

IntelliView® User Guide 1.2.0

940643-001, Revision A3



NORTH AMERICA | CENTRAL AMERICA | LATIN AMERICA | ASIA/PACIFIC RIM | EUROPE | MIDDLE EAST | AFRICA

VeriFone Systems, Inc.
2099 Gateway Place
Suite 600
San Jose, CA 95220
USA

Corporate Telephone: 1-800-VeriFone (837-4366)
Corporate Web Site: www.Verifone.com

IntelliView User Guide
Part Number: 940643-001
May 2013

Copyright 2013 by VeriFone Inc.

Printed in the United States of America.

All Rights Reserved.

This publication is proprietary to VeriFone Systems and is intended solely for use by its customers. This publication may not be reproduced or distributed for any purpose without the written permission of VeriFone.

The information VeriFone furnishes in this publication is believed to be accurate and reliable. However, the corporation assumes no responsibility for its use and reserves the right to make changes to the publication at any time without notice.

Trademarks

IntelliNAC and IntelliView are registered trademarks of VeriFone Inc. The VeriFone logo is the registered trademark of VeriFone.

This publication attempts to distinguish proprietary trademarks from descriptive terms by following the capitalization style the manufacturer uses. Every effort was made to supply complete and correct information. Any error in identifying or reflecting any proprietary marks or notices is inadvertent and unintentional.

Version	Date	Author	Description
1.0.1	11/7/2012	KO	Initial Release for 1.0
1.1	03/08/2013	RD	Updated for 1.1 added x.25 uplink config, DSO display, EFTSec passthru, Media trace, corrected the support email
1.2	05/15/2013	RD	Updated for 1.2 added

Table of Contents

CHAPTER 1- Introduction

Overview	1
Document Structure.....	1
Audience.....	1
Related Reading.....	1

CHAPTER 2- Product Overview

IntelliView.....	3
Supported Servers.....	4
Supported Clients	4
Licensing IntelliView	4
License Properties	5
License Dependencies	5
Installing a New License	6
Upgrading a License.....	6
Installation and Initial Setup.....	7
Install on Linux.....	8
Uninstall IntelliView.....	9
Upgrade IntelliView.....	9
Restore IntelliView	9
Stop IntelliView	9
Change Admin User Settings	10
Basic Operations	10
Logging On after Initial install:	11
Logging On after Initial Logon	13
Logging Off	13
Exiting IntelliView.....	13
Navigation.....	14
Main Screen	14
Map Views	15
System View	15
Network View	16
View Controls.....	16
Device Tree.....	17
Map	18
Device View	18
Icons	19
Device Icons.....	19
Submap Icons	20
Links	20
Synthetic Links.....	21
Toolbars.....	22
IntelliView Tools	22
Device Tools	22
Personal User Tools.....	23
My Profile	23
Help.....	24
Tables.....	24

Header	24
Data.....	24
Footer	25
Filtering	25
Paging.....	25
Sorting.....	26
Buttons	26
 CHAPTER 3-	
Getting Started	
Introduction	27
Security	27
System Accounts	27
Viewing Session Information	27
Authentication.....	28
Enable LDAP	29
Set up the LDAP Server	29
Set up Security Policy Strategy	29
Set up LDAP Authentication	30
Authorization.....	30
Permissions.....	31
Roles	31
Creating a Security Group	32
Modifying a Security Group	34
Deleting a Security Group	35
Exporting a Security Group	36
User Accounts	38
Configuration Data	38
Viewing User Accounts	38
Creating User Accounts.....	40
Deleting a User Account	42
Editing User Accounts	42
Permission Sets	44
Adding a Permission Set	44
Modifying a Permission Set	46
Deleting a Permission Set	47
Device Sets.....	48
Creating a Device Set.....	48
Modifying a Device Set.....	50
Deleting a Device Set	52
System Backup and Restore	53
Backup Types.....	53
Backup Permissions	54
System Backup for IntelliView	54
Backup Now	55
Restore Button	57
Export Backup File	57
Backup Configuration.....	58
Scheduled Backups	58
Scheduler Config.....	58
Scheduled Backups	59
Run Results.....	60

CHAPTER 4-
Configuration

Overview	63
Configure an IntelliNAC Node.....	63
Map Editing	64
Place Device.....	65
Add Unmanaged.....	65
Add Submap.....	66
Add Link.....	67
Move Device.....	68
Submap Properties.....	68
Editing a Submap Icon	68
Remove	69
Add Link (Device Icons).....	69
Link Path Details	69
NAC to NAC Configuration	72
Configure the NII's for load balance or fail over.....	93
Fail over	93
Load Balance	110
NAC to NAC with In-Band Management Configuration	126
Configure the Devices (Node).....	128
Configuring Nodes for In-Band Management.....	130
Configure the NII's for load balance	158
Load Balance	158
Alarm Configuration	174
Alarm Configuration Data	174
Alarm Overrides.....	174
Alarm Rules	178
Alarm Notifications.....	181
Email Configuration	187
Device File Manager Configuration	189
Uploading Files to IntelliView.....	190
Downloading Files from IntelliView	191
Staging Area.....	192
Uploading a File to the Device.....	193
Downloading a File from the Device	195
Statistics Configuration	197
Device Configuration (Node)	200
Online Device Configuration.....	200
Configuring a Device	200
System	201
Hardware.....	201
Configuring an I/O Module	201
General Port Configuration Navigation	203
Ethernet Port Configuration	205
ISDN PSTN Port Configuration	208
MFR2 PSTN Port Configuration	211
RBS PSTN Port Configuration.....	213
Analog PSTN Port Configuration	216
SNA Uplink Port Configuration	219
X.25 Uplink Port Configuration	225
X.25 Down Link Port Configuration	230

Transaction Routings	235
TCP/IP Downlinks Configuration	235
PSTN Downlinks Configuration	238
X.25 Downlinks Configuration	240
NII Lookup Tables Configuration	242
TCP/IP NII Table Configuration	242
DNIS NII Table Configuration	250
X.25 NII Table Configuration	259
CRI NII Table Configuration	267
NUA NII Table Configuration	269
Uplinks Configuration	271
TCP/IP Uplink Configuration	271
X.25 Uplink Configuration	274
SNA Uplink Configuration	276
Offline Device Configuration	278
Adding an Offline Configuration	278
Deleting an Offline Configuration	279
Copying an Offline Device Configuration	279
Manipulating the Configuration Objects	280
Downloading a Configuration	280
Uploading a Configuration	281
Split Dial Routing	283
Constraints	283
Configure Split Dial Routing	283

CHAPTER 5- Operations

Overview	285
Alarms and Events	285
Alarms	285
Alarm Details Screen	289
Alarm Rules	294
Alarm Dependencies	294
Events	294
Notifications	294
Events Table	294
Changing Elements	295
Archiving	296
Statistical Collection	297
Statistics Viewing	298
Manual Statistically Repository management	299
Manual Collect Statistics	300
Manual Reset All Statistics Now	301
Exporting Statistics	301
Electronic Funds Transfer Security	304
EFTSec TPDU Pass Through	304
Constrains	304
EFTSEC Operation	304

CHAPTER 6- Diagnostics

Table of Contents

Overview	305
Media Trace	305
Constraints	305
Media Trace Operation	306
Enable Trace	306
Disable Trace	309
View Trace Activity	310
View Trace Data	312
Transaction Trace	315
Logging Application Permissions	315
Trace Collection	316
Trace Log Viewer	316
Log Table Controls	317
Log Application Configuration	319
Log File Management	319
DS0 Channel Display	320
Constraints	320
View DS0 Channel Status	321

List of Figures

FIGURE 1. IntelliView Architecture	3
FIGURE 2. IntelliView Login screen.....	11
FIGURE 3. Initial IntelliView Login screen	12
FIGURE 4. IntelliView Login screen.....	13
FIGURE 5. Main screen	14
FIGURE 6. System view	16
FIGURE 7. View Controls region	17
FIGURE 8. Device Tree	17
FIGURE 9. Map tab.....	18
FIGURE 10. Device view for IntelliNAC	19
FIGURE 11. Device icons	19
FIGURE 12. Link illustration.....	20
FIGURE 13. Node Summary table.....	21
FIGURE 14. Link connection summary.....	21
FIGURE 15. IntelliView tools.....	22
FIGURE 16. Device tools	22
FIGURE 17. Personal user tools.....	23
FIGURE 18. User Profile screen.....	23
FIGURE 19. IntelliView table design	24
FIGURE 20. Filter icon	25
FIGURE 21. Paging controls.....	25
FIGURE 22. Column sorting	26
FIGURE 23. Sessions screen	28
FIGURE 24. LDAP configuration screen.....	29
FIGURE 25. Default Security groups	30
FIGURE 26. Initial Security Groups screen.....	32
FIGURE 27. Create Security Group screen	33
FIGURE 28. Security Group created confirmation.....	34
FIGURE 29. Updated list of security groups	34
FIGURE 30. Modify Security Group screen	35
FIGURE 31. Modify Security Group configuration	35
FIGURE 32. Object Deleted message	36
FIGURE 33. Security Group error message	36
FIGURE 34. CSV Open dialog box	37
FIGURE 35. CSV report - Excel.....	37
FIGURE 36. IntelliView Users screen	39
FIGURE 37. Modify IntelliView User screen	39
FIGURE 38. Create IntelliView User screen	40
FIGURE 39. User creation error.....	41
FIGURE 40. User created confirmation	41
FIGURE 41. Updated list of users.....	42
FIGURE 42. Object deleted confirmation.....	42
FIGURE 43. Modify IntelliView User screen	43
FIGURE 44. IntelliView User update confirmation	43
FIGURE 45. Permission Sets screen.....	44
FIGURE 46. Create Permission Set screen.....	45
FIGURE 47. Permission Set created confirmation.....	45
FIGURE 48. Updated list of permission sets.....	46

FIGURE 49. Modify Permission Set screen	47
FIGURE 50. Modify permission set confirmation	47
FIGURE 51. Object deleted confirmation.....	48
FIGURE 52. Device Sets screen.....	48
FIGURE 53. Create Device Set screen.....	49
FIGURE 54. Create Device Set screen (filled).....	50
FIGURE 55. Device created confirmation.....	50
FIGURE 56. Device Sets screen.....	51
FIGURE 57. Modify Device Set screen.....	51
FIGURE 58. Device set modified confirmation.....	52
FIGURE 59. Device set deletion confirmed	52
FIGURE 60. Updated list of device sets.....	53
FIGURE 61. System backup toolbar	55
FIGURE 62. System Backup screen.....	55
FIGURE 63. Backup Status times	56
FIGURE 64. Backup Status Complete	56
FIGURE 65. Restore from Backup screen	57
FIGURE 66. System information dialog	57
FIGURE 67. System Backup Config screen	58
FIGURE 68. Operation Scheduler screen.....	59
FIGURE 69. Scheduled Operations screen	59
FIGURE 70. Scheduled Operation screen	60
FIGURE 71. Operation Runs screen.....	61
FIGURE 72. Add Device dialog.....	65
FIGURE 73. Add Unmanaged dialog	66
FIGURE 74. Add Submap dialog	66
FIGURE 75. Add Link dialog	67
FIGURE 76. Move Device dialog	68
FIGURE 77. Submap Properties dialog	68
FIGURE 78. Unmanaged Properties dialog	69
FIGURE 79. Link Path Details table	70
FIGURE 80. Automatic Link Details screen	70
FIGURE 81. Modify Link Data screen	71
FIGURE 82. Transaction Load Balance and or Fail over example diagram	72
FIGURE 83. Ports configuration screen (Ethernet).....	73
FIGURE 84. Node 0210 Ethernet Port 1 Configuration screen.....	74
FIGURE 85. Node 0210 Ethernet Port 2 Configuration screen.....	75
FIGURE 86. Node 0210 Ethernet Port 3 Configuration screen.....	76
FIGURE 87. Node 0210 Ethernet Port 4 Configuration screen.....	77
FIGURE 88. Node 0208 Ethernet Port 1 Configuration screen.....	78
FIGURE 89. Node 0208 Ethernet Port 2 Configuration screen.....	79
FIGURE 90. Node 0208 Ethernet Port 3 Configuration screen.....	80
FIGURE 91. Node 0208 Ethernet Port 4 Configuration screen.....	81
FIGURE 92. Node 0209 Ethernet Port 1 Configuration screen.....	82
FIGURE 93. Node 0209 Ethernet Port 2 Configuration screen.....	83
FIGURE 94. Node 0209 Ethernet Port 3 Configuration screen.....	84
FIGURE 95. Node 0207 Ethernet Port 1 Configuration screen.....	85
FIGURE 96. Node 0207 Ethernet Port 2 Configuration screen.....	86

