

realm_id:local_name@host

realm_id:host

In these arguments, values are defined as follows:

- realm_id**—Name of a realm named in the MGCP configured; only complete realm names are accepted; entry must end with a colon (:)
- local_name**—Local name of the endpoint; must end with the at-sign (@)
- host**—Can be an FQDN, IP address, or IP address enclosed in square brackets ([]); wildcarded by using an asterisk (*) at the end to refer to multiple hosts; using the square brackets for an IP address value is optional

- Expression—If clearing by endpoint, enter the endpoint information.
- Click **Apply**.

Auditing the MGCP Registration Cache

To audit the MGCP process registration cache:

When you audit the MGCP registration cache, the Net-Net SBC sends an audit endpoint message (AUEP) to the MGCP endpoint to determine leachability, and a reply is expected from the endpoint.

MGCP audit messages are only sent to the endpoints in private realms. Requests sent to public realms are rejected and error messages are returned.

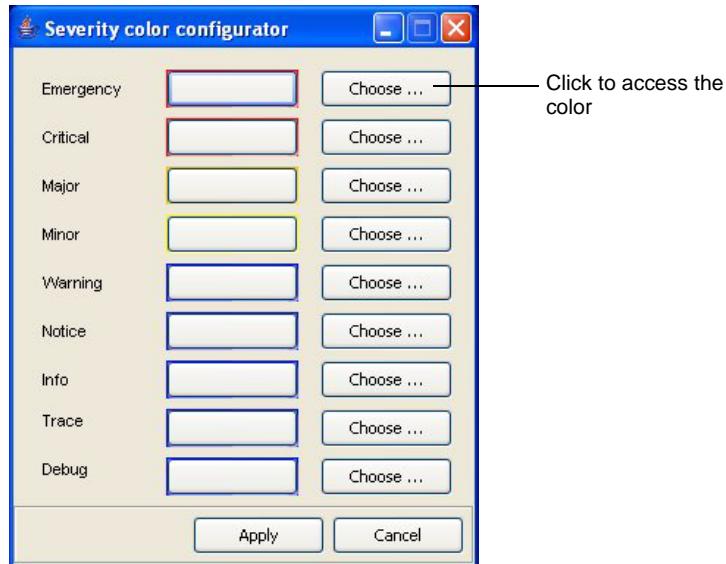
- Action—Choose audit from the Action drop-down list.
- Type—Choose by-endpoint from the drop-down list.
- Expression—Enter the endpoint information.
- Click **Apply**.

Configuring Severity Color-Coding

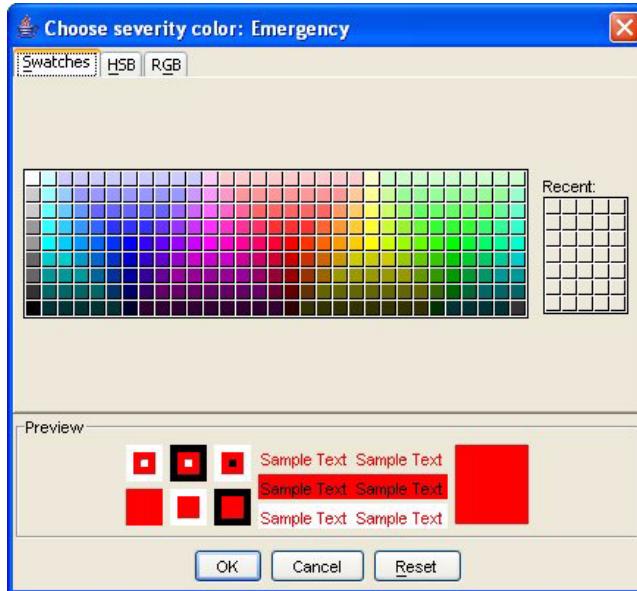
You can configure the colors used to indicate the different severity levels.

To configure colors:

1. Right-click Fault Management and choose Severity configurator from the option list. The Severity color configurator dialog box appears:



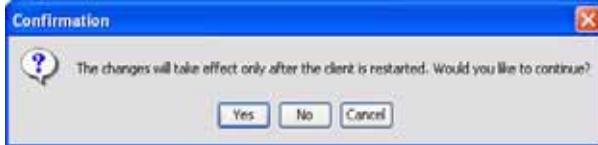
2. Choose the color you want for each severity level by clicking **Choose**. The Choose severity color window appears:



3. Edit the current color, hue/saturation/brightness (HSB) values, and red/green/blue (RGB) values by following the steps in the appropriate section.

After you make your edits and click **OK** in the Choose severity color window, you return to the Severity color configurator window. From there you can apply your edits.

4. Click **OK** to apply your changes. The Confirmation message appears:



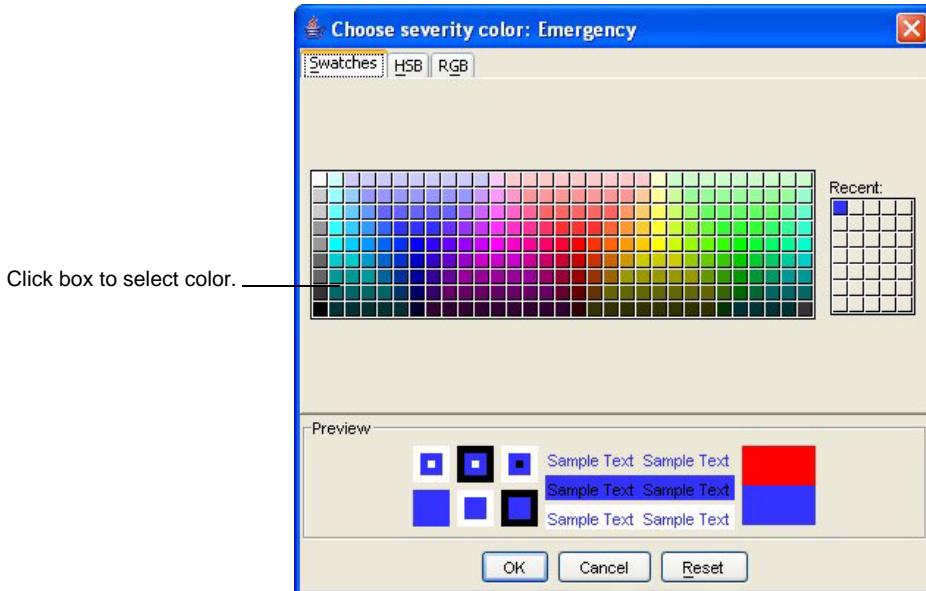
5. Click **Yes** to apply the changes and clear the message.
6. Exit the Severity color configurator.
7. Restart Net-Net EMS to apply your changes.

Choosing a New Color

To choose a new color:

1. In the Choose severity color window, ensure the **Swatches** tab is selected.
2. Click a box in the color grid to select a new color.

The Preview section of the window displays your color choice and the Recent grid displays the color in the top left block. For example:



3. View your changes in the preview section of the window.

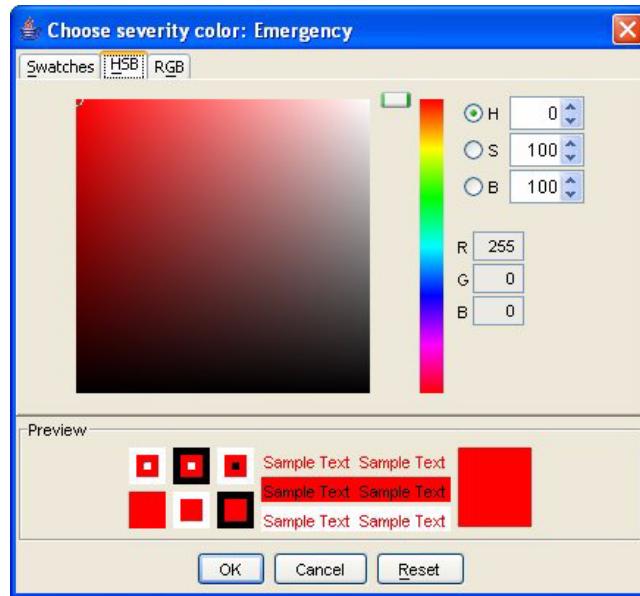
From here you can edit the HSB values and/or the RGB values, or you can click **OK** to return to the Severity color configurator window.

Editing HSB Values

To edit HSB values:

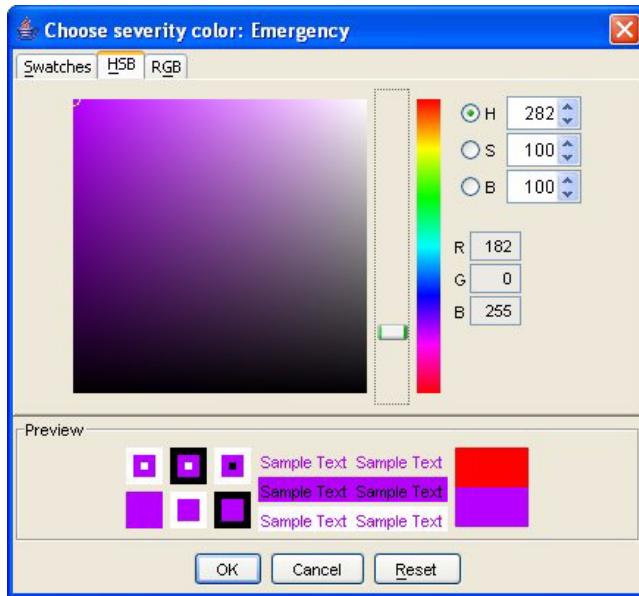
1. Click the HSB tab.

The HSB tab contains a color palette, text entry boxes for hue (H), saturation (S), and brightness (B) and display boxes for red (R), green (G), and blue (B) values. For example:



- RGB (red, green, and blue): a system for representing the colors in your display. Red, green, and blue are combined in various proportions to produce any color in the visible spectrum. Levels of red, green, and blue can each range from 0 to 100 percent of full intensity. Each level is represented by the range of decimal numbers from 0 to 255 (256 levels for each color). The total number of available colors is 256 x 256 x 256, or 16,777,216 possible colors.
 - HSB (hue, saturation, and brightness): aspects of color in the RGB scheme. All possible colors can be specified according to hue, saturation, and brightness.
2. Edit the values for hue, saturation, - and brightness by using one of the following methods:
 - 2a. Selecting from color palette. Left-click and hold the mouse button while moving the icon in the color palette to select a color.
 - 2b. Entering specific values. For example, edit the value for hue (H) by clicking the H radio button for the value to select it. Enter a new value.

The R, G, and B values change to reflect the changes made to H, S, or B. Also the slide next to the color bar moves to reflect your edits. For example:



- View your choice in the preview section of the window.

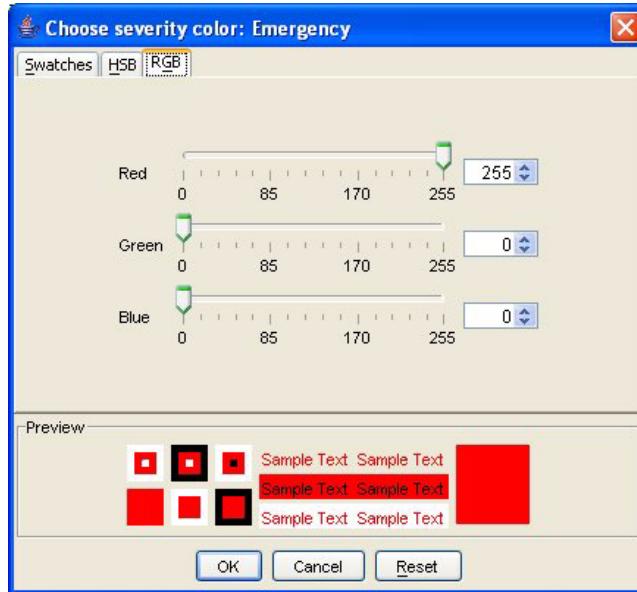
From here you can edit the RGB values or you can click **OK** to return to the Severity color configurator window.

Editing RGB Values

To edit RGB values:

- Click the RGB tab.

The RGB tab contains three sliders to use for changing the values. The values display in the boxes next to each slider. For example:

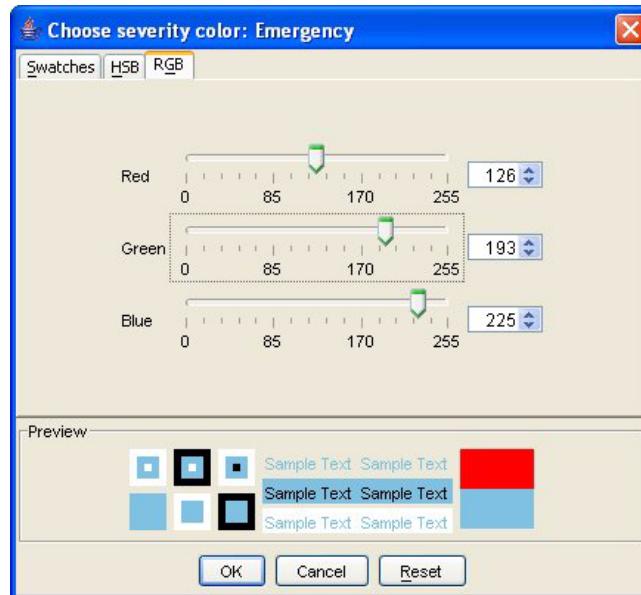


RGB (red, green, and blue) is a system for representing the colors in your display. Red, green, and blue are combined in various proportions to produce

any color in the visible spectrum. Levels of red, green, and blue can each range from 0 to 100 percent of full intensity. Each level is represented by the range of decimal numbers from 0 to 255 (256 levels for each color). The total number of available colors is 256 x 256 x 256, or 16,777,216 possible colors.

2. Left-click on the slider's bar and move it to the value you want or enter a value in the display box next to the slider.

The new values display next to the slider and the new color displays in the Preview section. For example:



3. View your choice in the preview section of the window.
4. Click **OK** to apply your changes and return to the Severity color configurator window. From there you can apply your changes.

Introduction

This chapter describes the Net-Net EMS performance management component. Performance management involves monitoring your Net-Net SBCs by collecting necessary data from each of them. The performance is measured based on various factors, such as number of bytes of data received/sent (over a period) by a particular interface of a device, the interface's current bandwidth in bits per second, and so on.

The Net-Net EMS displays performance data for your discovered Net-Net SBCs. It displays the statistical and state information provided by the Net-Net SBC software (in the form of MIBs).

In Net-Net EMS, performance management statistics are only gathered for display when you access a Performance management screen or when you click the Refresh button. To preserve data, you must save it to a file by using the Save button.

Note: You need to configure the SNMP community parameter on the Net-Net SBCs for which you want to view performance data. See the *Net-Net EMS 4000 Configuration Guide* and the *Net-Net ACLI Reference Guide* for details.

Accessing Performance Management Information

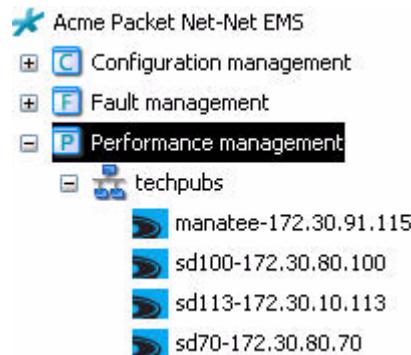
This section explains how to access the performance management information. The Performance management node is located in the EMS navigation pane's (left pane) hierarchical tree of nodes.

Listed under the Performance management node is a set of domains, each of which contains a list of Net-Net SBCs. The domains and Net-Net SBCs listed under Performance management always matches the list of Net-Net SBCs currently in the Active configuration category (located under the Configuration management node). Any additions and deletions to the Active configuration list of nodes is reflected in the Performance management list.

In the Performance management list, each member of an HA pair is listed individually, which differs from the display in the Active configuration area (where members of an HA pair are treated as a single managed device). You can view performance data for each of the Net-Net SBC systems that belong to the pair.

To access performance management information:

1. Click the plus (+) sign next to Performance Management to expand the category. A list of domain names appears. These are the same domain names that appear under the Configuration category.

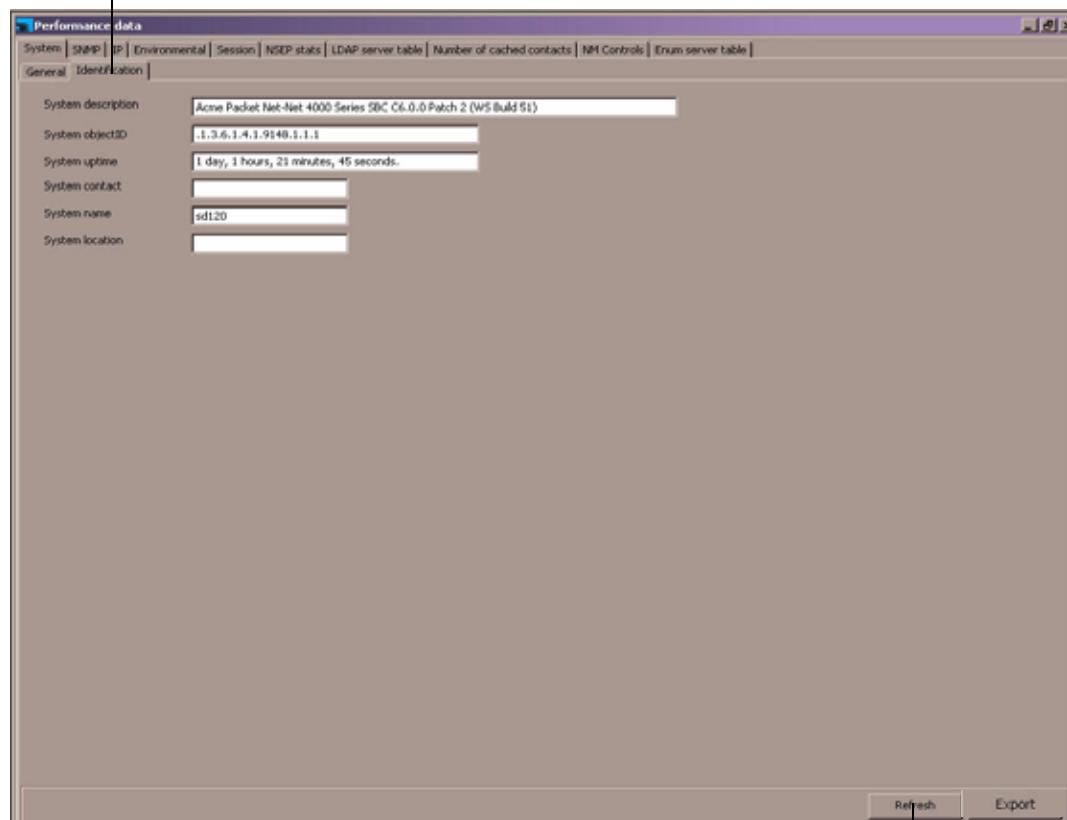


2. Click the plus (+) sign next to a domain name to expand it.
3. If accessing Net-Net SBCs that belong to an HA pair, click the + sign next to the name of the HA pair. For example:



4. Click the name of the Net-Net SBC for which you want to view performance data. The performance data for the Net-Net SBC appears in the right pane. For example

Click the tabs to access different data categories.



Click to refresh and save the data.

5. Access data by clicking the tabs across the top of the performance data window.

Refreshing Data

You can refresh the statistics displayed on each screen by clicking Refresh.

Saving Data

You can save the data displayed on each screen to a text file in comma separated format.

To save data to a file:

1. With the data displayed, click Export.

A Save window opens with a file name in the following format:

<stats screen name>-<tab name>-<date> <hh-mm-ss>.txt

For example:

System-General-2007-06-10 13-53-21.txt

2. Click Export to save the file and close the window.

Viewing System Information

This section explains the system performance information displayed by the Net-Net EMS.

Accessing System Data

To access System data:

1. Click the System tab in the Performance data screen. System performance data for the category General appears by default.
2. Click the Identification tab to view data that identifies this Net-Net SBC.

General

To access General data:

1. In the System window, click the General tab. The general system data appear:



The following table defines the data displayed by Net-Net EMS:

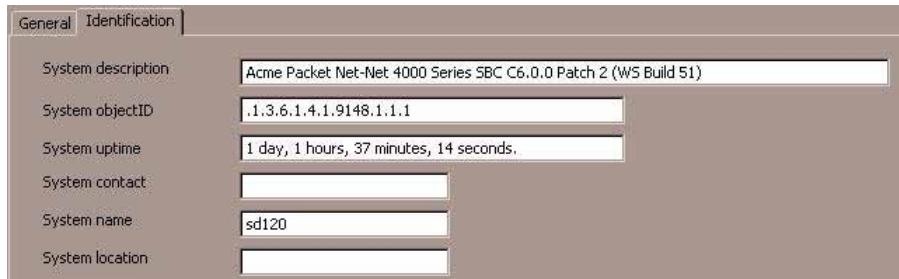
| Data | Description |
|---|---|
| CPU utilization (%) | Percentage of CPU utilization |
| Memory utilization (%) | Percentage of memory utilization |
| Health score (%) | System health percentage, with a system health percentage value of 100 (100%) being the healthiest |
| Redundancy state | For Net-Net HA pairs, information about this Net-Net SBC's state. Values are: <ul style="list-style-type: none"> • active • standby |
| Current signaling sessions (SIP, H.323, and MGCP) | Total number of global concurrent sessions at the moment |
| Current signaling rate (SIP, H.323, and MGCP) (CPS) | Number of global calls per second |
| CAM utilization (%) - media | Percentage of NAT table in Content Addressable Memory (CAM) utilization |

| Data | Description |
|---------------------------|---|
| CAM utilization (%) - ARP | Percentage of ARP table (in CAM) utilization |
| I2C bus state | <p>State of the environmental monitor located in the chassis. Values are:</p> <ul style="list-style-type: none"> • normal • not functioning |

Identification

To access Identification data:

1. In the System window, click the Identification tab. The system identification data appears:



The following table defines the data:

| Data | Description |
|--------------------|---|
| System description | Textual description of the entity. This value includes the full name and version identification of the system's hardware type, software operating-system, and networking software. |
| System objectID | Vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining what kind of box is being managed. |
| System uptime | Time (in hundredths of a second) since the network management portion of the system was last re-initialized. |
| System contact | Textual identification of the contact person for this managed node, together with information on how to contact this person. If no contact information is known, the value is the zero-length string. |
| System name | Administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. |
| System location | Physical location of this node. If the location is unknown, the value is the zero-length string. |

Viewing SNMP Information

This section describes the SNMP performance data displayed by the Net-Net EMS.

Accessing SNMP Data

To access SNMP data:

1. In the Performance data window, click the SNMP tab. The following data appear:

| System | | | |
|---------------------------|------|----------------------|---------|
| In | | Out | |
| In packets | 2309 | ASN parse errors | 0 |
| Out packets | 8615 | Authentication traps | enabled |
| Bad versions | 0 | Silent drops | 0 |
| Bad community names | 0 | Proxy drops | 0 |
| Bad community uses | 1 | | |
| | | | |
| Too bigs | 0 | Too bigs | 0 |
| No such names | 0 | No such names | 0 |
| Bad values | 0 | Bad values | 0 |
| Read only | 0 | General errors | 0 |
| General errors | 0 | Get requests | 0 |
| Total requested variables | 2325 | Get-nexsts | 0 |
| Total set variables | 0 | Set requests | 0 |
| Get requests | 3 | Get responses | 2357 |
| Get-nexsts | 2333 | Traps | 6306 |
| Set requests | 0 | | |
| Get responses | 0 | | |
| Traps | 0 | | |

The following table defines the information displayed:

| Data | Description |
|---------------------|---|
| In Packets | Total number of messages delivered to the SNMP entity from the transport service |
| Out packets | Total number of SNMP messages passed from the SNMP protocol entity to the transport service |
| Bad versions | Total number of SNMP messages delivered to the SNMP entity for an unsupported SNMP version |
| Bad community names | Total number of SNMP messages delivered to the SNMP entity which used a SNMP community name not known to said entity |
| Bad community uses | Total number of SNMP messages delivered to the SNMP entity which represented an SNMP operation which was not allowed by the SNMP community named in the message |

| Data | Description |
|---------------------------|--|
| ASN parse errors | Total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages |
| Authentication traps | Indicates whether the SNMP entity is permitted to generate authenticationFailure traps |
| Silent drops | Total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity that were silently dropped. They were dropped because the size of a reply containing an alternate Response-PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request. |
| Proxy drops | Total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity which were silently dropped. They were dropped because the transmission of the (possibly translated) message to a proxy target failed in a manner (other than a timeout) such that no Response-PDU could be returned. |
| In | |
| Too bigs | Total number of SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is <i>tooBig</i> . |
| No such names | Total number of SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is <i>noSuchName</i> . |
| Bad values | Total number of SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is <i>badValue</i> . |
| Read only | Total number of valid SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is <i>readOnly</i> . Note: Generating an SNMP PDU that contains the value <i>readOnly</i> in the error-status field is a protocol error. This value is provided to detect incorrect implementations of SNMP. |
| General errors | Total number of valid SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is <i>genErr</i> |
| Total requested variables | Total number of MIB objects retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs |

| Data | Description |
|---------------------|---|
| Total set variables | Total number of MIB objects altered successfully by the SNMP protocol entity as the result of receiving valid SNMP set-Request PDUs |
| Get requests | Total number of SNMP Get-Request PDUs that have been accepted and processed by the SNMP protocol entity |
| Get-nexts | Total number of SNMP Get-Next PDUs that have been accepted and processed by the SNMP protocol entity |
| Set requests | Total number of SNMP Set-Request PDUs that have been accepted and processed by the SNMP protocol entity |
| Get responses | Total number of SNMP Get-Responses that have been accepted and processed by the SNMP protocol entity |
| Traps | Total number of SNMP Trap PDUs that have been accepted and processed by the SNMP protocol entity |
| Out | |
| Too bigs | Total number of SNMP PDUs generated by the SNMP protocol entity and for which the value of the error-status field is <i>tooBig</i> |
| No such names | Total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is <i>noSuchName</i> |
| Bad values | Total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is <i>badValue</i> |
| General errors | Total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is <i>genErr</i> |
| Get requests | Total number of SNMP Get-Request PDUs generated by the SNMP protocol entity |
| Get-nexts | Total number of SNMP Get-Next PDUs generated by the SNMP protocol entity |
| Set requests | Total number of SNMP Set-Request PDUs generated by the SNMP protocol entity |
| Get responses | Total number of SNMP Get-Responses generated by the SNMP protocol entity |
| Traps | Total number of SNMP Trap PDUs generated by the SNMP protocol entity |

Viewing IP Information

This section describes the IP data displayed by Net-Net EMS.