FIGURE 97. Node 0207 Ethernet Port 3 Configuration screen.....	87
FIGURE 98. NAC links screen	88
FIGURE 99. NAC links Configuration screen.....	88
FIGURE 100. Node 0210 NAC links Configuration screens	89
FIGURE 101. Node 0208 NAC links Configuration screens	90
FIGURE 102. Node 0209 NAC links Configuration screens	91
FIGURE 103. Node 0207 NAC links Configuration screens	92
FIGURE 104. Node Configuration (Uplinks)	93
FIGURE 105. Node 0210 Host1 TCP/IP Uplink Primary Configuration screens.....	94
FIGURE 106. Node Configuration (Uplinks)	95
FIGURE 107. Node 0210 Host 1 TCP/IP Uplink Fail over Configuration screens	96
FIGURE 108. Node Configuration (Uplinks)	97
FIGURE 109. Node 0208 Host2 TCP/IP Uplink Primary Configuration screens.....	98
FIGURE 110. Node Configuration (Uplinks).....	99
FIGURE 111. Node 0208 Host2 TCP/IP Uplink Fail over Configuration screens.....	100
FIGURE 112. Node Configuration (Uplinks).....	101
FIGURE 113. Node 0209 Host1 TCP/IP Uplink Primary Configuration screens	102
FIGURE 114. Node Configuration (Uplinks).....	103
FIGURE 115. Node 0209 Host2 TCP/IP Uplink Fail over Configuration screens	104
FIGURE 116. Node Configuration (Uplinks).....	105
FIGURE 117. Node 0207 Host2 TCP/IP Uplink Primary Configuration screens	106
FIGURE 118. Node Configuration (Uplinks).....	107
FIGURE 119. Node 0207 Host1 TCP/IP Uplink Fail over Configuration screens	108
FIGURE 120. Node Configuration (Uplinks)	110
FIGURE 121. Node 0210 Host1 TCP/IP Uplink load Balance for node 0209	111
FIGURE 122. Node Configuration (Uplinks)	112
FIGURE 123. Node 0210 Host1 TCP/IP Uplink load Balance for node 0207	113
FIGURE 124. Node Configuration (Uplinks)	114
FIGURE 125. Node 0208 Host2 TCP/IP Uplink load Balance for node 0207	115
FIGURE 126. Node Configuration (Uplinks)	116
FIGURE 127. Node 0208 Host2 TCP/IP Uplink load Balance for node 0209	117
FIGURE 128. Node Configuration (Uplinks)	118
FIGURE 129. Node 0209 Host1 TCP/IP Uplink load Balance for node 0209	119
FIGURE 130. Node Configuration (Uplinks)	120
FIGURE 131. Node 0209 Host2 TCP/IP Uplink load Balance for node 0209	121
FIGURE 132. Node Configuration (Uplinks)	122
FIGURE 133. Node 0207 Host2 TCP/IP Uplink load Balance for node 0207	123
FIGURE 134. Node Configuration (Uplinks)	124
FIGURE 135. Node 0207 Host1 TCP/IP Uplink load Balance for node 0207	125
FIGURE 136. NAC to NAC link with in band management configuration	126
FIGURE 137. Device Manage screen.....	128
FIGURE 138. Device Configuration screen	129
FIGURE 139. Device unplaced side bar	131
FIGURE 140. Device System Configuration screen	132
FIGURE 141. Port Configuration screen	133
FIGURE 142. Ethernet Port 1 Configuration screen - node 0210	134
FIGURE 143. Ethernet Port 2 Configuration screen - node 0210	135
FIGURE 144. Ethernet Port 3 Configuration screen - node 0210	137

FIGURE 145. Ethernet Port 4 Configuration screen - node 0210	138
FIGURE 146. Ethernet Port 4 Static Route Configuration - node 0210	139
FIGURE 147. Ethernet Port 1 Configuration screen - node 0208	140
FIGURE 148. Ethernet Port 2 Configuration screen - node 0208	141
FIGURE 149. Ethernet Port 3 Configuration screen - node 0208	142
FIGURE 150. Ethernet Port 4 Configuration screen - node 0208	143
FIGURE 151. Ethernet Port 4 Static Route Configuration - node 0208	144
FIGURE 152. Ethernet Port 2 Configuration screen - node 0209	145
FIGURE 153. Ethernet Port 3 Configuration screen - node 0209	146
FIGURE 154. Ethernet Port 3 Static Route Configuration - node 0209	147
FIGURE 155. Ethernet Port 4 Configuration screen - node 0209	148
FIGURE 156. Ethernet Port 2 Configuration screen - node 0207	149
FIGURE 157. Ethernet Port 3 Configuration screen - node 0207	150
FIGURE 158. Ethernet Port 3 Static Route Configuration - node 0207	151
FIGURE 159. Ethernet Port 4 Configuration screen - node 0207	152
FIGURE 160. NAC Links Configuration screen	153
FIGURE 161. NAC Links status screen	153
FIGURE 162. NAC to NAC links configuration screens - node 0210	154
FIGURE 163. NAC to NAC links configuration screens - node 0208	155
FIGURE 164. NAC to NAC links configuration screens - node 0209	156
FIGURE 165. NAC to NAC links configuration screens - node 0207	157
FIGURE 166. Uplinks configuration screens.....	158
FIGURE 167. Host1 TCP/IP Uplink load Balance node 0210 for node 0209.....	159
FIGURE 168. Uplinks configuration screens.....	160
FIGURE 169. Host1 TCP/IP Uplink load Balance node 0210 for node 0207.....	161
FIGURE 170. Uplinks configuration screens.....	162
FIGURE 171. Host2 TCP/IP Uplink load Balance node 0208 for node 0209.....	163
FIGURE 172. Uplinks configuration screens.....	164
FIGURE 173. Host2 TCP/IP Uplink load Balance node 0208 for node 0207.....	165
FIGURE 174. Uplinks configuration screens.....	166
FIGURE 175. Host1 TCP/IP Uplink load Balance on node 0209 for node 0209.....	167
FIGURE 176. Uplinks configuration screens.....	168
FIGURE 177. Host2 TCP/IP Uplink load Balance on node 0209 for node 0209.....	169
FIGURE 178. Uplinks configuration screens.....	170
FIGURE 179. Host2 TCP/IP Uplink load Balance on node 0207 for node 0207.....	171
FIGURE 180. Uplinks configuration screens.....	172
FIGURE 181. Host1 TCP/IP Uplink load Balance on node 0207 for node 0207.....	173
FIGURE 182. Alarm System screen	174
FIGURE 183. Alarm Override screen.....	175
FIGURE 184. Alarm Override screen.....	176
FIGURE 185. Alarm System screen	178
FIGURE 186. Alarm Rule screen	179
FIGURE 187. Alarm Rule screen	179
FIGURE 188. Alarm System screen	181
FIGURE 189. Alarm Notification screen.....	182
FIGURE 190. Alarm Notification Properties screen - Level 1 tab	182
FIGURE 191. Alarm Notification Properties screen - Level 2 tab	183
FIGURE 192. Alarm Notification Properties screen - Alarm Clear tab	184

List of Figures

FIGURE 193. Alarm Notification Properties screen - Alarm Ack tab.....	185
FIGURE 194. Alarm Notification Properties screen - Audibles tab	186
FIGURE 195. Email Configuration screen	187
FIGURE 196. Email configuration confirmation	188
FIGURE 197. Device File Manager.....	189
FIGURE 198. Upload Files tab page.....	190
FIGURE 199. File Upload screen.....	191
FIGURE 200. Updated list of uploaded files	191
FIGURE 201. Downloaded Files tab page	192
FIGURE 202. Configuration tab page	193
FIGURE 203. Files on Device screen	194
FIGURE 204. Staging area screen.....	194
FIGURE 205. Updated Device File Listing	195
FIGURE 206. Selecting the desired file	195
FIGURE 207. Download confirmation	196
FIGURE 208. IntelliView Properties screen	197
FIGURE 209. Statistic Schedule screen	198
FIGURE 210. Navigational pane.....	200
FIGURE 211. Online Device Configuration	201
FIGURE 212. IO Modules screen	202
FIGURE 213. Add I/O Module.....	202
FIGURE 214. IO Module screen	203
FIGURE 215. Ethernet Ports screen.....	203
FIGURE 216. ISDN PSTN Port screen	204
FIGURE 217. Ethernet Ports screen.....	205
FIGURE 218. Ethernet Ports Configuration screen	206
FIGURE 219. Ethernet Port Static Route configuration screen.....	207
FIGURE 220. ISDN PSTN Ports screen	208
FIGURE 221. ISDN PSTN Port configuration screen	209
FIGURE 222. Switch types supported	210
FIGURE 223. MFR2 PSTN Ports screen	211
FIGURE 224. MFR2 PSTN Port configuration screen	212
FIGURE 225. Switch types supported	213
FIGURE 226. RBS PSTN Ports screen	214
FIGURE 227. RBS PSTN Port configuration screen.....	214
FIGURE 228. Analog PSTN Port Screen.....	216
FIGURE 229. Analog PSTN Port configuration screen.....	217
FIGURE 230. SNA Uplink Ports screen	219
FIGURE 231. SNA Uplink Port configuration screen	220
FIGURE 232. SNA Protocol configuration Tab.....	221
FIGURE 233. SNA Serial configuration Tab.....	223
FIGURE 234. SNA SDLC configuration Tab	224
FIGURE 235. X.25 Uplink Ports screen	225
FIGURE 236. X.25 Uplink Port configuration screen	226
FIGURE 237. X.25 Protocol configuration Tab.....	227
FIGURE 238. X.25 Serial configuration Tab.....	228
FIGURE 239. X.25 LAPB configuration Tab.....	228
FIGURE 240. X.25 Down link Ports screen	230

FIGURE 241. X.25 Down Link Port configuration screen	231
FIGURE 242. X.25 Protocol configuration Tab.....	232
FIGURE 243. X.25 Serial configuration Tab.....	233
FIGURE 244. X.25 LAPB configuration Tab.....	234
FIGURE 245. Downlinks Configuration screen.....	235
FIGURE 246. TCP/IP Downlink screen.....	236
FIGURE 247. Downlinks Configuration screen.....	238
FIGURE 248. PSTN Downlink screen.....	238
FIGURE 249. PSTN Downlink configuration screen	239
FIGURE 250. Downlinks Configuration screen	240
FIGURE 251. X.25 Downlink screen.....	240
FIGURE 252. X.25 Downlink configuration screen	241
FIGURE 253. TCP/IP NII screen.....	242
FIGURE 254. TCP/IP NII Configuration screen	243
FIGURE 255. TCP/IP NII Lookup Table screen	243
FIGURE 256. Upper part of TCP/IP NII Lookup Table screen	244
FIGURE 257. Protocol Options of TCP/IP NII Lookup Table screen.....	245
FIGURE 258. TCP/IP NII Visa protocol tab.....	247
FIGURE 259. TCP/IP DNIS Alarm tab	248
FIGURE 260. TermMaster tab.....	249
FIGURE 261. DNIS NII screen.....	250
FIGURE 262. DNIS NII Configuration screen	251
FIGURE 263. Upper part of DNIS Lookup Table screen.....	252
FIGURE 264. Protocol Options of DNIS Lookup Table screen	254
FIGURE 265. DNIS Visa protocol tab	256
FIGURE 266. TCP/IP DNIS Alarm tab	257
FIGURE 267. TermMaster tab.....	258
FIGURE 268. X.25 NII screen.....	259
FIGURE 269. X.25 NII Configuration screen	260
FIGURE 270. Upper part of X.25 Lookup Table screen	261
FIGURE 271. Protocol Options of X.25 Lookup Table screen	262
FIGURE 272. X.25 Visa protocol tab	264
FIGURE 273. X.25 DNIS Alarm tab	265
FIGURE 274. TermMaster tab.....	266
FIGURE 275. CRI NII screen.....	267
FIGURE 276. CRI NII Configuration screen.....	267
FIGURE 277. CRI NII screen.....	269
FIGURE 278. CRI NII Configuration screen.....	269
FIGURE 279. TCP/IP Uplinks screen	271
FIGURE 280. TCP/IP Uplink screen	272
FIGURE 281. X.25 Uplinks screen.....	274
FIGURE 282. X25 Uplink screen	275
FIGURE 283. SNA Uplinks screen.....	276
FIGURE 284. SNA Uplink screen	276
FIGURE 285. Offline Config Stores screen.....	278
FIGURE 286. Offline Config Store screen.....	278
FIGURE 287. Offline Config Store creation confirmation	279
FIGURE 288. Copy Config Store screen.....	279

List of Figures

FIGURE 289. Config App screen	280
FIGURE 290. Download Config screen	281
FIGURE 291. Upload Config screen	282
FIGURE 292. Alarm table	286
FIGURE 293. Alarms details screen	289
FIGURE 294. Info tab page	291
FIGURE 295. Notes tab page	292
FIGURE 296. Details tab page	293
FIGURE 297. Events tab page	293
FIGURE 298. Events table	295
FIGURE 299. Event Details screen	295
FIGURE 300. Statistics Selection screen	299
FIGURE 301. Statistics Display example screen	299
FIGURE 302. Statistics directory screen	300
FIGURE 303. Statistics Selection screen	302
FIGURE 304. Statistics record example screen	303
FIGURE 305. Statistics CSV example screen	303
FIGURE 306. EFTSec Message Format	304
FIGURE 307. Trace Toggle Confirmation	308
FIGURE 308. Trace Disable	309
FIGURE 309. Trace Disable Confirmation	309
FIGURE 310. Trace Activity Status	311
FIGURE 311. Downloaded Trace file from IntelliNAC	314
FIGURE 312. Managed Element screen - trace collection settings	316
FIGURE 313. Trace Log Viewer	317
FIGURE 314. Log Application Configuration screen	319
FIGURE 315. DS0 Status Display	321

List of Figures

CHAPTER 1

Introduction

Overview

The IntelliView® User Guide details the features and functions of the IntelliView application and its interaction with the IntelliNAC® device.

Document Structure

The guide is divided into several key sections:

- Installation - describes how to install IntelliView
- Getting Started - describes how to get the system up and running
- Administration - describes basic administrative tasks
- Configuration - describes how to configure your network
- Operations - describes key IntelliView operations
- Troubleshooting - describes how to correct common issues.

Audience

This guide is designed for the end-user as well as the trained service technician.

Related Reading

Refer to the following documents for additional information:

- IntelliNAC/IntelliView Release Notes
- IntelliNAC Planning Guide (#940642-003)
- IntelliNAC Hardware and Troubleshooting Guide (#940642-002)
- IntelliNAC Installation Guide (#940642-001)

CHAPTER 2

Product Overview

IntelliView

IntelliView is build on a multi-tiered management system framework using a multi-threaded Java server, a web client is used for the front end, and a database for backups.

The system supports multiple clients and multiple devices.

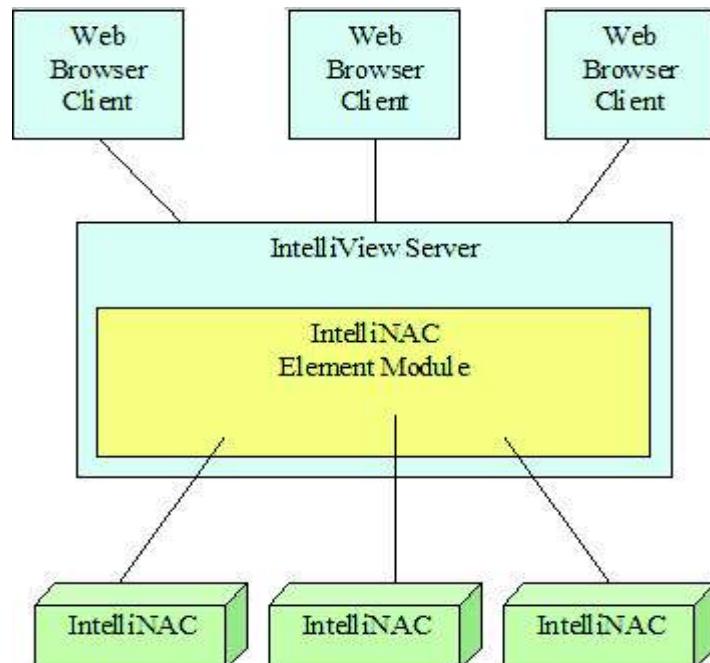


FIGURE 1. IntelliView Architecture

The IntelliView framework provides a model/generation framework. Data objects (such as configuration objects, status objects, operation commands) and interfaces are modeled in files. A code generator is currently used to create Java based on the data. Components generated include GUI screens, data, database files, local interfaces, database layer, and model to be used at runtime.

Supported Servers

IntelliView is a Java-based system that installs and runs on Intel 64-bit servers running Redhat Enterprise Linux 5.x and up or CentOS 5.x and up Linux.

The IntelliView server must be a dedicated server with the below minimum requirements. If placed in a virtual environment, the same requirements are applied.

- CPU: Dual Core 2GHz, Hyper Threaded
- Memory: 4GB RAM
- 1 Gb wired Ethernet port
- Disk: 250GB (to store statistics, alarms and Logs)

Supported Clients

As IntelliView is web-based, it requires no installation on a client. It runs in a variety of browsers:

- Microsoft Internet Explorer 9+
- Mozilla FireFox
- Google Chrome

Note: As a component of Windows XP Internet Explorer 8 is no longer support by Microsoft (4/14/2009). IntelliView can be run on IE8 but VeriFone will not support any issues identified on IE8.

Additionally: GWT(Google Web Toolkit) stopped supporting Internet Explorer 8 on Nov. 25 2012.

We recommend running Chrome or Firefox on Windows XP.

Licensing IntelliView

There are two versions of IntelliView available: Basic and Standard. Each version has its own separate feature set.

A 60-day evaluation license is for the Basic version. This can be permanently upgraded at any time during and or after the evaluation period to any other version.

Standard and Enterprise versions are not available for evaluations.

The version features are:

Feature	Basic	Standard	Enterprise
Configuration for number of devices (nodes)	3	100 ¹	Unlimited ^{1,3}
Events Management	Yes	Yes	Yes

Feature	Basic	Standard	Enterprise
Alarms Management	Yes	Yes	Yes
Statistics Management	Yes	Yes	Yes
Concurrent Client Connections	Limited	Unlimited ¹	Unlimited ¹
Number of user accounts	Limited to four	Unlimited ¹	Unlimited ¹
User Authentication	Local (IntelliView)	Local and LDAP	Local and LDAP
Reports Customization Advanced Reports	No	No	Yes ³
Failover/Failback Capability	No	No	Yes ³
Load Balancing	No	No	Yes ³
Statistics Thresholds	No	No	Yes ³
IntelliView Platform Reports	No	No	Yes ³

1 - Constrained only by server capability (CPUs, system memory, etc.)

2 - IntelliNACs are not discovered by IntelliView, instead devices are added explicitly.

3 - Scheduled for release 2.0

Only Basic and Standard versions will be available for Release 1. The Enterprise version feature set will be released in Release 2.

A license renewal does not impact the system's operation. Even a license level change within IntelliView will cause the feature set to change on the fly without the need to restart IntelliVIEW.

License Properties

The following properties are necessary to define the IntelliView license generation and usage:

- Only VeriFone generates IntelliView licenses. They will be generated at VeriFone's facility under secure conditions.
- Each license must be digitally signed to ensure that the license actually came from VeriFone.
- Each license is encrypted to ensure that external agencies are unable to view the license contents.
- Each license is tied to a specific system (i.e., a specific instance of IntelliView). Thus, copying a license file and installing it on another system will result in the feature not being enabled on the other system (the license is not transferable).
- The license contains the following information:
 - The licensing authority (VeriFone).
 - The entity to whom the license has been issued (customer).
 - The license expiration date.
 - The feature set included in the license.

License Dependencies

The following dependencies apply to IntelliView licenses:

- A specific permission for license administration is added to the permission/security subsystem.

- The code for all subsystems with licensable features is verified before execution.
- Whenever a license changes (a new one is installed or the monitoring code determines that the license has expired), a message is sent to the system message bus. Interested subsystems (those that cache license information) subscribe to this notification to invalidate their caches and reload new license information.

Installing a New License

Note: The license file will only install successfully on the system identified with its unique ID.

To install a new license:

1. Order a specific license from VeriFone. You will need to provide the System Id (generated during the installation) for which the license is being requested. The System ID can be displayed via the IntelliView user interface.
2. With the License Generation utility, VeriFone will take the following inputs and generate a license file that contains the appropriate licensed features:
 - System ID
 - Feature Set
 - Expiration Date
 - Issuing Authority (VeriFone)
 - Issuing To (Customer)
3. The license file will be digitally signed using VeriFone private key. This allows IntelliView to verify that the file came from VeriFone. This verification is done using VeriFone public key, which was shipped with IntelliView. For additional security, this key was encrypted using a unique password so that only the IntelliView software can read its contents.
4. The generated license file is then sent to the customer.
5. Once received, the customer can install the new license using the IntelliView user interface.

Upgrading a License

To upgrade a system license:

1. The customer orders a specific license from VeriFone (Basic, Standard, or Enterprise). The customer needs to provide the System ID (generated during the installation) for which the license is being requested. The System ID can be displayed via the IntelliView user interface.
2. With a License Generation utility, VeriFone will take the following inputs and generate a license file that contains the appropriate licensed features:
 - System ID
 - Feature set
 - Expiration date
 - Issuing authority (VeriFone)
 - Issued to (customer)
3. The license file will be digitally signed using VeriFone's private key. This will allow IntelliView to verify that the file came from VeriFone. This verification is done using VeriFone's public key,

which was shipped with IntelliView. For additional security, this key was encrypted using a unique password so that only the IntelliView software can read its contents.

4. The generated license file is then sent to the customer.
5. Once received, the customer can install the new license using the IntelliView user interface. This installation will override the current license. The system will take on all the features enumerated by the new license.

Note: The license file will only install successfully on the system identified with its unique ID.

Installation and Initial Setup

IntelliView is supplied as a zip file. The zip file is in this form:

IntelliView-{majorReleaseNumber}_{minorReleaseNumber}_{buildNumber}.zip

For example, for release 1.0, build 1, the file will be named **IntelliView_linux_1_0_1.zip**.