Accessing IP Data

To access IP data:

1. In the Performance data window, click the IP tab. The IP performance data appears for the following categories:
 - General: general performance data
 - Addresses: information about this Net-Net SBC's IP addressing
 - Interfaces: information about the Net-Net SBC's interfaces. Each interface is thought of as being attached to a *subnet*.
 - ICMP: information about this Net-Net SBC and Internet Control Message Protocol (ICMP)
 - TCP: information about this Net-Net SBC's existing TCP connections
 - UDP: information about this Net-Net SBC's UDP end-points, upon which a local application is currently accepting datagrams

General

To access General data:

1. In the IP window, click the General tab. The following data appears:

| System SNMP IP Environmental Session NSEP stats LDAP server table Number of cached contacts NM Controls Enum server table | | | |
|---|----------------|------------------------------|-------|
| General Addresses Interfaces Extended interfaces table ICMP TCP UDP | | | |
| Forwarding capability | not-forwarding | Reassembly timeout (s) | 60 |
| Default time-to-live (s) | 64 | Reassemblies required | 0 |
| Total datagrams received | 187431 | Reassembled datagrams | 0 |
| Datagrams forwarded | 0 | Fragmented datagrams | 0 |
| | | Fragmentation failures | 0 |
| | | Created due to fragmentation | 0 |
| | | Routing discards | 0 |
| In | | Out | |
| Header errors | 0 | Requests | 40119 |
| Address errors | 1063 | Discards | 0 |
| Unknown protocols | 1854 | No routes | 0 |
| Discards | 0 | | |
| Delivered | 184526 | | |

The following table defines the data displayed:

| Data | Description |
|------------------------------|---|
| Forwarding capability | Indicates whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this entity. IP gateways forward datagrams. IP hosts do not (except those source-routed via the host). Note that for some managed nodes, this object may take on only a subset of the values possible. Accordingly, it is appropriate for an agent to return a <i>badValue</i> response if a management station attempts to change this object to an inappropriate value. |
| Default time-to-live(s) | Default value inserted into the Time-To-Live (TTL) field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol |
| Total datagrams received | Total number of input datagrams received from interfaces, including those received in error |
| Datagrams forwarded | Number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP gateways, this counter includes only those packets which were Source-Routed via this entity, and the Source-Route option processing was successful. |
| Reassembly timeout(s) | Maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity |
| Reassemblies required | Number of IP fragments received which needed to be reassembled at this entity |
| Reassembled datagrams | Number of IP datagrams successfully re-assembled |
| Fragmented datagrams | Number of IP datagrams that have been successfully fragmented at this entity |
| Fragmentation failures | Number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be (for example, because their Don't Fragment flag was set) |
| Created due to fragmentation | Number of IP datagram fragments that have been generated as a result of fragmentation at this entity |
| Routing discards | Number of routing entries that were discarded although they were valid. A reason for discard could be to free up buffer space for other routing entries. |
| Header errors | Number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on |
| Address errors | Number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example., 0.0.0.0) and addresses of unsupported Classes (for example., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address. |
| Unknown protocols | Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol |

| Data | Description |
|-----------|---|
| Discards | Number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). (Note that this counter does not include any datagrams discarded while awaiting re-assembly.) |
| Delivered | Total number of input datagrams successfully delivered to IP user-protocols including Internet Control Message Protocol (ICMP) |
| Requests | Total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. (Note that this counter does not include any datagrams counted in ipForwDatagrams.) |
| Discards | Number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). (Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.) |
| No routes | Number of IP datagrams discarded because a route could not be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this “no-route” criterion. (This includes any datagrams which a host cannot route because all of its default gateways are down.) |

Addresses

To access Address data:

1. In the IP window, click the Address tab. The following data appears:

| System SNMP IP Environmental Session NSEP stats LDAP server table Number of cached contacts NM Controls Enum server table | | | | | |
|---|----------------|-----------------|-------------------|---------------------|--|
| General Addresses Interfaces Extended interfaces table ICMP TCP UDP | | | | | |
| Index | Address | Netmask | Broadcast address | Max reassembly size | |
| 3 | 10.0.0.1 | 255.255.255.0 | 1 | 65535 | |
| 5 | 64.211.16.178 | 255.255.255.240 | 1 | 65535 | |
| 5 | 64.214.217.66 | 255.255.255.240 | 1 | 65535 | |
| 5 | 64.215.8.50 | 255.255.255.240 | 1 | 65535 | |
| 5 | 64.215.15.130 | 255.255.255.240 | 1 | 65535 | |
| 5 | 64.215.34.98 | 255.255.255.240 | 1 | 65535 | |
| 5 | 64.215.70.139 | 255.255.255.248 | 1 | 65535 | |
| 5 | 67.17.20.82 | 255.255.255.240 | 1 | 65535 | |
| 5 | 67.17.20.213 | 255.255.255.240 | 1 | 65535 | |
| 5 | 67.17.21.181 | 255.255.255.240 | 1 | 65535 | |
| 2 | 127.0.0.1 | 255.0.0.0 | 1 | 65535 | |
| 5 | 162.97.4.108 | 255.255.255.248 | 1 | 65535 | |
| 5 | 162.97.6.186 | 255.255.255.248 | 1 | 65535 | |
| 5 | 162.97.52.130 | 255.255.255.240 | 1 | 65535 | |
| 5 | 162.97.53.5 | 255.255.255.240 | 1 | 65535 | |
| 5 | 162.97.58.52 | 255.255.255.240 | 1 | 65535 | |
| 5 | 162.97.61.140 | 255.255.255.248 | 1 | 65535 | |
| 5 | 162.97.62.229 | 255.255.255.240 | 1 | 65535 | |
| 5 | 162.97.67.21 | 255.255.255.240 | 1 | 65535 | |
| 5 | 162.97.71.146 | 255.255.255.240 | 1 | 65535 | |
| 5 | 162.97.107.210 | 255.255.255.240 | 1 | 65535 | |
| 5 | 162.97.120.229 | 255.255.255.240 | 1 | 65535 | |
| 5 | 162.97.124.117 | 255.255.255.240 | 1 | 65535 | |
| 5 | 162.97.125.53 | 255.255.255.240 | 1 | 65535 | |

The following table defines the information displayed for the Net-Net system's control and maintenance interfaces (such as wancom and loopback):

| Data | Description |
|---------------------|---|
| Index | Index value which uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex. |
| Address | IP address to which this entry's addressing information pertains |
| Netmask | Subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits set to 1 and all the host bits set to 0. |
| Broadcast address | Value of the least-significant bit in the IP broadcast address used for sending datagrams on the (logical) interface associated with the IP address of this entry. For example, when the Internet standard all-ones broadcast address is used, the value is 1. This value applies to both the subnet and network broadcasts addresses used by the entity on this (logical) interface. |
| Max reassembly size | Size of the largest IP datagram which this entity can re-assemble from incoming IP fragmented datagrams received on this interface |

Interfaces

To access Interfaces data:

1. In the IP window, click the Interfaces tab. The STD Interfaces sub-tab and Utilization sub-tab appears.

To view STD interface data:

1. From the Interfaces tab, click the STD Interface subtab for the following Net-Net system's control and maintenance interfaces (such as wancom and loopback):

| System SNMP IP Environmental Session NSEP stats LDAP server table Number of cached contacts Trap table summary Storage utilization IDS NM Co | | | | | | | |
|--|------|-------------|------------------|------|------------|-------------------|--------------|
| General Addresses Interfaces Extended interfaces table ICMP TCP UDP | | | | | | | |
| STD interfaces Utilization | | | | | | | |
| Index | Name | Description | Type | MTU | Speed | Physical address | Admin status |
| 1 | | eth0 | ethernetCsmacd | 1500 | 100000000 | 00:08:25:a0:5e:50 | up |
| 2 | | lo0 | softwareLoopback | 1536 | 0 | 00:00:00:00:00:00 | up |
| 3 | | eth1 | ethernetCsmacd | 1500 | 1000000000 | 00:08:25:a0:5e:51 | up |
| 4 | | eth2 | ethernetCsmacd | 1500 | 1000000000 | 00:08:25:a0:5e:52 | up |
| 5 | M00 | M00 | gigabitEthernet | 1500 | 1000000000 | 00:08:25:a0:5e:53 | up |
| 6 | | | gigabitEthernet | 1500 | 1000000000 | 00:00:00:00:00:00 | down |
| 7 | | | gigabitEthernet | 1500 | 1000000000 | 00:00:00:00:00:00 | down |
| 8 | | | gigabitEthernet | 1500 | 1000000000 | 00:00:00:00:00:00 | down |
| 13 | | sp0 | ethernetCsmacd | 1500 | 100000000 | 00:08:25:a0:5e:53 | up |

The following table defines the information displayed in the STD Interfaces tab.

| Data | Description |
|--------------------|--|
| Index | Unique value for each interface. Value has a range between 1 and the value of ifNumber and must remain constant at least from one re-initialization of the entity's NMS to the next re-initialization. |
| Name | Name of this STD interface. |
| Description | Textual string containing information about the interface. This string includes the name of the manufacturer, the product name, and the version of the hardware interface. |
| Type | Information about the type of interface, distinguished according to the physical/link protocol(s) immediately <i>below</i> the network layer in the protocol stack |
| MTU | Size of the largest datagram which can be sent/received on the interface, specified in octets. For interfaces that transmit network datagrams, this is the size of the largest network datagram that can be sent on the interface. |
| Speed | Estimate of the interface's current bandwidth in bits per second. For interfaces which do not vary in bandwidth or for those where an accurate estimation cannot be made, it contains the nominal bandwidth. |
| Physical address | Interface's address at the protocol layer immediately <i>below</i> the network layer in the protocol stack. For interfaces which do not have such an address (for example, a serial line), it contains an octet string of zero length. |
| Admin status | Current administrative state of the interface. Values are: <ul style="list-style-type: none"> • up • down • testing |
| Operational status | Current operational state of the interface. Values are: <ul style="list-style-type: none"> • up • down • testing |
| Last change time | Value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then it contains a zero value. |
| In | |
| Octets | Total number of octets received on the interface, including framing characters |
| Unicast pkts | Number of subnetwork-unicast packets delivered to a higher-layer protocol |
| Non-Unicast pkts | Number of non-unicast (for example, subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol |
| Discards | Number of inbound packets which were chosen to be discarded although no errors had been detected to prevent their being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space. |

| Data | Description |
|------------------|--|
| Errors | Number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol |
| Out | |
| Octets | Total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent |
| Unicast pkts | Total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent |
| Non-Unicast pkts | Total number of packets that higher-level protocols requested be transmitted to a non-unicast (i.e., a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent |
| Discards | Number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space. |
| Errors | Number of outbound packets that could not be transmitted because of errors |
| Specific media | Returns a reference to MIB definitions specific to the particular media being used to realize the interface. For example, if the interface is realized by an ethernet, then the value of this object refers to a document defining objects specific to Ethernet. If this information is not present, its value should be set to the OBJECT IDENTIFIER {0 0}, which is a syntactically valid object identifier, and any conformant implementation of ASN.1 and BER must be able to generate and recognize this value. |