The zip file will contain the following files:

- IntelliView-{majorReleaseNumber}-{minorReleaseNumber}-Build{buildNumber}.tar.gz
For example, for release 1.0 build 1, it will be named: IntelliView-1-0-Build1.tar.gz.
- install.sh (IntelliView install script)
- uninstall.sh (IntelliView uninstall script)
- upgrade.sh (IntelliView upgrade script)
- restore.sh (IntelliView restore script)
- HYC-SW_Lic.txt (Software end user license agreement)
- HycKeyStore (Keystore file)

Note: Before installing IntelliView, there are a few assumptions and/or points to remember:

- The scripts on the CD (have an extension of .sh) are executed from the Linux command line.
- Only root can execute the scripts provided in the install CD. If a non-user tries to run any of the above scripts, execution of the script will be aborted.
- Please make sure that in **/etc/login.defs**, the following option is set to yes:
USERGROUPS_ENAB.
- IntelliView is installed using default Apache Tomcat's ports: **8080** for HTTP, **8443** for HTTPS.
Please make sure these ports are accessible for users that will be using IntelliView.
- IntelliView is using a keystore with a default certificate. As a result, a store file is created with a key pair for HTTPS connections. Also, the keystore and certificate passwords have to be the same (Tomcat's limitation), so as part of the installation, the user will be asked to enter a password that will be used for both. The client has the option of having their own trusted certificate by creating a new keystore file with a key pair and values, creating a CSR, sending it to an external CA, importing the root certificates and signed certificates, and storing it in the keystore file. More details of the process are available in the "Create HycKeyStore Certificate Procedure for IntelliView" section.
- IntelliView will be installed in **/opt**. Please make sure that there is enough disk space for the installation.

Install on Linux

To install IntelliView on Linux:

1. Log in as root to the Linux host.
2. Create a folder where the IntelliView zip file will be copied to.

In the root directory (/root), create the install folder by typing the following at the xterm command prompt: **mkdir IntelliView**.

So, for release 1.0 build 0, the command will be **mkdir IntelliView_1_0_1_install**.

3. Copy the IntelliView zip file from the CD to the newly created folder using this command:

cp {cdrom folder}/{filename} /root/ {install folder}/

where **{filename}** is IntelliView-{majorReleaseNumber}_{minorReleaseNumber}_{buildNumber}.zip

{install folder} is IntelliView_{releaseMajorNumber}_{releaseMinorNumber}_{buildNumber}_install

{cdrom folder} is the mounted folder of the CD drive, usually /media/cdrom or /dev/cdrom

For release 1.0 build 1 and the CD folder /dev/cdrom, the command will be:

cp /dev/cdrom/IntelliView_1_0_1.zip /root/IntelliView_1_0_1_install/

4. Unzip the zip file by executing the following from the command prompt:

/usr/bin/unzip IntelliView-{majorReleaseNumber}_{minorReleaseNumber}_{buildNumber}.zip

For release 1.0 build 1, the command will be: **/usr/bin/unzip IntelliView_linux_1_0_1.zip**.

After executing this command, you should see the file list described above in your local folder.

5. Go to the install directory by executing the following command:

cd {install folder}

where **{install folder}** is IntelliView_{releaseMajorNumber}_{releaseMinorNumber}_{buildNumber}_install

For release 1.0 build 1, the command will be: **cd /root/IntelliView_1_0_1_install**.

6. Execute the IntelliView script:

./install.sh {IntelliView install file}

where **{IntelliView install file}** is IntelliView-{releaseMajorNumber}.{releaseMinorNumber}-{buildNumber}.tar.gz

For release 1.0 build 1, the command will be: **./install.sh IntelliView-1.0-Build1.tar.gz**

Note: When running the installation script, there are two times when a user response is needed:

- Before installation can take place, the user has to accept the IntelliView Software End User License Agreement. Immediately after executing the command in step 6 above, the first page of the license agreement will be displayed. Read the page and when done, press the spacebar to display the next page. At the end of the license agreement, the following question will be displayed:

DO YOU ACCEPT THE SOFTWARE LICENSE AGREEMENT [y/n]?

Pressing **y** will install IntelliView, pressing **n** will abort the installation.

- The user will be asked to choose a keystore password. Enter it twice for verification.

From this point, installation will continue and, at the end, the following message will be displayed:

Install completed successfully

Uninstall IntelliView

To uninstall IntelliView, run the uninstall script from the command line:

cd {install folder}

where {install folder} is IntelliView_{releaseMajorNumber}_{releaseMinorNumber}_{buildNumber}_install

For example, release 1.0 build 1, the command will be: cd /root/IntelliView_1_0_1_install
./uninstall.sh

Upgrade IntelliView

To upgrade IntelliView, run the upgrade script by executing the following from the command line:

cd {install folder}

where {install folder} is IntelliView_{releaseMajorNumber}_{releaseMinorNumber}_{buildNumber}_install

For example, for release 1.0 build 1, the command will be: cd /root/IntelliView_1_0_1_install
./upgrade.sh {IntelliViewInstallFilename}

where {IntelliViewInstallFilename} is IntelliView_{releaseMajorNumber}_{releaseMinorNumber}_{buildNumber}.tar.gz

For example, for release 1.0 build 1, the command will be: ./upgrade.sh IntelliView_1_0_1.tar.gz.

Restore IntelliView

To restore IntelliView, run the restore script from the command line:

cd {install folder}

where {install folder} is IntelliView_{releaseMajorNumber}_{releaseMinorNumber}_{buildNumber}_install

For example, for release 1.0 build 1, the command will be: cd /root/IntelliView_1_0_1_install
./restore.sh {IntelliViewBackupFilename}

where {IntelliViewBackupFilename} is
IntelliView_{releaseMajorNumber}_{releaseMinorNumber}_{buildNumber}.tar.gz

For example, for release 1.0 build 1, the command will be: ./restore.sh IntelliView_1_0_1.tar.gz

Stop IntelliView

To stop the IntelliView service, execute the command:

service IntelliView stop

Change Admin User Settings

To change the Admin user's settings:

1. Enter the URL: where \${servername} is the DNS name or IP address of the machine on which IntelliView has been installed.
2. Log into the default user account (admin/lview&Lv&2012).
3. If initial login follow immediate steps below, else step 9
4. IntelliView will prompt for a new Administration password
5. Enter new password if the following requirements:

 Password length must be 8 characters minimum

 Must contain a minimum of one each of the following:

 Upper case

 Lower case

 Numeric

 Special character not in first character location

 Also can not be any of the previous 4 passwords

6. In the "Security App" allows the ability to change the administrator login password.
7. Create any other users needed.

Basic Operations

The basic operations for all users, including the Administrator, include:

- Logging on
- Logging off
- Exiting IntelliView

Logging On after Initial install:

1. Open a compatible Web browser.
2. Enter system initial user name and password. admin lview&Lv&2012

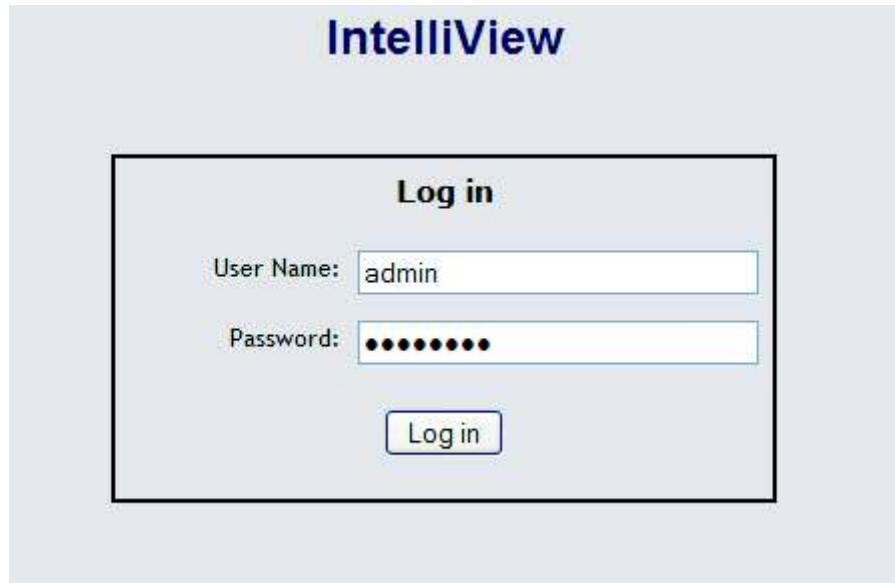


FIGURE 2. IntelliView Login screen

3. Click **Log in**. After authentication, IntelliView requires the changing of the administrator password on initial logon.



FIGURE 3. Initial IntelliView Login screen

This will complete the initial installation of IntelliView

Logging On after Initial Logon

To log onto IntelliView:

1. Open a compatible Web browser.
2. Enter your user name and password.

If you do not have an active login, the login dialog box appears first:

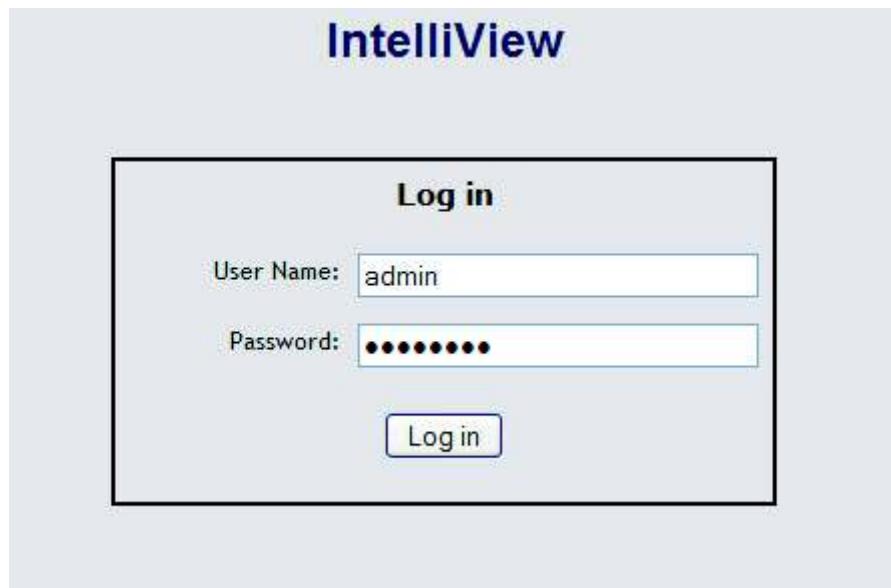


FIGURE 4. IntelliView Login screen

3. Click **Log in**. After authentication, the main screen appears.

Logging Off

There are two options for logging IntelliView:

- **Close** - This action closes the browser window, but leaves the current session and application active
- **Exit** - This action closes the browser window, but leaves the current session and application active

Exiting IntelliView

From the Personnel User toolbar, select “**Log Out**”. You are logged off and your changes are not saved.

Navigation

There are several tools available to aid you in navigation within IntelliView:

- Toolbars
- Tables
- Icons
- Personal User Tools
- My Profile
- Buttons

Main Screen

The IntelliView main screen appears when you successfully log in. The default system view is displayed in the middle part of the screen under the toolbar and above the Alarms and Events region.

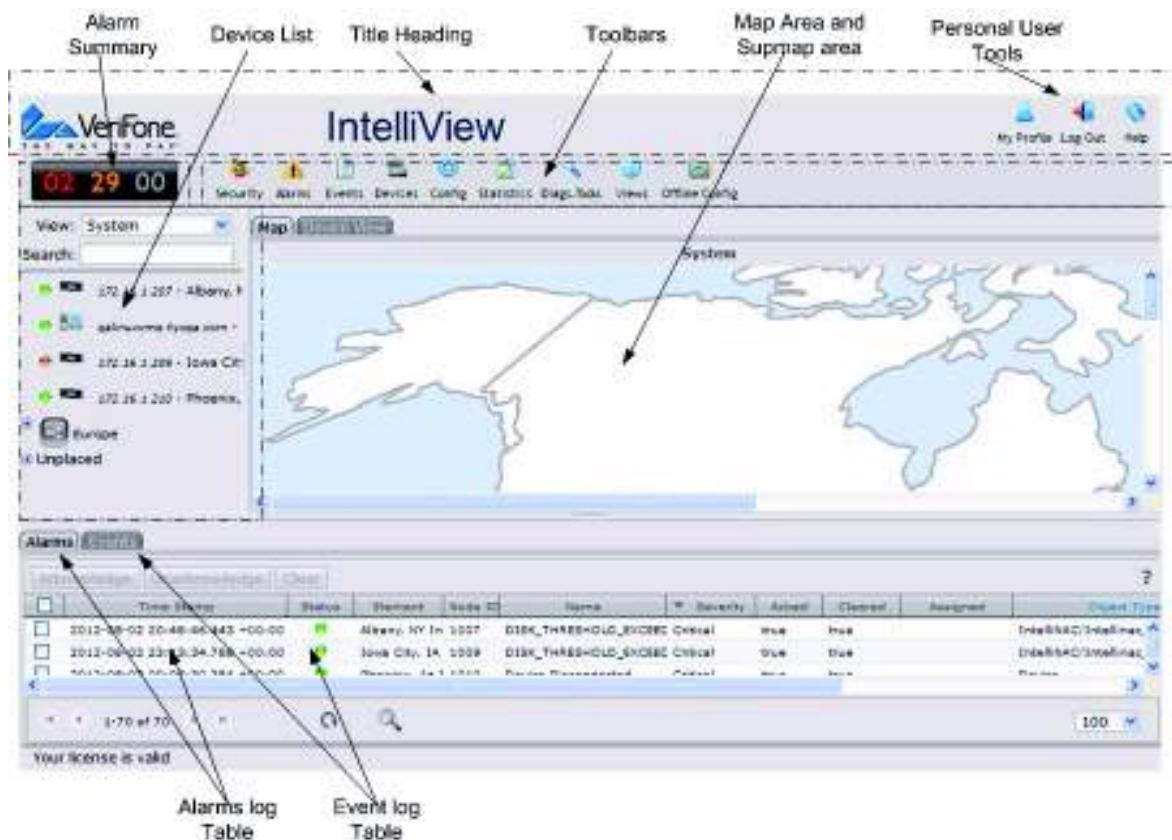


FIGURE 5. Main screen

It is comprised of the following components:

- **Title Heading** - The top section of the main screen
- **Alarm Summary** - The Alarm Summary displays the current number of unacknowledged alarms of each severity. The alarm table is accessible by clicking on a value to filter to the severity.
- **Toolbars** - The toolbars display the core system or select device tools. The tools appear conditionally according to the user's permissions.
- **Device List** - The Device List is a hierarchical tree of devices and domains with colored icons. The hierarchical tree contains the device list. The list of devices matches those found in the map/submap hierarchy. Devices managed to the system, but not yet placed in any domain in the view are placed in a special tree node called "Unplaced Devices".

You can select a device, search for a device by name/address. The device's icon reflects the alarm status for the device.

- **Map** - The tabbed section presents either the network or device map.
- **Events Log Table** - The Events Log Table displays a running log of events entering the system.
- **Alarms Log Table** - The Alarms Log Table displays a running log of alarms entering the system.

Map Views

Multiple views can be defined within IntelliView to accommodate multiple perspectives of the management domain. Changing the arrangement of items in one view does not affect the other views. A view can be locked from being edited to prevent inadvertent modifications.

System View

The system initially starts in a default state where a single view has been created and is named System. The device system, if the user has permission to see it, is initially present in the Unplaced List as a device.

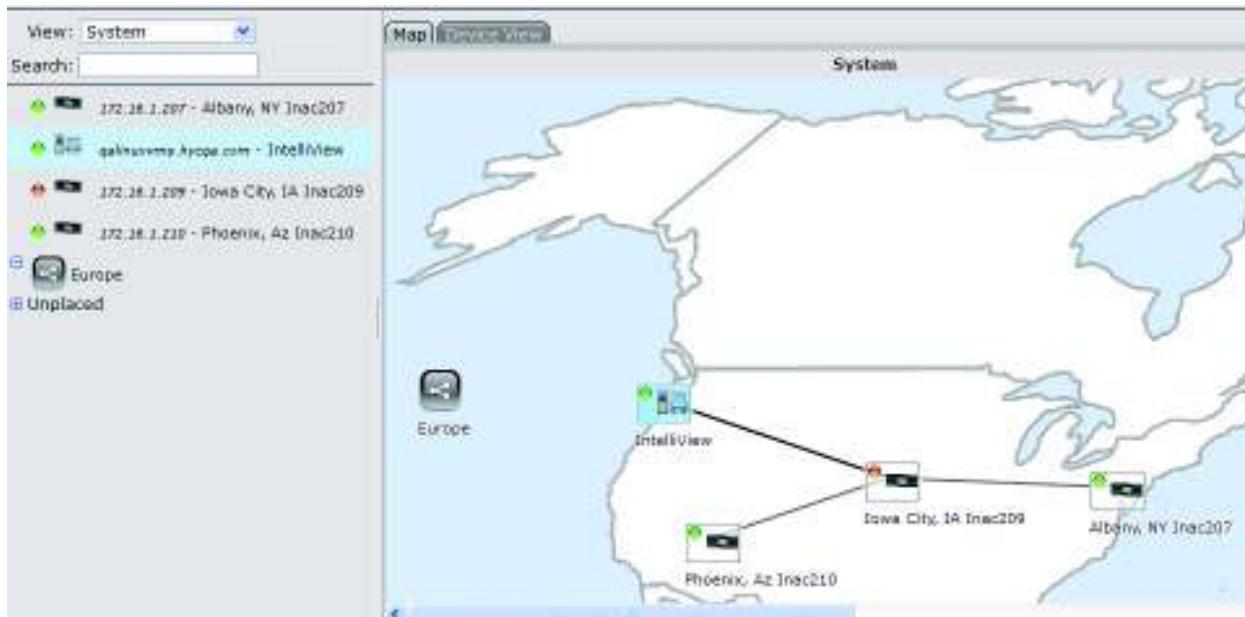


FIGURE 6. System view

The View table is used to create, update, and delete view definitions.

A view has a name, description, and the option to be locked. A locked view is not editable in the network view.

Network View

The network view is displayed in the middle part of the screen under the toolbar and above the alarms and events region. The network view provides four distinct regions:

- View Controls
- Device Tree
- Map
- Device View

View Controls

The View Controls region of the main screen provides the ability to choose which view is being displayed and offers a search of the currently selected view.



FIGURE 7. View Controls region

All of the existing views defined in IntelliView are listed. Choosing a view other than the current view switches the display to the new view.

The Search function operates against the view's organization. The function suggests possible completions as you type in the beginning characters of a name. The suggested devices are those that have been placed on the map in the Unplaced List. The Search function also suggests submaps and unmanaged icons that belong to the view.

If the suggestion is chosen, the icon of the choice in both the Device Tree and the map are selected in the view. The Search entry box then clears for the next search.

Device Tree

The Device Tree is located directly below the View Controls region.

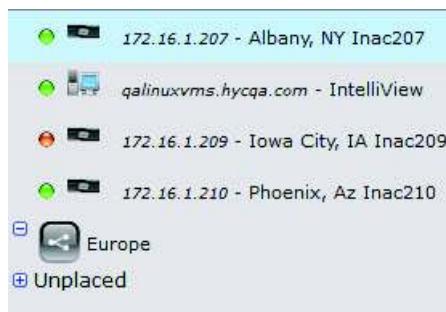


FIGURE 8. Device Tree

The Device Tree is a list of a view's submaps and devices grouped by submap and follow the same groups in the map.

The list of devices and submaps are ordered alphabetically by name. The devices are grouped together and listed first, followed by the submaps. The tree icons expand and collapse the immediate children of a submap. Initially, the tree shows only the devices and submaps that belong to the "root" of the view only.

Each submap and device is represented by a row in the list that tracks status and provides identification with an icon and descriptive label. Right-click menus are available on devices in the tree. The menus' content vary based on the device and the user's privileges.

The initial display of the device tree shows the devices and submaps that belong to the root of the view only. The tree allows the user to navigate through the view's map structure by showing the devices and submaps which belong to various submaps.

Submaps within the list may hide or show the submaps and devices that belong to them. The tree control icons expand (+) and collapse (-) the immediate children of a submap.

Selecting a device node in the tree will display the submap to which the device belongs and select the device's icon in the Map tab. Selecting a submap displays the submap in the Map tab.

Right-click menus are available on device in the tree. The menu will be selected that is within the context of the device and user's privileges for the device and IntelliView.

Map

The Map system provides the graphical display of the View organization and tools for editing the View organization. Interaction with the map system is through the Map tab located right of the Device Tree and View Control regions.



FIGURE 9. Map tab

The Map tab shares the same area on the main screen as the Device view. You can switch between the two views by clicking on the appropriate tab, Map or Device View. When a view is first shown or reloaded, the top-most set of devices and submaps are displayed in the map.

Device View

The Device View contents are based on the selected device. Typical content could be a summary of the device and a realistic depiction of the device. It is also used to create a detailed description of the node and view the installed software version. This can be done for the IntelliView version as well as the IntelliNAC software version.

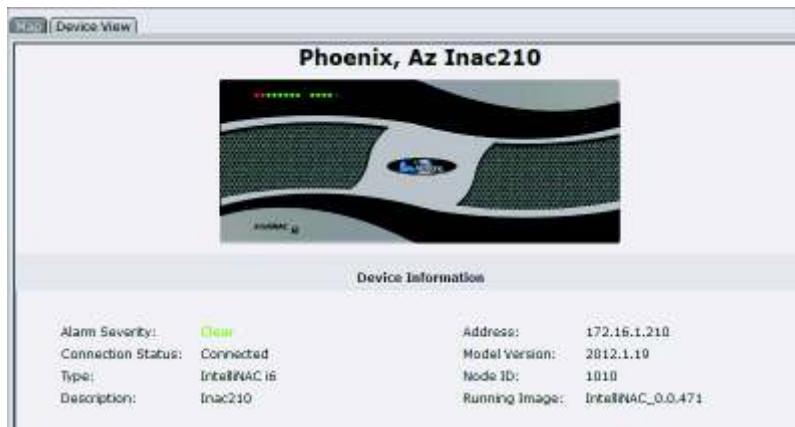


FIGURE 10. Device view for IntelliNAC

Icons

Icons depict the devices and submaps of the system with unique imagery and a color indicator of the status of the device or the highest severity of the devices and submaps belonging to a submap.

Upload icons to make them available for use with Unmanaged devices and submaps. The icon image must be 24 pixels x 24 pixels.

When an icon is selected, the toolbar of the Main screen is in the context of the selection. Icons can also be dragged and dropped in order to move them around on a submap background. When moved, the new location is persisted on the server.

Deleting an icon that is in use causes a “broken” icon in the icons for the Unmanaged devices or submaps.

Device Icons

The status color indicator of the icon provides single-click access to an Alarms table for the particular device. The name of the device is displayed at the bottom of the icon.



FIGURE 11. Device icons

Rolling over the color status indicator indicates that clicking on the color status indicator opens an Alarm table for the device.

Submap Icons

Submap icons indicate the highest severity status of the submaps and devices belonging to it by the color of the whole icon. An image, selectable for each individual submap, is centered over the status color indicator. The name of the submap is displayed at the bottom of the icon.

When single-clicking on a submap, the select of the submap has a special behavior. The map changes to graphically display the contents of the submap.

Within each submap, an icon is automatically placed in the upper left corner of the map to represent the “parent” or submap to which this submap belongs. If the submap is at the top-most level of the view organization, the “parent” appears as a submap icon with the name of the view.

The upper-left “parent” icon is unique in that it cannot be moved and links are drawn to it when a connection to a device within the submap is to a device outside of the devices belonging to a submap or one of its submaps.