2. From the Interfaces tab, click the Utilization subtab to view data related to RX utilization and TX utilization of media ports.

| Utilization | | | |
|-------------|------|----------------|----------------|
| Index | Name | Rx Utilization | Tx Utilization |
| 5 | M00 | 0 | 0 |
| 6 | M10 | 0 | 0 |

The following table defines the information displayed in the Utilization tab.

| Data | Description |
|----------------------|--|
| Index | Unique value for each interface. Value has a range between 1 and the value of ifNumber and must remain constant at least from one re-initialization of the entity's NMS to the next re-initialization. |
| apPhyUtilTableRXUtil | RX utilization of media ports indexed by IF index. |
| apPhyUtilTableTXUtil | TX utilization of media ports indexed by IF index. |

Extended Interfaces**To access extended interfaces data:**

1. In the IP window, click the Extended interfaces tab. The following data appears:

| Index | Name | In Multicast Pkts | In Broadcast ... | Out Multicast ... | Out Broadcast... | HC In Octets | HC In |
|-------|-------------------|-------------------|------------------|-------------------|------------------|--------------|-------|
| 5 | CustomerInterface | 0 | 0 | 0 | 4236 | 0x0 | 0x0 |

The following table defines the information displayed for the Net-Net 9000's media interfaces:

| Data | Description |
|----------------|--|
| Index | Unique value for each interface. Value has a range between 1 and the value of ifNumber and must remain constant at least from one re-initialization of the entity's NMS to the next re-initialization. |
| Name | Textual string containing the name of the interface. The name is the one assigned by the local device. It could be a text name or a port number, depending on the interface naming syntax of the device. |
| In | |
| Multicast Pkts | Number of packets delivered from this layer to a higher layer that were addressed to a multicast address. For a MAC layer protocol, it includes both group and functional addresses. |
| Broadcast Pkts | Number of packets delivered by this layer to a higher level that were addressed to a broadcast address |
| Out | |
| Multicast Pkts | Number of packets that higher-level protocols requested be transmitted that were addressed to a multicast address at this layer, including those discarded or not sent |
| Broadcast Pkts | Number of packets higher-level protocols requested to be transmitted that were addressed to a broadcast address at this layer, including those discarded or not sent |
| HC In | |

| Data | Description |
|----------------------------|---|
| Octets | Total number of octets received on the interface, including framing characters |
| Ucast Pkts | Number of packets delivered by this layer to a higher layer that were not addressed to a multicast or broadcast address at this layer |
| Multicast Pkts | Number of packets delivered by this layer to a higher layer that were addressed to a multicast address at this layer. For a MAC layer protocol, this includes both group and functional addresses. |
| Broadcast Pkts | Number of packets delivered by this layer to a higher layer that were addressed to a broadcast address at this layer |
| HC out | |
| Octets | Total number of octets transmitted out of the interface, including framing characters |
| Ucast Pkts | Total number of packets that higher-level protocols requested be transmitted that were not addressed to a multicast or broadcast address at this layer; including those discarded or not sent |
| Multicast Pkts | Total number of packets that higher-level protocols requested be transmitted that were addressed to a multicast address at this layer, including those discarded or not sent. For a MAC layer protocol, this includes both the group and functional addresses. |
| Broadcast Pkts | Total number of packets that higher-level protocols requested be transmitted that were addressed to a broadcast address at this layer; including those discarded or not sent |
| LinkUpDownTrap Enable | Indicates whether linkUp/linkDown traps should be generated for this interface. The value should be enabled(1) for interfaces that do no operate on top of any other interface and disabled(2) otherwise. |
| High Speed | Estimate of the interface's current bandwidth in units of 1,000,000 bits per second. If a value of n is reported, the speed of the interface is in the range of n-500,00 to n+499,999. For interfaces that do not vary in bandwidth or for those where no accurate estimation can be made, a nominal bandwidth is given. |
| Promiscuous Mode | If the interface only accepts packets/frames addressed to this station, the value is false(2). If the interface accepts all packets/frames transmitted on the media, the value is true(1). This object has a true(1) value only on certain types of media. This value does not affect the reception of broadcast and multicast packets/frames by the interface. |
| Connector Present | If the interface layer has a physical connector, the value is true(1). Otherwise it is false(2) |
| Alias | Provides a location in which a non-volatile interface-naming value can be stored. This lets a network manager give one or more interfaces their own unique names, regardless of any interface-stack relationship. |
| Counter Discontinuity Time | Value of sysUpTime on the most recent occasion at which one or more of this interface's counters suffered a discontinuity |

ICMP

To access ICMP data:

1. In the IP window, click the ICMP tab. The following data appears:

| General | | Addresses | | Interfaces | | Extended interfaces table | | ICMP | TCP | UDP |
|--------------------------|--|-----------|--|------------|--|---------------------------|--|--------------------------|-----|-----|
| In | | | | | | | | Out | | |
| Messages | | | | | | | | Messages | | |
| Errors | | | | | | | | Errors | | |
| Destination unreachables | | | | | | | | Destination unreachables | | |
| Time exceeded | | | | | | | | Time exceeded | | |
| Parameter problems | | | | | | | | Parameter problems | | |
| Source quenches | | | | | | | | Source quenches | | |
| Redirects | | | | | | | | Redirects | | |
| Echos | | | | | | | | Echos | | |
| Echo replies | | | | | | | | Echo replies | | |
| Timestamps | | | | | | | | Timestamps | | |
| Timestamp replies | | | | | | | | Timestamp replies | | |
| Address masks | | | | | | | | Address masks | | |
| Address mask replies | | | | | | | | Address mask replies | | |

The following table defines the information displayed:

| Data | Description |
|--------------------------|--|
| In | |
| Messages | Total number of ICMP messages which the Net-Net SBC received. (Note that this counter includes all those counted by icmpInErrors.) |
| Errors | Number of ICMP messages which the Net-Net SBC received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so on) |
| Destination unreachables | Number of ICMP Destination Unreachable messages received |
| Time exceeded | Number of ICMP Time Exceeded messages received |
| Parameter problems | Number of ICMP Parameter Problem messages received |
| Source quenches | Number of ICMP Source Quench messages received |
| Redirects | Number of ICMP Redirect messages received |
| Echoes | Number of ICMP Echo (request) messages received |
| Echo replies | Number of ICMP Echo Reply messages received |
| Timestamps | Number of ICMP Timestamp (request) messages received |
| Timestamp replies | Number of ICMP Timestamp Reply messages received |
| Address masks | Number of ICMP Address Mask Request messages received |
| Address mask replies | Number of ICMP Address Mask Reply messages received |
| Out | |

| Data | Description |
|--------------------------|---|
| Messages | Total number of ICMP messages which the Net-Net SBC attempted to send. (This counter includes all those counted by icmpOutErrors.) |
| Errors | Number of ICMP messages which the Net-Net SBC did not send due to problems discovered within ICMP such as a lack of buffers. This value does not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value. |
| Destination unreachables | Number of ICMP Destination Unreachable messages sent |
| Time exceeded | Number of ICMP Time Exceeded messages sent |
| Parameter problems | Number of ICMP Parameter Problem messages sent |
| Source quenches | Number of ICMP Source Quench messages sent |
| Redirects | Number of ICMP Redirect messages sent |
| Echoes | Number of ICMP Echo (request) messages sent |
| Echo replies | Number of ICMP Echo Reply messages sent |
| Timestamps | Number of ICMP Timestamp (request) messages sent |
| Timestamp replies | Number of ICMP Timestamp Reply messages sent |
| Address masks | Number of ICMP Address Mask Request messages sent |
| Address mask replies | Number of ICMP Address Mask Reply messages sent |

TCP**To access TCP data:**

1. In the IP window, click the TCP tab. The following data appears:

| General | Addresses | Interfaces | Extended interfaces table | ICMP | TCP | UDP |
|---------------------------------|------------|------------------------|---------------------------|-------------|----------------------------------|----------------------------------|
| Retransmission algorithm | vanj | Attempt fails | 0 | | | |
| Retransmission timeout min (ms) | 1000 | Established resets | 45 | | | |
| Retransmission timeout max (ms) | 64000 | Current established | 54 | | | |
| Max connections | -1 | In segments | 15449 | | | |
| Active opens | 26 | Out segments | 15406 | | | |
| Passive opens | 73 | Retransmitted segments | 0 | | | |
| Local address | Local port | Remote add... | Remote port | State | | |
| 0.0.0.0 | 21 | 0.0.0.0 | 0 | listen | <input type="button" value="▲"/> | <input type="button" value="▼"/> |
| 0.0.0.0 | 22 | 0.0.0.0 | 0 | listen | <input type="button" value="▲"/> | <input type="button" value="▼"/> |
| 0.0.0.0 | 23 | 0.0.0.0 | 0 | listen | <input type="button" value="▲"/> | <input type="button" value="▼"/> |
| 127.0.0.1 | 1024 | 127.0.0.1 | 3000 | established | <input type="button" value="▲"/> | <input type="button" value="▼"/> |
| 127.0.0.1 | 1025 | 127.0.0.1 | 3000 | established | <input type="button" value="▲"/> | <input type="button" value="▼"/> |
| 127.0.0.1 | 1026 | 127.0.0.1 | 3000 | established | <input type="button" value="▲"/> | <input type="button" value="▼"/> |
| 127.0.0.1 | 1027 | 127.0.0.1 | 3000 | established | <input type="button" value="▲"/> | <input type="button" value="▼"/> |
| 127.0.0.1 | 1028 | 127.0.0.1 | 3000 | established | <input type="button" value="▲"/> | <input type="button" value="▼"/> |
| 127.0.0.1 | 1029 | 127.0.0.1 | 3000 | established | <input type="button" value="▲"/> | <input type="button" value="▼"/> |
| 127.0.0.1 | 1030 | 127.0.0.1 | 3000 | established | <input type="button" value="▲"/> | <input type="button" value="▼"/> |
| 127.0.0.1 | 1031 | 127.0.0.1 | 3000 | established | <input type="button" value="▲"/> | <input type="button" value="▼"/> |

The following table defines the information displayed:

| Data | Description |
|---------------------------------|--|
| Retransmission algorithm | Algorithm used to determine the timeout value used for retransmitting unacknowledged octets |
| Retransmission timeout min (ms) | Minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is <code>rsre</code> , an object of this type has the semantics of the LBOUND quantity described in RFC 793. |
| Retransmission timeout max (ms) | Maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is <code>rsre</code> , an object of this type has the semantics of the UBOUND quantity described in RFC 793. |
| Max connections | Total number of TCP connections the Net-Net SBC supports. In entities where the maximum number of connections is dynamic, this object contains the value <code>-1</code> . |
| Active opens | Number of times TCP connections made a direct transition to the SYN-SENT state from the CLOSED state |
| Passive opens | Number of times TCP connections made a direct transition to the SYN-RCVD state from the LISTEN state |
| Attempt fails | Number of times TCP connections made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections made a direct transition to the LISTEN state from the SYN-RCVD state |
| Established resets | Number of times TCP connections made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state |
| Current established | Number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT |
| In segments | Total number of segments received, including those received in error. This count includes segments received on currently established connections |
| Out segments | Total number of segments sent, including those on current connections but excluding those containing only retransmitted octets |
| Retransmitted segments | Total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets |

You can scroll through a list of connections displayed in the bottom section of the screen.

| Local address | Local port | Remote addr... | Remote port | State |
|---------------|------------|----------------|-------------|-------------|
| 0.0.0.0 | 21 | 0.0.0.0 | 0 | listen |
| 0.0.0.0 | 22 | 0.0.0.0 | 0 | listen |
| 0.0.0.0 | 23 | 0.0.0.0 | 0 | listen |
| 127.0.0.1 | 1024 | 127.0.0.1 | 3000 | established |
| 127.0.0.1 | 1026 | 127.0.0.1 | 3000 | established |
| 127.0.0.1 | 1028 | 127.0.0.1 | 3000 | established |
| 127.0.0.1 | 1030 | 127.0.0.1 | 3000 | established |
| 127.0.0.1 | 1032 | 127.0.0.1 | 3000 | established |
| 127.0.0.1 | 1034 | 127.0.0.1 | 3000 | established |

The following table defines the information displayed:

| Data | Description |
|----------------|---|
| Local address | Local IP address for this TCP connection. In the case of a connection in the listen state, the value is 0.0.0.0. |
| Local port | Local port number for this TCP connection |
| Remote address | Remote IP address for this TCP connection |
| Remote port | Remote port number for this TCP connection |
| State | State of this TCP connection. Values are: <ul style="list-style-type: none"> • closed • listen • established |

UDP**To access UDP data:**

1. In the IP window, click the UDP tab. The following data appears:

The screenshot shows the IP window with the UDP tab selected. At the top, there are four text input fields: 'In datagrams' (7531), 'No ports' (162006), 'In errors' (0), and 'Out datagrams' (23138). Below these is a table titled 'Listeners' with two columns: 'Local address' and 'Local port'. The table lists 12 entries, each consisting of a local IP address and a corresponding port number.

| Local address | Local port |
|---------------|------------|
| 0.0.0.0 | 123 |
| 0.0.0.0 | 161 |
| 0.0.0.0 | 1062 |
| 0.0.0.0 | 1063 |
| 0.0.0.0 | 1064 |
| 0.0.0.0 | 1812 |
| 127.0.0.1 | 1038 |
| 127.0.0.1 | 1040 |
| 127.0.0.1 | 1044 |
| 127.0.0.1 | 1046 |
| 127.0.0.1 | 1048 |

The following table defines the information displayed:

| Data | Description |
|------------------|---|
| In datagrams | Total number of UDP datagrams delivered to UDP users |
| No ports | Total number of received UDP datagrams for which there was no application at the destination port |
| In errors | Number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port |
| Out datagrams | Total number of UDP datagrams sent from this Net-Net SBC |
| Listeners | |
| Local address | Local IP address for this UDP listener. In the case of a UDP listener which is willing to accept datagrams for any IP interface associated with the node, the value is 0.0.0.0. |
| Local port | Local port number for this UDP listener |

Viewing Environmental Information

This section describes the environmental information displayed by Net-Net EMS.