Links

Links represent network connections between devices. They are graphically depicted as lines drawn between devices and submaps.

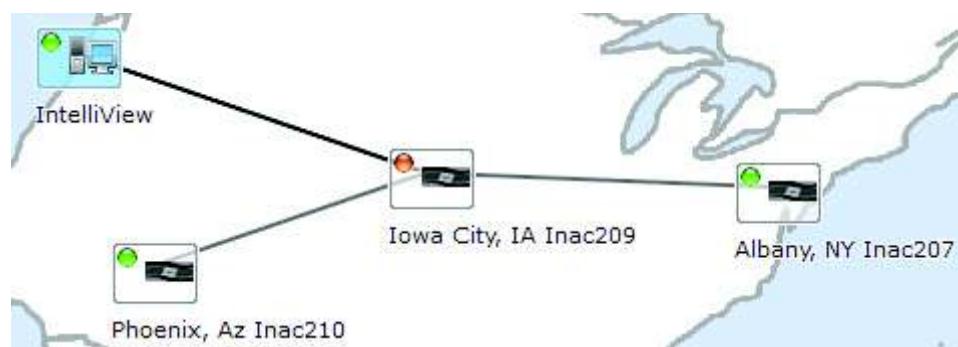


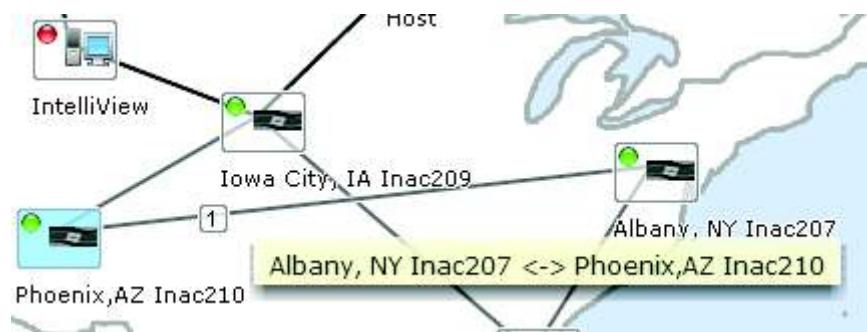
FIGURE 12. Link illustration

When the mouse moves over a link, a badge icon is displayed that indicates the number of actual device connections comprising the link. Hovering over a badge icon displays a listing of the connections. Single-clicking on the badge icon opens up the Link Path Details table.

**FIGURE 13.** Node Summary table

The status color indicator of a link is the color of the link line. The link line, like a submap, reflects the highest severity link status of all the links of the link line.

There are two types of links, automatic and synthetic. Both types appear similarly in the map, but differ in both their details and what controls the user has over the link.

**FIGURE 14.** Link connection summary

Automatic Links

Automatic links are created automatically by the system through management of devices. When the device is contacted, connectivity information is retrieved and used to generate links between managed devices. These links only appear in the map as links when both devices that make up the endpoints of the link are added to the view.

Synthetic Links

Synthetic links are manually created. They are unique to the view to which it is added and representative of connections that are not automatically derived from the managed devices.

Toolbars

The IntelliView main screen contains two core and device-specific toolbars:

- IntelliView tools
- IntelliNAC tools

IntelliView Tools

The IntelliView Tools are part of the main toolbar when an IntelliView component is selected.



FIGURE 15. IntelliView tools

The following menus are included:

- **Security** - displays the Security menu
- **Devices** - displays the devices menu
- **Offline Config** - displays the Configure Objects screen
- **Statistics** - displays the Statistics screen
- **Alarms** - displays the Alarm Table screen
- **Events** - displays the Events Table screen
- **Diag Tools** - displays the Diag Tools screen
- **Views** - displays the View table with a listing of IntelliView views.

Device Tools

The Device tools are part of the expanded main toolbar. The tools are displayed when IntelliView connects to an IntelliNAC device. Only shown if device selected.

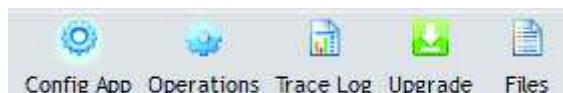


FIGURE 16. Device tools

The tools include: Note same as right clicking on the Node/Device

- Config Apps - Takes you to node/device configuration
- Operations - Pulls down a menu for system operations
- Trace Log - Takes you to Trace window

Navigation

- Upgrade - Pulls down a menu for upgrade functions
- Files

These tools are device specific.

Personal User Tools

The Personal User tools are not part of the main toolbar, but they are found on the main screen. Located in the upper right corner, the three tools provide personal interaction.



FIGURE 17. Personal user tools

The tools include:

- My Profile
- Log Out
- Help

My Profile

Clicking the **My Profile** button in the Personal User Tools displays the User Profile screen.

A screenshot of a Windows-style dialog box titled "User Profile". The dialog contains the following fields:

- User Name: admin
- Password: (redacted)
- Verify Password: (redacted)
- Email Address: x@y.com
- Security Groups:
 - Email Enabled
 - Table Audibles EnabledAdmins
- User Origin: Internal data store

At the bottom are "Cancel" and "OK" buttons.

FIGURE 18. User Profile screen

Product Overview

From this screen, you change your password, email address, map, and other personal settings.

Log Out

Clicking the **Log Out** button allows you to terminate this session and close the system.

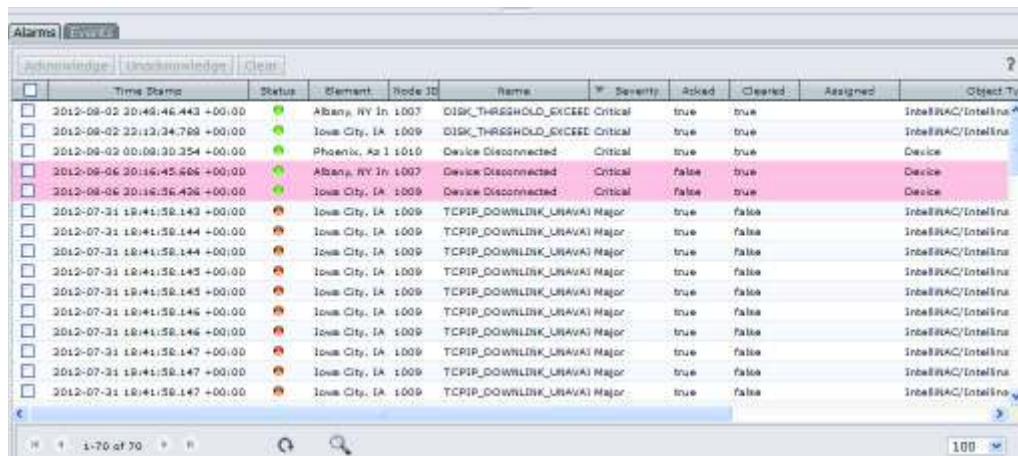
Help

Clicking the **Help** button connects you to the IntelliView online help system. The first page is automatically displayed. Currently under construction!!!

Tables

Tables within IntelliView can be embedded into other screens or occupy the entire window. The tables have three main components:

- Header
- Data
- Footer



The screenshot shows a table interface with the following columns: Time Stamp, Status, Element, Node ID, Name, Severity, Asked, Cleared, Assigned, and Object Type. The data rows include various alarms and device status entries from different locations like Albany, NY and Iowa City, IA, with severity levels ranging from Critical to Major. The table has a header row with icons for sorting and filtering, and a footer row with pagination controls.

	Time Stamp	Status	Element	Node ID	Name	Severity	Asked	Cleared	Assigned	Object Type
<input type="checkbox"/>	2012-08-02 20:46:46.443 +00:00	●	Albany, NY In	1:007	DISK_THRESHOLD_EXCEEDED	Critical	true	true		IntelliWAC/IntelliWa
<input type="checkbox"/>	2012-08-02 22:12:24.789 +00:00	●	Iowa City, IA	1:009	DISK_THRESHOLD_EXCEEDED	Critical	true	true		IntelliWAC/IntelliWa
<input type="checkbox"/>	2012-08-02 00:09:30.354 +00:00	●	Phoenix, Az 1	1:010	Device Disconnected	Critical	true	true		Device
<input type="checkbox"/>	2012-08-06 20:16:45.603 +00:00	●	Albany, NY In	1:007	Device Disconnected	Critical	false	true		Device
<input type="checkbox"/>	2012-08-06 20:16:46.426 +00:00	●	Iowa City, IA	1:009	Device Disconnected	Critical	false	true		Device
<input type="checkbox"/>	2012-07-31 19:41:58.143 +00:00	●	Iowa City, IA	1:009	TCPPIP_DOWNLINK_UNAVAI	Major	true	false		IntelliWAC/IntelliWa
<input type="checkbox"/>	2012-07-31 19:41:58.144 +00:00	●	Iowa City, IA	1:009	TCPPIP_DOWNLINK_UNAVAI	Major	true	false		IntelliWAC/IntelliWa
<input type="checkbox"/>	2012-07-31 19:41:58.144 +00:00	●	Iowa City, IA	1:009	TCPPIP_DOWNLINK_UNAVAI	Major	true	false		IntelliWAC/IntelliWa
<input type="checkbox"/>	2012-07-31 19:41:58.145 +00:00	●	Iowa City, IA	1:009	TCPPIP_DOWNLINK_UNAVAI	Major	true	false		IntelliWAC/IntelliWa
<input type="checkbox"/>	2012-07-31 19:41:58.145 +00:00	●	Iowa City, IA	1:009	TCPPIP_DOWNLINK_UNAVAI	Major	true	false		IntelliWAC/IntelliWa
<input type="checkbox"/>	2012-07-31 19:41:58.145 +00:00	●	Iowa City, IA	1:009	TCPPIP_DOWNLINK_UNAVAI	Major	true	false		IntelliWAC/IntelliWa
<input type="checkbox"/>	2012-07-31 19:41:58.146 +00:00	●	Iowa City, IA	1:009	TCPPIP_DOWNLINK_UNAVAI	Major	true	false		IntelliWAC/IntelliWa
<input type="checkbox"/>	2012-07-31 19:41:58.146 +00:00	●	Iowa City, IA	1:009	TCPPIP_DOWNLINK_UNAVAI	Major	true	false		IntelliWAC/IntelliWa
<input type="checkbox"/>	2012-07-31 19:41:58.147 +00:00	●	Iowa City, IA	1:009	TCPPIP_DOWNLINK_UNAVAI	Major	true	false		IntelliWAC/IntelliWa
<input type="checkbox"/>	2012-07-31 19:41:58.147 +00:00	●	Iowa City, IA	1:009	TCPPIP_DOWNLINK_UNAVAI	Major	true	false		IntelliWAC/IntelliWa
<input type="checkbox"/>	2012-07-31 19:41:58.147 +00:00	●	Iowa City, IA	1:009	TCPPIP_DOWNLINK_UNAVAI	Major	true	false		IntelliWAC/IntelliWa

FIGURE 19. IntelliView table design

Header

The Header component is located at the top of a table. It contains the title of the table, descriptive text describing the table, and a row of buttons providing additional functionality for the table residing in the component. The title, descriptive text, and buttons are all optional and may not be displayed in tables where they do not add value.

Data

Table data is located in the middle of the table. The columns are resizable. A row or column headers label each column. Clicking on the column header sorts the column contents. A small icon is located to the right of the column headers and expands the width of all of the columns to fill the window or screen. A checkbox in the first column of the header selects all rows displayed. Each row can be selected by selecting the checkbox located next to it or by choosing the row itself.

Some table cells have a single-click action associated to them by the table's definition. Some cells have tool tips over the cell which display when the cursor hovers over them. Double-clicking on a row usually launches a detail screen on the row item.

Footer

The Footer components is located at the bottom of the table. It contains paging controls, refresh and filtering options.

Filtering

Filtering allows the displayed results to be scoped to a particular set of values. Each table has a filter defined in a dialog box which appears when the Filter icon is selected in the table footer.



FIGURE 20. Filter icon

If there is no icon, then the table does not offer filtering.

Filter buttons include:

- **Clear** - clears all the filter values in the dialog box
- **Apply** - invokes the current filter values in the dialog box as a filter, and generates a result set
- **Close** - exits the dialog box. This button is not necessary if you click **Apply** since the dialog box closes automatically

Paging

Paging produces smaller pages of the dataset which is so large that looking at it in its entirety is not practical. The dataset can be filtered and sorted.

Paging controls on the left side of the table footer allow you to select an arbitrary page and the navigational icons go the first, previous, next, and last pages of the dataset.

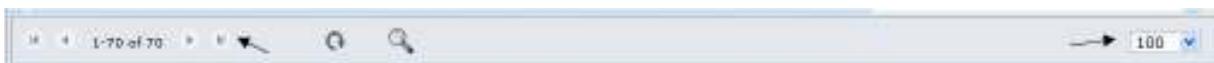


FIGURE 21. Paging controls

Paging controls on the right side of the footer allow you to select the size of each page as well as the displayed information about the rows and table row statistics, such as the total number of rows and the particular set of rows being displayed in relation to the total number of rows.

The **Refresh** button re-queries the server for the currently displayed table data.

Sorting

Sorting can be performed by simply clicking on a column header. The data is sorted in either an ascending or descending order.



	Severity	Acked
LD_EXCEED	Critical	true
LD_EXCEED	Critical	true
ected	Critical	true
ected	Critical	false
ected	Critical	false
NK_UNAVAI	Major	true
IAVAII	Major	true

FIGURE 22. Column sorting

An arrow icon displays the direction of the sort.

Each click on the header toggles the sort order between ascending and descending.

Note: Not every column may be sortable. Each table defines which columns are used for sorting.

Buttons

Buttons offer additional actions. Each table defines its own buttons, though many buttons offer CRUD-like services such as adding/deleting a row. Buttons may also launch external windows or perform other actions defined by the table definition.

CHAPTER 3

Getting Started

Introduction

This section details the steps needed to create and maintain IntelliView accounts and security settings.

Security

This section describes the IntelliView security system which allows the creation of users, permission groups, and device groups to manage access to the application.

System Accounts

An IntelliView administrator with the appropriate privileges can perform the following operations:

- View system information
- Install new license

A specific permission for license administration is part of the permissions/security subsystem. For more information on licensing, see the *Product Overview* section.

Viewing Session Information

To view Session information:

From the main toolbar, click **Security > Current Sessions**. The Sessions screen appears.



FIGURE 23. Sessions screen

If the system is in the evaluation period, the System ID and the details of the evaluation license (with canned data) displays.

If a valid license is installed, the following license information displays:

- ID - System ID
- Login - Who is logged in
- Host - From which host (IP address)
- Login Time - When did the login occur
- User Idle time - Time to last user action
- Application Idle Time - Application Idle time
- User Origin - User login location Remote or internal

Authentication

This is accomplished through:

- Authentication - a log in/out system that validates a user's password to gain access to the application.
- Authorization - a permission system that authorizes user requests. This system ensures that the user does not access parts of the application for which they have no permission.
- Audit - a mechanism that logs user activity.

There are two types of authentication available, password and LDAP.

Each user is configured with a password. Passwords can be configured to expire on a schedule, requiring the user to change their password at that time.

The user's password is saved in the database after encryption (MD5 hash). Upon login, the password is entered, hashed, and checked against the user's saved password hash.

When logging in, if a user is not found in the local store, and LDAP is enabled, then the system will try to authenticate the user via LDAP. If LDAP authentication success, LDAP will return a token. The token is then used to find a LDAP security profile to use to determine the user's permissions.

Enable LDAP

From the main toolbar, click **Security > LDAP**. The Sessions screen appears.

To enable LDAP authentication, select the enable LDAP authentication check box in the LDAP configuration dialog box.

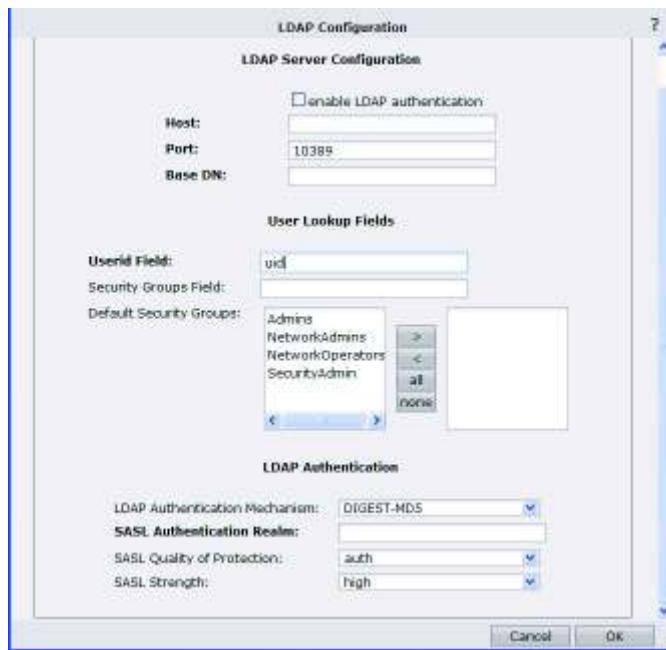


FIGURE 24. LDAP configuration screen

To disable a configured LDAP server, clear the checkbox. The server settings will be saved. To re-enable the server, select the checkbox.

Set up the LDAP Server

To set up the LDAP server, in the LDAP Configuration dialog box, enter values for the following fields:

- **Host** - The hostname of the LDAP server
- **Port** - The port the LDAP server is listening to
- **Base DN** - The distinguished name of the object in the directory tree that will contain the users for authentication.

Set up Security Policy Strategy

To set up the Security Policy Strategy, enter values in the following fields in the User Lookup Fields area on the LDAP Configuration dialog box:

- **Userid** - The name of the attribute containing the userid for looking up an LDAP user's security policy. The default value is uid.
- **Security Groups Field** - The name of the LDAP field containing the comma-separated list of IntelliView security groups to which the user belongs.

- **Default Security Groups** - A comma-separated list of Security Group names to apply to all LDAP-authenticated users who do not have individual security policies configured.

NetworkAdmins
NetworkOperators
SecurityAdmin
Admins

FIGURE 25. Default Security groups

Set up LDAP Authentication

To set up LDAP authentication on the LDAP Configuration dialog box, enter the following:

- **LDAP Authentication Mechanism** - Select either DIGEST_MD5 SASL authentication or Simple authentication
- **SASL Authentication Realm** - If DIGEST_MD5 was selected above, supply the name of the realm in which to authenticate users
- **SASL Quality of Protection** - If DIGEST_MD5 was selected above, select the Quality of Protection level
- **SASL Strength** - If DIGEST_MD5 was selected above, select the strength of protection.

Authorization

User requests are authorized against their assigned permissions. Permissions are assigned to users via permission groups, which cluster permissions, devices, and device groups. A permission consists of a permission name and a level. The permission types are defined by the core system and the device module.

Permission	Type	Level	Description
Configuration	Core	Read, Write	
Map	IntelliView	View, Modify, Manage	Manage to create new View, delete Views
Devices	IntelliView	View, Manage	Add/remove devices from system, edit device details
IntelliView Users	IntelliView	View, Manage	Manage to add/remove/edit users
IntelliView Admin	IntelliView	View, Manage	View to see sessions and audit log. Edit to interact with sessions (log off user, terminate session)
IntelliView License	IntelliView	View, Manage	Manage to install new license
Stats	Core	Report, Configure	Configure to change statistics collection settings
Alarms	IntelliView, IntelliNAC	View, Note, ACK	View allows the user to view alarms. Note allows the user to add notes. ACK allows the user to acknowledge an alarm.

Security

Permission	Type	Level	Description
ACK Alarm	IntelliView	Use	Allows the user to acknowledge alarms
Diags	Core	Use	Use diagnostic utilities on a device
Events	IntelliView	View	
Images	Core	Manage, Download, Upload	Download allows the user to copy images from the device. Upload allows the user to copy images to the device.

Permissions

The Security Configuration pages allow you to specify the permissions that are granted to a user through Device File Management. There are five settings or levels. Granting a higher level setting automatically grants permissions for operations corresponding to a lower level setting.

- **None** - No File Management permissions are available to the user. The menu option used to launch file management operations is not visible, the user is unable to do anything.
- **View** - The user can view files that are staged on IntelliView.
- **Manage** - The user may upload new files to IntelliView, these files will be stored in the staging area.
- **Download** - The user can download files from the device onto the staging area on IntelliView, and further download them onto their desktop.
- **Upload** - The user can upload files from the staging area on IntelliView to the device. Since uploading these files can affect device operation, this is the highest privilege level.

Roles

IntelliView's predefined roles specify set privileges and access rights:

Role	Permission	Level
IntelliView Administrator	Configuration	Write
	Devices	Manage
	License	Manage
	IntelliView Users	Manage
	Stats	Configure
	Alarms	View, Note, ACK
Network Administrator	Configuration	Write
	Stats	Configure
	Diag	Use
	Events	View, Note, ACK
	Alarms	View, Note, ACK
	Device Images	Upload
Network Operator	Stats	Configure
	Configuration	View
	Device Images	Upload

Role	Permission	Level
Security Administrator	IntelliView Users	Manage
	IntelliView Devices	Manage

Creating a Security Group

Security groups combine permissions and device specifications. The permission specifications are applied to the devices specified.

To create a security group:

1. From the toolbar, select **Security > Configuration**.
2. Click on the **Security Groups** tab. The Security Groups screen appears.