Accessing Environmental Data

To access environmental data:

- From the Performance data window, click the Environmental tab. Data for the following categories appears:
 - Voltage
 - Temperature
 - Fans
 - Power supplies
 - Phy cards

Voltage

To access Voltage data:

- In the Environmental window, click the Voltage tab. The following data appears:

| Index | Voltage type | Description | Current voltage (milli volts) | Sensor state |
|-------|--------------|--------------------------|-------------------------------|--------------|
| 1 | v5 | 5V voltage (millivolts) | 4921 | normal |
| 2 | cpu | CPU voltage (millivolts) | 1265 | normal |

The following table defines the information displayed:

| Data | Description |
|------------------------------|--|
| Index | A monotonically increasing integer. When it reaches the maximum value the agent wraps the value back to 1. |
| Voltage type | <p>Value which indicates the sensor monitoring voltage. Values are:</p> <ul style="list-style-type: none"> • v2p5 - 2.5v sensor. This monitors L3 cache core voltage, micro-processor and co-processor I/O voltage, and Field-Programmable Gate Array (FPGA) memories I/O voltage. • v3p3 - 3.3V sensor. This monitors general TTL supply rail, control logic, micro-processor; micro-processor and co-processor; and SDRAM voltage. • v5 - 5V sensor. This monitors fans and micro-processor core voltage regulator. • CPU sensor. This monitors CPU voltage and micro-processor core voltage. |
| Description | <p>Description of the entity being monitored for voltage. Values are:</p> <ul style="list-style-type: none"> • 2.5V voltage (millivolts) • 3.3V voltage (millivolts) • 5V voltage (millivolts) • CPU voltage (millivolts) |
| Current voltage (millivolts) | Current voltage measurement, in millivolts, if available. A value of -1 indicates that the monitor cannot obtain a value. |
| Sensor state | <p>Current state of the voltage for the device being monitored. Values are:</p> <p>Host Processor 7450 and 7455</p> <ul style="list-style-type: none"> • normal range: 1.55v to 1.65v • minor range: 1.4v to 1.55v or 1.65v to 1.8v • shutdown range: <1.4v or >1.8v <p>Host Processor 7457</p> <p>Version 1.0</p> <ul style="list-style-type: none"> • normal range: 1.35v to 1.45v • minor range: 1.00v to 1.35v or 1.45v to 1.6v • shutdown range: <1.0v or >1.6v <p>Version 1.1 and later</p> <ul style="list-style-type: none"> • normal range: 1.25v to 1.35v • minor range: 1.00v to 1.25v or 1.35v to 1.6v • shutdown range: <1.0v or >1.6v |

Temperature**To access Temperature data:**

1. In the Environmental window, click the Temperature tab. The following data appears:

| Environmental | | | | |
|---------------|--------------------|-----------------------------|----------------------------|--------------|
| Voltage | Temperature | Fans | Power supplies | Cards |
| Index | Temperature source | Description | Current temperature (de... | Sensor state |
| 1 | ds1624sCPU | Host processor PROM Temp... | 39 | normal |

The following table defines the information displayed:

| Data | Description |
|---------------------------------------|--|
| Index | A monotonically increasing integer. When it reaches the maximum value the agent wraps the value back to 1. |
| Temperature source | Indicates the entity being monitored for temperature. |
| Description | Description of the temperature being monitored. |
| Current temperature (degrees Celsius) | The current temperature of the main board PROM in Celsius. |
| Sensor state | <p>Current state of the temperature which can have one of the following values:</p> <ul style="list-style-type: none"> • initial: temperature is at its initial state • normal: temperature is normal • minor alarm: temperature is greater than or equal to 53 degrees Celsius and less than 63 degrees Celsius • major alarm: temperature is greater than or equal to 63 degrees Celsius and less than 73 degrees Celsius • critical alarm: temperature is greater than 73 degrees Celsius • shutdown: system should be shutdown immediately • not present: temperature sensor does not exist • not functioning: temperature sensor is not functioning properly • unknown: cannot obtain information due to an internal error |

Fans**To access fan data:**

1. In the Environmental window, click the Fans tab. The following data appears:

| Environmental | | | | |
|---------------|-------------|-------------|-----------------------------|-----------|
| Voltage | Temperature | Fans | Power supplies | Cards |
| Index | Location | Description | Current speed (% of ran...) | Fan state |
| 1 | right | Fan 2 speed | 99 | normal |
| 2 | middle | Fan 3 speed | 100 | normal |
| . | | | | |

The following table defines the information displayed:

| Data | Description |
|-------------|--|
| Index | A monotonically increasing integer. When it reaches the maximum value the agent wraps the value back to 1. |
| Location | Location of the fan. Values are: <ul style="list-style-type: none"> • left fan • middle fan • right fan |
| Description | Description of the fan. Values are: <ul style="list-style-type: none"> • fan 1 • fan 2 • fan 3 |

| Data | Description |
|----------------------------|---|
| Current speed (% or range) | Current measurement of fan speed in percentage |
| Fan state | <p>Current state of the fan speed. Values are:</p> <ul style="list-style-type: none"> • initial: fan speed is at its initial state • normal: fan speed is normal • minor: fan speed is between 75% and 90% of the full fan speed • major: fan speed is between 50% and 75% of the full fan speed • critical: fan speed is less than 50% of the full fan speed • shutdown: system should be shutdown immediately • not present: fan sensor does not exist • not functioning: fan sensor is not functioning properly • unknown: cannot obtain information due to an internal error |

Power Supplies

To access Power supplies data:

1. In the IP window, click the Power supplies tab. The following data appears:

| Power supplies | | | |
|----------------|----------|----------------|------------|
| Index | Location | Description | State |
| 1 | left | Power supply A | normal |
| 2 | right | Power supply B | notPresent |

The following table defines the information displayed:

| Data | Description |
|----------|--|
| Index | A monotonically increasing integer. When it reaches the maximum value the agent wraps the value back to 1. |
| Location | <p>Location of the power supply. Values are:</p> <ul style="list-style-type: none"> • Left power supply (A) • Right power supply (B) |

| Data | Description |
|-------------|---|
| Description | Description of the power supply. Values are: <ul style="list-style-type: none">• Power supply A• Power supply B |
| State | Current state of the power supply. Values are: <ul style="list-style-type: none">• normal: the power supply is normal• unknown: the power supply sensor does not exist |

Cards

To access card data:

1. In the IP window, click the Cards tab. The following data appears:

| Cards | | | |
|-------|----------|-------------|--------|
| Index | Location | Description | State |
| 1 | left | Phy 0 | normal |
| 2 | right | Phy 1 | normal |

The following table defines the information displayed:

| Data | Description |
|-------------|---|
| Index | A monotonically increasing integer. When it reaches the maximum value the agent wraps the value back to 1. |
| Location | Location of the phy card. Values are: <ul style="list-style-type: none">• left phy card (Phy 0)• right phy card (Phy 1) |
| Description | Description of the phy card. Values are: <ul style="list-style-type: none">• Phy 0 for the left phy card• Phy 1 for the right phy card |
| State | The current state of the phy card. Values are: <ul style="list-style-type: none">• normal: state of the phy card is normal• unknown: phy card is not present |

Viewing Session Information

This section describes the session data displayed by the Net-Net EMS.

Displaying Session Data

When viewing session information, you can customize the table data in increments of 50, 75, or 100 records. The default is 50 records retrieved at a time.

You can specify the number of records to display on the following tabs:

- SIP session agents
- Realm
- H323 session agents
- Combined session agents

Specifying the Number of Records to Display

To specify the number of records displayed:

1. **Number to retrieve**—Click a number from the dropdown list to choose the number of records you want displayed. You can choose from increments of 50, 75, or 100 records. The default number of records displayed is 50. Then you must click one of the following:
 - **Restart**—Retrieves the first set of records in the increment specified. For example, if you click 75 in the **Number to retrieve** dropdown list, when you click **Restart**, you will get the first 75 records.
 - **More**—Retrieves the next set of records in the increment specified. For example, if you click 75 in the **Number to retrieve** dropdown list, when you click **More**, there will be 75 records displayed.

If you click **More** again, there will be 150 records displayed, and so on. The more button is disabled, or grayed out, when all records are retrieved.

The **Number currently in the table** field lists the number of records retrieved. This is not an editable field and is informational only.

Displaying All Records

To display all records:

1. **All**—Click **All** to retrieve and display all records.

Refreshing Records

To refresh the records displayed in the table:

1. **Refresh**—Click **Refresh** to refresh the data of the records previously retrieved.

Saving Records

To save the records displayed in the table:

1. **Export**—Click **Export** to export and save the records to a file.

| | | | | | | |
|---------------------------|-----|--|-------------------------------------|------------------------------------|---------------------------|-----|
| Number to retrieve | 75 | <input type="button" value="Restart"/> | <input type="button" value="More"/> | <input type="button" value="All"/> | Number currently in table | 375 |
| | 50 | | | | | |
| | 75 | | | | | |
| | 100 | | | | | |

Accessing Session Data

To access session data:

1. From the Performance data window, click the Session tab. Session data for the following categories appears:
 - SIP session agents
 - Current details
 - Average/period state
 - Realm
 - Current details
 - Average/period state
 - Monthly minutes
 - QoS
 - H.323 session agents
 - Current details
 - Average/period state
 - Combined session agents
 - Current details
 - Average/period state

SIP Session Agents

To access SIP session agent data:

1. In the Session window, click the SIP session agents tab.
2. Click the Current details tab. The following data appears:

The screenshot shows a software interface for managing session agents. At the top, there are tabs for "SIP session agents", "Realm", "H323 session agents", and "Combined session agents". Below these tabs, there are two sub-tabs: "Current details" (which is selected) and "Average/period state". The main area is a table with the following data:

| Hostname | Index | Session type | Status | Inbound curr... | Inbound curr... | Outbound curr... | Outbound curr... | Inbound sess... |
|----------|-------|--------------|-----------|-----------------|-----------------|------------------|------------------|-----------------|
| sip-sa | 1 | sip | inService | 0 | 0 | 0 | 0 | 0 |
| sip-sa1 | 2 | sip | inService | 0 | 0 | 0 | 0 | 0 |
| sip-sa2 | 3 | sip | inService | 0 | 0 | 0 | 0 | 0 |

The following table defines the information displayed:

| Data | Description |
|--------------------------------|---|
| Hostname | The hostname of the session agent for which the following statistics are being calculated |
| Index | A monotonically increasing integer for the sole purpose of indexing session agents. When it reaches the maximum value the agent wraps the value back to 1. |
| Session type | The type of the specified session agent, SIP |
| Status | The current status of the specified session agent, which is expressed as: <ul style="list-style-type: none"> • inService • outOfService • outOfServiceconstraintsViolation • BecomingOutOfService • ForcedOutOfService |
| Inbound | |
| Current active sessions | Number of current active inbound sessions |
| Current session rate (CPS) | Current inbound session rate in CPS |
| Outbound | |
| Current active sessions | Number of current active outbound sessions |
| Current session rate (CPS) | Current outbound session rate in CPS |
| Period-based statistics | |
| Inbound | |
| Session admitted | Total number of inbound sessions during the period |
| Session not admitted | Total number of inbound sessions rejected due to insufficient bandwidth |
| Outbound | |
| Sessions admitted | Total number of outbound sessions during the period |
| Sessions not admitted | Total number of outbound sessions rejected because of insufficient bandwidth |

3. Click the Average/period state tab. The following data appears:

| SIP session agents Realm H323 session agents Combined session agents | | | | | | | |
|--|-------|--------------|-----------|-----------------|-----------------|-----------------|--------------|
| Current details Average/period state | | | | | | | |
| Hostname | Index | Session type | Status | Inbound high... | Inbound aver... | Outbound hig... | Outbound av. |
| sip-sa | 1 | sip | inService | 0 | 0 | 0 | 0 |
| sip-sa1 | 2 | sip | inService | 0 | 0 | 0 | 0 |
| sip-sa2 | 3 | sip | inService | 0 | 0 | 0 | 0 |

The following table defines the information displayed:

| Data | Description |
|------------------------------------|---|
| Hostname | The hostname of the session agent for which the following statistics are being calculated |
| Index | A monotonically increasing integer for the sole purpose of indexing session agents. When it reaches the maximum value the agent wraps the value back to 1. |
| Session type | The type of the specified session agent, SIP |
| Status | The current status of the specified session agent, which is expressed as: <ul style="list-style-type: none"> • inService • outOfService • outOfServiceconstraintsViolation • BecomingoutOfService • ForcedoutOfService |
| Period-based statistics | |
| Inbound | |
| Highest number concurrent sessions | Highest number of concurrent inbound sessions during the period. |
| Average session rate (CPS) | Average rate of inbound sessions during the period in CPS |

| Data | Description |
|--|---|
| Outbound | |
| Highest number concurrent sessions | Highest number of concurrent outbound sessions during the period |
| Period-based statistics | |
| Max burst rate (in+out) (CPS) | Maximum burst rate of traffic measured during the period (combined inbound and outbound) |
| Total seizures | Total number of seizures during the period |
| Total answered sessions | Total number of answered sessions during the period |
| Answer/Seizure ratio (%) | The answer-to-seizure ratio, expressed as a percentage. For example, a value of 90 would represent 90%, or .90. |
| Average one-way signaling latency (ms) | Average observed one-way signaling latency during the period |
| Maximum one-way signaling latency (ms) | Maximum observed one-way signaling latency during the period |

Realm**To access realm data:**

1. In the Session window, click the Realm tab.
2. Click the Current details tab. The following data appears:

The screenshot shows a software interface titled "Session". At the top, there are tabs: "SIP session agents", "Realm" (which is highlighted in blue), "H323 session agents", and "Combined session agents". Below these, a sub-tab bar includes "Current details" (selected, highlighted in blue), "Average/period state", "Monthly minutes", and "QoS". The main content area displays a table with the following columns: Index, Realm name, Realm status, Inbound curr..., Inbound curr..., Outbound curr..., Outbound curr..., and Inbound sessi. The table contains 9 rows, each representing a realm named "access", "access1", "access2", "access3", "acme", "core", "core1", "core2", and "core3", all in an "inService" status. All numerical values in the table are zero.

| SIP session agents | Realm | H323 session agents | Combined session agents | | | | |
|--------------------|----------------------|---------------------|-------------------------|-----------------|------------------|------------------|---------------|
| Current details | Average/period state | Monthly minutes | QoS | | | | |
| Index | Realm name | Realm status | Inbound curr... | Inbound curr... | Outbound curr... | Outbound curr... | Inbound sessi |
| 1 | access | inService | 0 | 0 | 0 | 0 | 0 |
| 2 | access1 | inService | 0 | 0 | 0 | 0 | 0 |
| 3 | access2 | inService | 0 | 0 | 0 | 0 | 0 |
| 4 | access3 | inService | 0 | 0 | 0 | 0 | 0 |
| 5 | acme | inService | 0 | 0 | 0 | 0 | 0 |
| 6 | core | inService | 0 | 0 | 0 | 0 | 0 |
| 7 | core1 | inService | 0 | 0 | 0 | 0 | 0 |
| 8 | core2 | inService | 0 | 0 | 0 | 0 | 0 |
| 9 | core3 | inService | 0 | 0 | 0 | 0 | 0 |

The following table defines the information displayed:

| Data | Description |
|--------------------------------|--|
| Index | A monotonically increasing integer for the sole purpose of indexing realms. When it reaches the maximum value the agent wraps the value back to 1. |
| Realm name | The name of the realm for which the following statistics are being calculated |
| Realm status | Current status of the specified realm, which is expressed as INS, constraintViolation, or callLoadReduction. |
| Inbound | |
| Current active sessions | Number of current active inbound sessions |
| Current session rate (CPS) | Current Inbound Session rate in CPS |
| Outbound | |
| Current active sessions | Number of current active outbound sessions |
| Current session rate (CPS) | Current outbound session rate in CPS |
| Period-based statistics | |

| Data | Description |
|-----------------------|---|
| Short sessions | The lifetime number of sessions whose duration was less than the configured short session duration. |
| Inbound | |
| Session admitted | Total number of inbound sessions during the period |
| Session not admitted | Total number of inbound sessions rejected due to insufficient bandwidth |
| Outbound | |
| Sessions admitted | Total number of outbound sessions during the period |
| Sessions not admitted | Total number of outbound sessions rejected because of insufficient bandwidth |

3. Click the Average/period state tab. The following data appears:

| Index | Realm name | Realm status | Inbound high... | Inbound aver... | Outbound hig... | Outbound av... | Max burst rat. |
|-------|------------|--------------|-----------------|-----------------|-----------------|----------------|----------------|
| 1 | access | inService | 0 | 0 | 0 | 0 | 1 |
| 2 | access1 | inService | 0 | 0 | 0 | 0 | 1 |
| 3 | access2 | inService | 0 | 0 | 0 | 0 | 0 |
| 4 | access3 | inService | 0 | 0 | 0 | 0 | 1 |
| 5 | acme | inService | 0 | 0 | 0 | 0 | 1 |
| 6 | core | inService | 0 | 0 | 0 | 0 | 1 |
| 7 | core1 | inService | 0 | 0 | 0 | 0 | 1 |
| 8 | core2 | inService | 0 | 0 | 0 | 0 | 1 |
| 9 | core3 | inService | 0 | 0 | 0 | 0 | 1 |

The following table defines the information displayed:

| Data | Description |
|--------------|--|
| Index | A monotonically increasing integer for the sole purpose of indexing realms. When it reaches the maximum value the agent wraps the value back to 1. |
| Realm name | The name of the realm for which the following statistics are being calculated |
| Realm status | Current status of the specified realm, which is expressed as INS, constraintViolation, or callLoadReduction. |

| Data | Description |
|------------------------------------|--|
| Period-based statistics | |
| Inbound | |
| Highest number concurrent sessions | Highest number of concurrent inbound sessions during the period |
| Average session rate (CPS) | |
| Outbound | |
| Highest number concurrent sessions | Highest number of concurrent outbound sessions during the period |
| Average session rate | Average rate of outbound sessions during the period in CPS |
| Period-based statistics | |
| Max burst rate (in+out) (CPS) | Maximum burst rate of traffic measured during the period (combined inbound and outbound) |
| Total seizures | Total number of seizures during the period |
| Total answered sessions | Total number of answered sessions during the period |
| Answer/Seizure ratio (%) | The answer-to-seizure ratio, expressed as a percentage |
| Average latency | Average observed signaling latency during the period |
| Max latency | Maximum observed signaling latency during the period |

4. Click the Monthly minutes tab. The following data appears:

| SIP session agents | Realm | H323 session agents | Combined session agents | |
|--------------------|----------------------|---------------------|-------------------------|--|
| Current details | Average/period state | Monthly minutes | QoS | |
| | | | | |
| | | | | |

The following table defines the information displayed:

| Data | Description |
|------------------|--|
| Index | A monotonically increasing integer for the sole purpose of indexing realms. When it reaches the maximum value the agent wraps the value back to 1. |
| Realm name | The name of the realm for which the following statistics are being calculated |
| Realm status | Current status of the specified realm, which is expressed as INS, constraintViolation, or callLoadReduction. |
| Minutes left | The number of monthly-minutes left in the pool per calendar month for a given realm. |
| Minutes rejected | The number of rejected calls due to monthly-minutes constraints exceeded. |

5. Click the QoS tab. The following data appears:

| Current details Average/period state Monthly minutes [QoS] | | | | | | | |
|--|------------|--------------|------------------|-----------------|------------------|-----------------|------------------|
| Index | Realm name | Realm status | Period averag... | Period maxim... | Period exceee... | Total exceee... | Period exceee... |
| 1 | access | inService | 0 | 0 | 0 | 0 | 0 |
| 2 | access1 | inService | 0 | 0 | 0 | 0 | 0 |
| 3 | access2 | inService | 0 | 0 | 0 | 0 | 0 |
| 4 | access3 | inService | 0 | 0 | 0 | 0 | 0 |
| 5 | acme | inService | 0 | 0 | 0 | 0 | 0 |
| 6 | core | inService | 0 | 0 | 0 | 0 | 0 |
| 7 | core1 | inService | 0 | 0 | 0 | 0 | 0 |
| 8 | core2 | inService | 0 | 0 | 0 | 0 | 0 |
| 9 | core3 | inService | 0 | 0 | 0 | 0 | 0 |

The following table defines the information displayed:

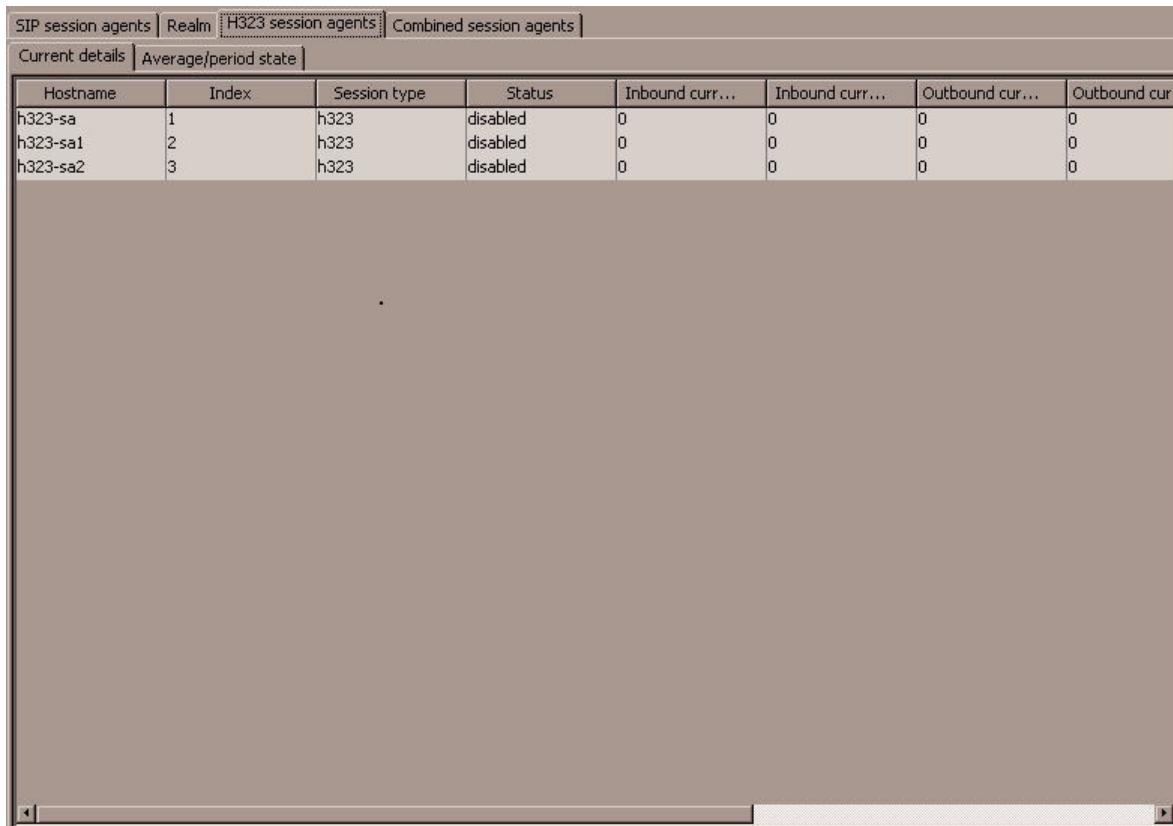
| Data | Description |
|------------|--|
| Index | A monotonically increasing integer for the sole purpose of indexing realms. When it reaches the maximum value the agent wraps the value back to 1. |
| Realm name | The name of the realm for which the following statistics are being calculated |

| Data | Description |
|--------------------------------|--|
| Realm status | Current status of the specified realm, which is expressed as INS, constraintViolation, or callLoadReduction. |
| Period-based statistics | |
| Period average QoS | Average QoS factor observed during the period. |
| Period maximum QoS | Maximum QoS factor observed during the period. |
| Period exceeded major | Peg counts the number of times the major Rfactor threshold was exceeded during the period. |
| Total exceeded major | Peg counts the number of times the major Rfactor threshold was exceeded during the lifetime. |
| Period exceeded critical | Peg counts the number of times the critical Rfactor threshold was exceeded during the period. |
| Total exceeded critical | Peg counts the number of times the critical Rfactor threshold was exceeded during the lifetime. |

H.323 Session Agents

To access H.323 session agent data:

1. In the Session window, click the H.323 session agents tab.
2. Click the Current details tab. The following data appears:



The screenshot shows a software interface for managing session agents. At the top, there are tabs: SIP session agents, Realm, H323 session agents (which is the active tab), and Combined session agents. Below the tabs, there are two sub-tabs: Current details (which is active) and Average/period state. The main area displays a table of session data. The columns are: Hostname, Index, Session type, Status, Inbound curr..., Inbound curr..., Outbound cur..., and Outbound cur... (with ellipses indicating continuation). There are three rows of data corresponding to hosts h323-sa, h323-sa1, and h323-sa2. All sessions are listed as disabled with a value of 0 for all metrics.

| Hostname | Index | Session type | Status | Inbound curr... | Inbound curr... | Outbound cur... | Outbound cur... |
|----------|-------|--------------|----------|-----------------|-----------------|-----------------|-----------------|
| h323-sa | 1 | h323 | disabled | 0 | 0 | 0 | 0 |
| h323-sa1 | 2 | h323 | disabled | 0 | 0 | 0 | 0 |
| h323-sa2 | 3 | h323 | disabled | 0 | 0 | 0 | 0 |

The following table defines the information displayed:

| Data | Description |
|--------------------------------|---|
| Hostname | The hostname of the session agent for which the statistics are being calculated |
| Index | A monotonically increasing integer for the sole purpose of indexing session agents. When it reaches the maximum value the agent wraps the value back to 1. |
| Session type | The type of the specified session agent, H.323 |
| Status | The current status of the specified session agent, which is expressed as: <ul style="list-style-type: none"> • inService • outOfService • outOfServiceconstraintsViolation • BecomingOutOfService • ForcedOutOfService |
| Inbound | |
| Current active sessions | Number of current active inbound sessions |
| Current session rate (CPS) | Current Inbound Session rate in CPS |
| Outbound | |
| Current active sessions | Number of current active outbound sessions |
| Current session rate (CPS) | Current outbound session rate in CPS |
| Period-based statistics | |
| Inbound | |
| Session admitted | Total number of inbound sessions during the period |
| Session not admitted | Total number of inbound sessions rejected due to insufficient bandwidth |
| Outbound | |
| Sessions admitted | Total number of outbound sessions during the period |
| Sessions not admitted | Total number of outbound sessions rejected because of insufficient bandwidth |

3. Click the Average/period state tab. The following data appears:

| H323 session agents | | | | | | | | |
|----------------------|-------|--------------|----------|-----------------|-----------------|-----------------|--------------|--|
| Current details | | | | | | | | |
| Average/period state | | | | | | | | |
| Hostname | Index | Session type | Status | Inbound high... | Inbound aver... | Outbound hig... | Outbound av. | |
| h323-sa | 1 | h323 | disabled | 0 | 0 | 0 | 0 | |
| h323-sa1 | 2 | h323 | disabled | 0 | 0 | 0 | 0 | |
| h323-sa2 | 3 | h323 | disabled | 0 | 0 | 0 | 0 | |

The following table defines the information displayed:

| Data | Description |
|--|---|
| Hostname | The hostname of the session agent for which the statistics are being calculated |
| Index | A monotonically increasing integer for the sole purpose of indexing session agents. When it reaches the maximum value the agent wraps the value back to 1. |
| Session type | The type of the specified session agent, H.323 |
| Status | The current status of the specified session agent, which is expressed as: <ul style="list-style-type: none"> • inService • outOfService • outOfServiceconstraintsViolation • BecomingOutOfService • ForcedOutOfService |
| Period-based statistics | |
| Inbound | |
| Highest number concurrent sessions | Highest number of concurrent inbound sessions during the period |
| Average session rate (CPS) | Average rate of inbound sessions during the period in CPS |
| Outbound | |
| Highest number concurrent sessions | Highest number of concurrent outbound sessions during the period |
| Average session rate | Average rate of outbound sessions during the period in CPS |
| Period-based statistics | |
| Max burst rate (in+out) (CPS) | Maximum burst rate of traffic measured during the period (combined inbound and outbound) |
| Total seizures | Total number of seizures during the period |
| Total answered sessions | Total number of answered sessions during the period |
| Answer/Seizure ratio (%) | The answer-to-seizure ratio, expressed as a percentage. For example, a value of 90 would represent 90%, or .90. |
| Average one-way signaling latency (ms) | Average observed one-way signaling latency during the period |
| Maximum one-way signaling latency (ms) | Maximum observed one-way signaling latency during the period |

Combined Session Agents

To access Address data:

1. In the Session window, click the Combined session agents tab.
2. Click the Current details tab. The following data appears:

| Combined session agents | | | | | | | |
|-------------------------|-------|----------------------|-----------|-----------------|-----------------|------------------|------------------|
| Current details | | Average/period state | | | | | |
| Hostname | Index | Session type | Status | Inbound curr... | Inbound curr... | Outbound curr... | Outbound curr... |
| sip-sa | 1 | sip | inService | 0 | 0 | 0 | 0 |
| sip-sa1 | 2 | sip | inService | 0 | 0 | 0 | 0 |
| sip-sa2 | 3 | sip | inService | 0 | 0 | 0 | 0 |
| h323-sa | 4 | h323 | disabled | 0 | 0 | 0 | 0 |
| h323-sa1 | 5 | h323 | disabled | 0 | 0 | 0 | 0 |
| h323-sa2 | 6 | h323 | disabled | 0 | 0 | 0 | 0 |

The following table defines the information displayed:

| Data | Description |
|-------------------------|---|
| Hostname | The hostname of the session agent for which the following statistics are being calculated |
| Index | A monotonically increasing integer for the sole purpose of indexing session agents. When it reaches the maximum value the agent wraps the value back to 1. |
| Session type | The type of the specified session agent, SIP or H.323 |
| Status | The current status of the specified session agent, which is expressed as: <ul style="list-style-type: none"> • inService • outOfService • outOfServiceconstraintsViolation • BecomingoutOfService • ForcedoutOfService |
| Inbound | |
| Current active sessions | Number of current active inbound sessions |

| Data | Description |
|--------------------------------|--|
| Current session rate (CPS) | Current Inbound Session rate in CPS |
| Outbound | |
| Current active sessions | Number of current active outbound sessions |
| Current session rate (CPS) | Current outbound session rate in CPS |
| Period-based statistics | |
| Inbound | |
| Session admitted | Total number of inbound sessions during the period |
| Session not admitted | Total number of inbound sessions rejected due to insufficient bandwidth |
| Outbound | |
| Sessions admitted | Total number of outbound sessions during the period |
| Sessions not admitted | Total number of outbound sessions rejected because of insufficient bandwidth |

3. Click the Average/period state tab. The following data appears:

| H323 session agents | | | | | | | |
|---------------------|-------|--------------|----------|-----------------|-----------------|-----------------|--------------|
| Current details | | | | | | | |
| Hostname | Index | Session type | Status | Inbound high... | Inbound aver... | Outbound hig... | Outbound av. |
| h323-sa | 1 | h323 | disabled | 0 | 0 | 0 | 0 |
| h323-sa1 | 2 | h323 | disabled | 0 | 0 | 0 | 0 |
| h323-sa2 | 3 | h323 | disabled | 0 | 0 | 0 | 0 |

The following table defines the information displayed:

| Data | Description |
|--|---|
| Hostname | The hostname of the session agent for which the following statistics are being calculated |
| Index | A monotonically increasing integer for the sole purpose of indexing session agents. When it reaches the maximum value the agent wraps the value back to 1. |
| Session type | The type of the specified session agent, SIP or H.323 |
| Status | The current status of the specified session agent, which is expressed as: <ul style="list-style-type: none">• inService• outOfService• outOfServiceconstraintsViolation• BecomingoutOfService• ForcedoutOfService |
| Period-based statistics | |
| Inbound | |
| Highest number concurrent sessions | Highest number of concurrent inbound sessions during the period |
| Average session rate (CPS) | Average rate of inbound sessions during the period in CPS |
| Outbound | |
| Highest number concurrent sessions | Highest number of concurrent outbound sessions during the period |
| Average session rate | Average rate of outbound sessions during the period in CPS |
| Period-based statistics | |
| Max burst rate (in+out) (CPS) | Maximum burst rate of traffic measured during the period (combined inbound and outbound) |
| Total seizures | Total number of seizures during the period |
| Total answered sessions | Total number of answered sessions during the period |
| Answer/Seizure ratio (%) | The answer-to-seizure ratio, expressed as a percentage. For example, a value of 90 would represent 90%, or .90. |
| Average one-way signaling latency (ms) | Average observed one-way signaling latency during the period |
| Maximum one-way signaling latency (ms) | Maximum observed one-way signaling latency during the period |

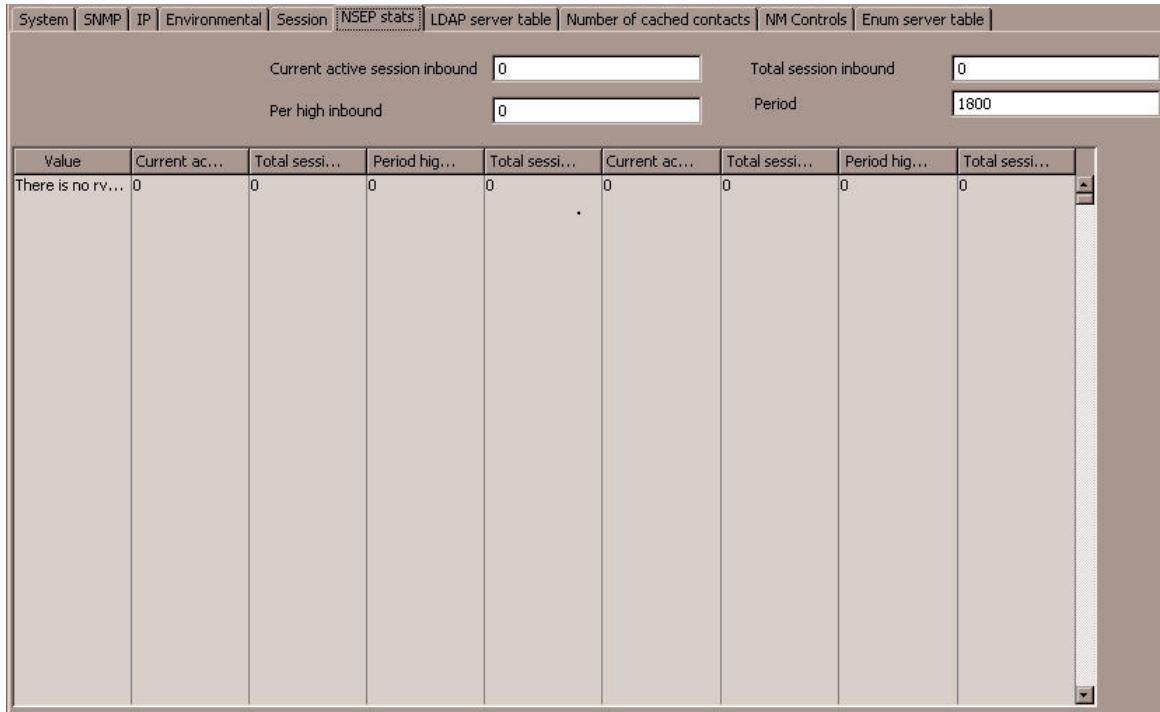
Viewing NSEP Information

This section describes the NSEP data displayed by the Net-Net EMS.

Accessing NSEP Data

To access NSEP data:

- From the Performance data screen, click the NSEP stats tab. Data for the following categories appears:



| Value | Current ac... | Total sessi... | Period hig... | Total sessi... | Current ac... | Total sessi... | Period hig... | Total sessi... |
|-------------------|---------------|----------------|---------------|----------------|---------------|----------------|---------------|----------------|
| There is no rv... | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

The following table defines the information displayed:

| Data | Description |
|--------------------------------------|---|
| Value | Specific value used for indexing |
| Current active sessions inbound | Number of current active NSEP sessions |
| Total sessions inbound | Total number of inbound NSEP sessions during the period |
| Period high inbound | Highest number of concurrent inbound NSEP sessions during the period |
| Total sessions not admitted inbound | Total number of inbound NSEP sessions rejected |
| Current active sessions outbound | Number of current active outbound NSEP sessions |
| Total sessions outbound | Total number of outbound NSEP sessions during the period |
| Period high outbound | Highest number of concurrent outbound NSEP sessions during the period |
| Total sessions not admitted outbound | Total number of outbound NSEP sessions rejected |

Viewing LDAP Server Information

This section describes the LDAP server table information displayed by the Net-Net EMS.

Accessing LDAP Server Data

To access LDAP server data:

- From the Performance data screen, click the LDAP server table tab. Data for the following categories appears:

| LDAP config name | LDAP server IP address | LDAP server status |
|------------------|------------------------|--------------------|
| | | |

The following table defines the information displayed:

| Data | Description |
|------------------------|--|
| LDAP config name | The name of the LDAP configuration for which the statistics are being calculated |
| LDAP server IP address | The IP address of the LDAP server for which the statistics are being calculated |
| LDAP server status | The status for this LDAP server |

Viewing Number of Cached Contacts

This section describes the number of cached contact data displayed by the Net-Net EMS.

Accessing Number of Cached Contacts

To access number of cached contacts data:

- From the Performance data screen, click the Number of cached contacts tab.
Data for the following categories appears:

| | | | | | | | | | |
|--|------|----|---------------|---------|------------|-------------------|---------------------------|-------------|-------------------|
| System | SNMP | IP | Environmental | Session | NSEP stats | LDAP server table | Number of cached contacts | NM Controls | Enum server table |
| Active SIP local contacts 0 MGCP GW endpoints 0 H.323 registrations 0 | | | | | | | | | |

The following table defines the information displayed:

| Data | Description |
|---------------------------|-------------------------------------|
| Active SIP local contacts | Number of active SIP local contacts |
| MGCP GW endpoints | Number of MGCP GW endpoints |
| H.323 registrations | Number of H.323 registrations |

Viewing Trap Table Summary Information

This section describes the summary of trap data generated by the Net-Net SBC.

Displaying Trap Table Data

When viewing trap data, you can customize the table data in increments of 50, 75, or 100 records. The default is 50 records retrieved at a time.

Specifying the Number of Records to Display

To specify the number of records displayed:

1. **Number to retrieve**—Click a number in the dropdown list to choose the number of records you want displayed. You can choose from increments of 50, 75, or 100 records. The default number of records displayed is 50. Then you must click one of the following:
 - **Restart**—Retrieves the first set of records in the increment specified. For example, if you click 75 in the **Number to retrieve** dropdown list, when you click **Restart**, you will get the first 75 records.
 - **More**—Retrieves the next set of records in the increment specified. For example, if you click 75 in the **Number to retrieve** dropdown list, when you click **More**, there will be 75 records displayed.

If you click **More** again, there will be 150 records displayed, and so on. The **more** button is disabled, or grayed out, when all records are retrieved.

The **Number currently in the table** field lists the number of records retrieved. This is not an editable field and is informational only.

Displaying All Records

To display all records:

1. **All**—Click **All** to retrieve and display all records.

Refreshing Records

To refresh the records displayed in the table:

1. **Refresh**—Click **Refresh** to refresh the data of the records previously retrieved.

Saving Records

To save the records displayed in the table:

1. **Export**—Click **Export** to export and save the records to a file.

| | | | | | | | | | | | |
|--------------------|----|----|----|-----|---------|------|-----|---------------------------|-----|---------|--------|
| Number to retrieve | 75 | 50 | 75 | 100 | Restart | More | All | Number currently in table | 375 | Refresh | Export |
|--------------------|----|----|----|-----|---------|------|-----|---------------------------|-----|---------|--------|

Accessing Trap Table Summary Data

To access Trap table summary data:

- From the Performance data screen, click the Trap table summary tab. Data for the following categories appears:

| System | SNMP | IP | Environmental | Session | NSEP stats | LDAP server table | Number of cached contacts | Trap table summary | NM Controls | Enum server t |
|-------------------|----------------|----------|---------------------------------|---------|------------|-------------------|---------------------------|----------------------------------|-------------|---------------|
| System time | Instance index | Num data | System uptime | | | | | Trap oid | | |
| 2009-3-23 9:56:32 | 1 | 0 | 0 hours, 0 minutes, 45 seconds. | | | | | coldStart | | |
| 2009-3-23 9:56:38 | 1 | 3 | 0 hours, 0 minutes, 50 seconds. | | | | | apEnvMonStatusChangeNotification | | |
| 2009-3-23 9:56:38 | 2 | 3 | 0 hours, 0 minutes, 50 seconds. | | | | | apEnvMonStatusChangeNotification | | |
| 2009-3-23 9:56:38 | 3 | 3 | 0 hours, 0 minutes, 50 seconds. | | | | | apEnvMonStatusChangeNotification | | |
| 2009-3-23 9:56:38 | 4 | 3 | 0 hours, 0 minutes, 50 seconds. | | | | | apEnvMonStatusChangeNotification | | |
| 2009-3-23 9:56:38 | 5 | 3 | 0 hours, 0 minutes, 50 seconds. | | | | | apEnvMonStatusChangeNotification | | |
| 2009-3-23 9:56:39 | 1 | 2 | 0 hours, 0 minutes, 51 seconds. | | | | | apSysMgmtGroupTrap | | |
| 2009-3-23 9:56:39 | 2 | 3 | 0 hours, 0 minutes, 51 seconds. | | | | | apEnvMonStatusChangeNotification | | |
| 2009-3-23 9:56:39 | 3 | 3 | 0 hours, 0 minutes, 51 seconds. | | | | | apEnvMonStatusChangeNotification | | |
| 2009-3-23 9:56:39 | 4 | 3 | 0 hours, 0 minutes, 51 seconds. | | | | | apEnvMonStatusChangeNotification | | |
| 2009-3-23 9:56:39 | 5 | 3 | 0 hours, 0 minutes, 51 seconds. | | | | | apEnvMonStatusChangeNotification | | |
| 2009-3-23 9:56:39 | 6 | 3 | 0 hours, 0 minutes, 51 seconds. | | | | | apEnvMonStatusChangeNotification | | |
| 2009-3-23 9:56:39 | 7 | 3 | 0 hours, 0 minutes, 51 seconds. | | | | | apEnvMonStatusChangeNotification | | |
| 2009-3-23 9:56:39 | 8 | 3 | 0 hours, 0 minutes, 51 seconds. | | | | | apEnvMonStatusChangeNotification | | |

The following table defines the information displayed

| Data | Description |
|----------------|---|
| System time | The system time of the Net-Net SBC. |
| Instance index | The instance index of the trapID incremented with a resolution of a second. |
| Num data | The number of information encoded in the trap. |
| System uptime' | The snmp sysUptime when the trap was generated. |
| Trap oid | The trapID associated with the fault condition. |

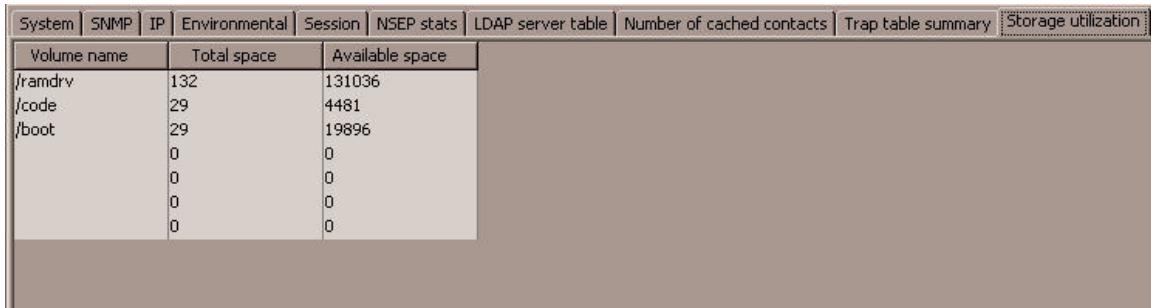
Viewing Storage Utilization Information

This section describes the summary of storage utilization data generated by the Net-Net SBC.

Accessing Storage Utilization Data

To access storage utilization data:

- From the Performance data screen, click the Storage Utilization tab. Storage utilization data for the following categories appears:



The screenshot shows a table with three columns: Volume name, Total space, and Available space. The data is as follows:

| Volume name | Total space | Available space |
|-------------|-------------|-----------------|
| /ramdrv | 132 | 131036 |
| /code | 29 | 4481 |
| /boot | 29 | 19896 |
| | 0 | 0 |
| | 0 | 0 |
| | 0 | 0 |
| | 0 | 0 |

The following table defines the information displayed:

| Data | Description |
|-----------------|--|
| Volume name | The name of the disk partition as defined by the user. |
| Total space | Total amount of disk space. |
| Available space | Available, free disk space available. |

Viewing IDS Information

This section describes the intrusion detection system (IDS) data displayed by the Net-Net EMS.

Accessing IDS Data

To access IDS data:

- From the Performance data screen, click the IDS tab. IDS data for the following categories appears:

| System | | SNMP | IP | Environmental | Session | NSEP stats | LDAP server table | Number of cached contacts | Trap table summary | Storage utilization | <input checked="" type="checkbox"/> IDS | NM Co |
|---|--|------|----|---------------|---------|------------|-------------------|---------------------------|--------------------|---------------------|---|-------|
| SIP endpoint demotions from trusted to untrusted | | 0 | | | | | | | | | | |
| SIP endpoint demotions from untrusted to denied | | 0 | | | | | | | | | | |
| MGCP endpoint demotions from trusted to untrusted | | 0 | | | | | | | | | | |
| MGCP endpoint demotions from untrusted to denied | | 0 | | | | | | | | | | |

The following table defines the information displayed:

| Data | Description |
|---|---|
| SIP endpoint demotions from trusted to untrusted | Global counters for SIP endpoint demotions from trusted to untrusted. |
| SIP endpoint demotions from untrusted to denied | Global counters for SIP endpoint demotions from untrusted to denied. |
| MGCP endpoint demotions from trusted to untrusted | Global counter for MGCP endpoint demotions from trusted to untrusted. |
| MGCP endpoint demotions from untrusted to denied | Global counters for MGCP endpoint demotions from untrusted to denied. |

Viewing Network Management Controls Information

This section describes the network management (NM) control data displayed by the Net-Net EMS.

Accessing NM Control Data

To access NM control data:

- From the Performance data screen, click the NM Controls tab. Session data for the following categories appears:

| NM Controls | | | | | | | | |
|---------------------|------|---------------|----------|---------------|-----------------|-----------------|------------|--|
| Name | Type | IncomingTotal | Rejected | DivertedTotal | IncomingCurr... | RejectedCurr... | DivertedCu | |
| There are no net... | | 0 | 0 | 0 | 0 | 0 | 0 | |

The following table defines the information displayed:

| Data | Description |
|---------------------|--|
| Name | Name of the network management control |
| Type | Type of network management control |
| Incoming Total | Total number of incoming calls that match a destination identifier |
| Rejected Total | Total number of incoming calls that are rejected |
| Diverted Total | Total number of incoming calls that are diverted |
| Incoming Current | Number of incoming calls during the current period that match a destination identifier |
| Rejected Current | Number of incoming calls that are rejected during the current period |
| Diverted Current | Number of incoming calls diverted during the current period |
| Incoming Period Max | Maximum number of incoming calls during a period that match a destination identifier |
| Rejected Period Max | Number of the maximum incoming calls rejected in a period |
| Diverted Period Max | Number of the maximum incoming calls diverted in a period |

Viewing ENUM Server Information

This section describes the ENUM server table data displayed by the Net-Net EMS.

Accessing ENUM Server Data

To access ENUM server data:

- From the Performance data screen, click the ENUM server table tab. ENUM server table data for the following categories appears:

| Enum config name | Enum server IP address | Enum server status |
|-----------------------|------------------------|--------------------|
| NoEnumAgentsAvailable | 0.0.0.0 | oosunreachable |

The following table defines the information displayed:

| Data | Description |
|------------------------|--------------------------------|
| Enum config name | Name of the ENUM configuration |
| Enum server IP address | IP address for the ENUM server |
| Enum server status | Status of the ENUM server |