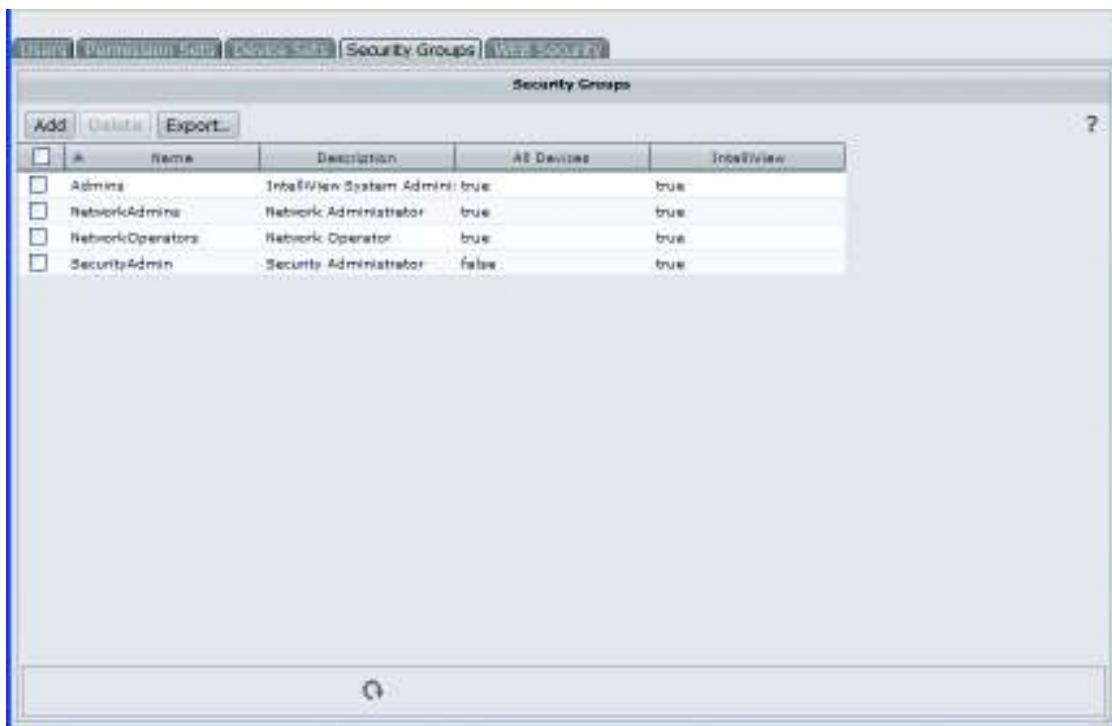


FIGURE 26. Initial Security Groups screen

3. Click **Add**. The **Create Security Group** screen opens.

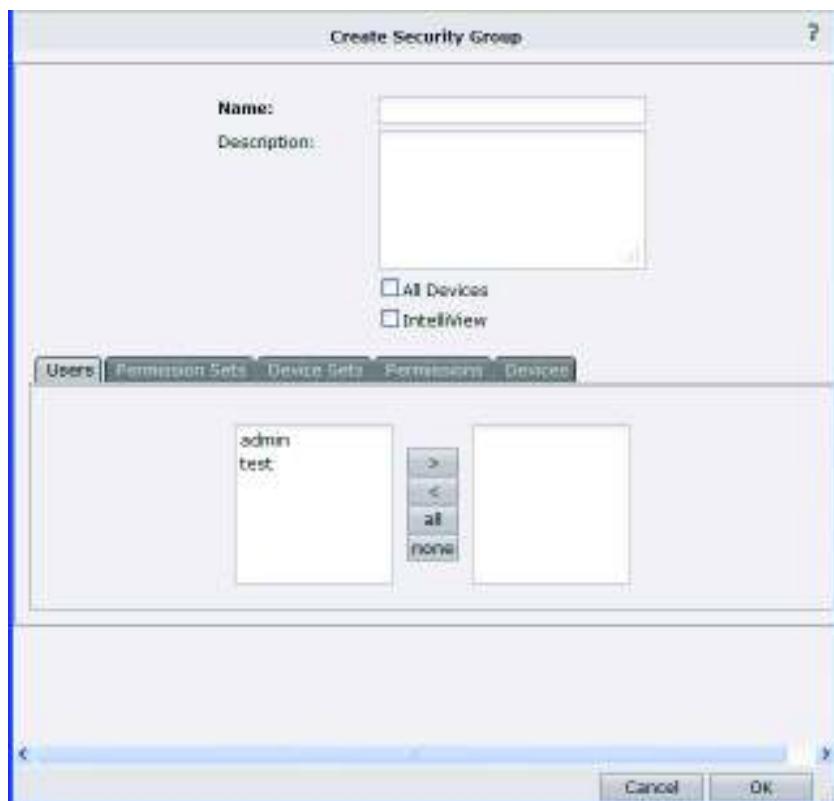


FIGURE 27. Create Security Group screen

- Name - Name of created security groups
 - Description - Unique description of the Security group
 - All Devices - If checked this security group is applied to all node/device managed by this instance of IntelliVIEW
 - IntelliVIEW - If Check this security group is applied to IntelliVIEW
 - Use the tabs to input the group information:
 - Users
 - Permission Sets
 - Device Sets
 - Permissions
 - Devices
4. Use the left and right arrows to select/deselect the displayed options.
 5. Click **OK** when done. A system message appears.



FIGURE 28. Security Group created confirmation

6. Click **OK**. A new security group appears in the list.

A screenshot of the IntelliView software interface showing the "Security Groups" tab. The window title is "Security Groups". Below the title, there are buttons for "Add", "Delete", and "Export...". The main area is a table with columns: Name, Description, All Devices, and IntelliView. There are five rows of data:

	Name	Description	All Devices	IntelliView
<input type="checkbox"/>	Admins	IntelliView System Admin	true	true
<input type="checkbox"/>	Monthly Test	Test of systems run monthly	false	false
<input type="checkbox"/>	NetworkAdmins	Network Administrator	true	true
<input type="checkbox"/>	NetworkOperators	Network Operator	true	true
<input type="checkbox"/>	SecurityAdmin	Security Administrator	false	true

FIGURE 29. Updated list of security groups

Modifying a Security Group

To modify an existing security group:

1. From the toolbar, select **Security > Configuration**.
2. Click on the **Security Groups** tab. The Security Groups screen opens.
3. Double-click on the desired security group from the listing. The Modify Security Group screen appears.

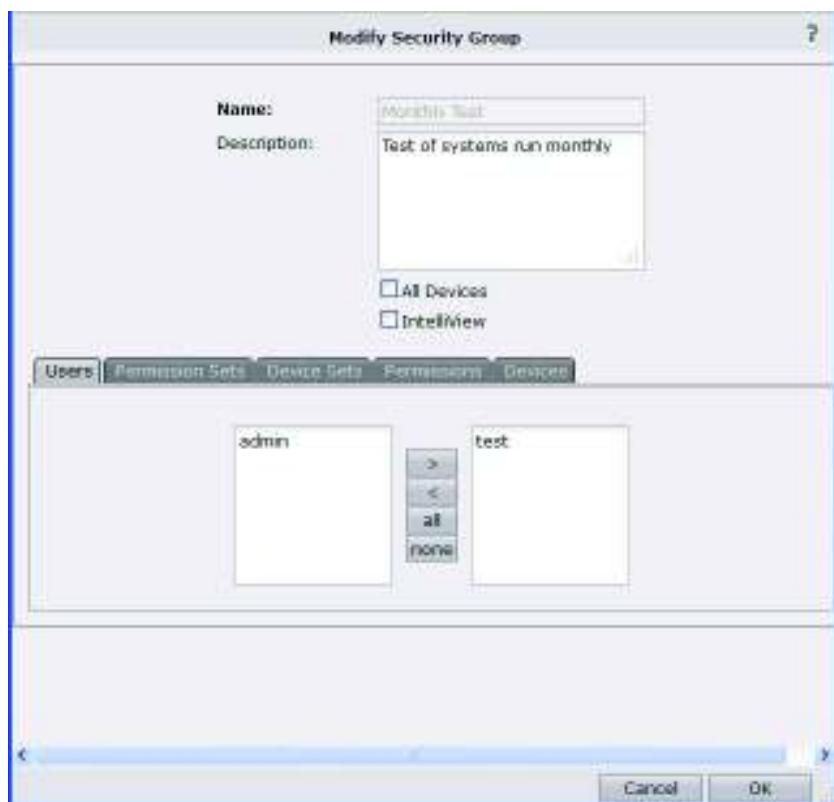


FIGURE 30. Modify Security Group screen

4. Use the right/left arrows to adjust the selected groups.
5. Click **OK** when done. The system message appears.



FIGURE 31. Modify Security Group configuration

6. Click **OK**.

Deleting a Security Group

To delete a security group:

1. From the toolbar, select **Security > Configuration**.
2. Click on the **Security Groups** tab. The Security Groups screen opens.
3. Select the desired security group from the listing.

4. Click **Delete** in the toolbar. The selected security group is removed from the listing and a system message appears.

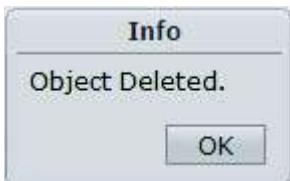


FIGURE 32. Object Deleted message

5. Click **OK**.

Note: Remove the devices attached to the selected security group first. If not, a system message appears.



FIGURE 33. Security Group error message

Exporting a Security Group

To export a security group's information:

1. From the toolbar, select **Security > Configuration**.
2. Click the **Security Groups** tab. The Security Groups screen opens.
3. Select the desired security group from the listing.
4. Click **Export** in the toolbar. The Open [filename] dialog box appears.



FIGURE 34. CSV Open dialog box

5. Select the file destination (open or save).
6. Click **OK**. The displayed csv file appears.

A screenshot of an Excel spreadsheet titled 'EMS_SecurityGroup.csv [Read-Only]'. The table has columns A, B, C, and D. Column A contains row numbers 1 through 22. Column B contains names: NetworkAdmins, NetworkOperators, SecurityAdmin, Admins, NetworkAdmins. Column C contains descriptions: IntelliView Administrator, Network Operator, Security Administrator, IntelliView Administrator, IntelliView Administrator. Column D contains 'All Devices': TRUE, FALSE, TRUE, TRUE, TRUE, FALSE, TRUE, FALSE, TRUE, FALSE, TRUE, TRUE, TRUE, FALSE, TRUE, TRUE, TRUE, FALSE, TRUE, TRUE, FALSE. Column E contains 'EMS': FALSE, TRUE, TRUE, TRUE, FALSE, TRUE, TRUE, FALSE, TRUE, TRUE, TRUE, TRUE, FALSE, TRUE, TRUE, TRUE, FALSE, TRUE, TRUE, TRUE, FALSE, TRUE, TRUE.

FIGURE 35. CSV report - Excel

User Accounts

User accounts are maintained by the Admin User. The Admin User creates/deletes user accounts, sets accounts privileges and system access.

To change the Admin user's settings:

1. Open a browser on a client machine.
2. Enter the URL: `http://${servername}`
where \${servername} is the DNS name or IP address of the machine on which IntelliView has been installed.
3. Log into the default user account: (admin/lview&Lv&2012).
4. Go to the security application and change the admin login password.

Configuration Data

The following data is configured through IntelliView Configuration screens. These value settings need to conform to associated standards recommended by PCI for secure operation where applicable. Please refer to the current PCI-DSS guidelines for implementation.

- System security configuration
- Idle user timeout (seconds)
- Maximum concurrent users
- Password expiration (days)
- LDAP
 - Enabled
 - LDAP server address
 - LDAP server port

Viewing User Accounts

To view all logged on users:

1. From the main toolbar, select **Security > Configuration**. The IntelliView Users screen appears.

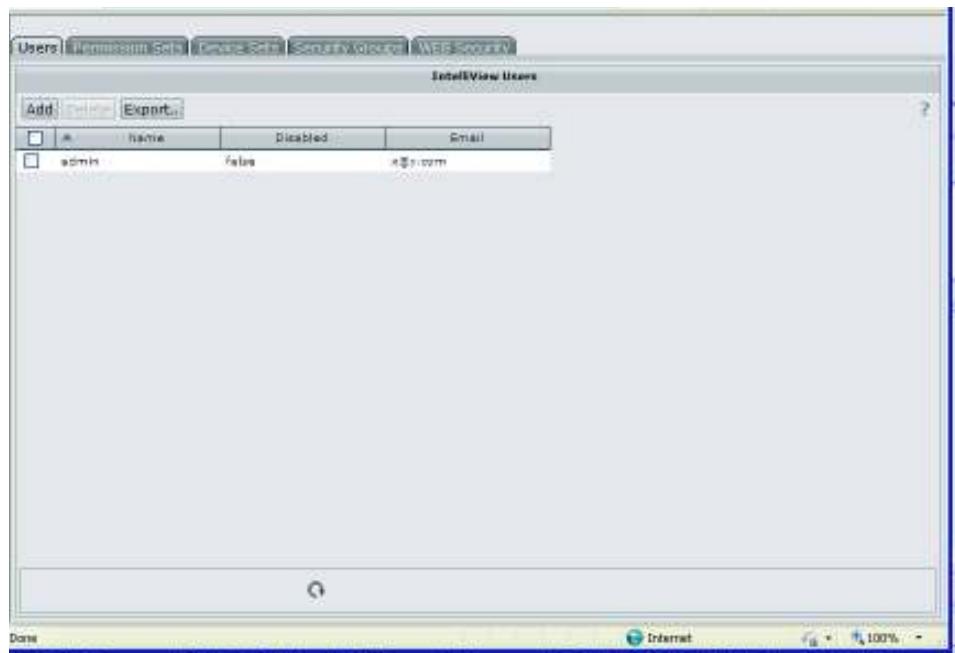


FIGURE 36. IntelliView Users screen

This screen contains a listing of all current IntelliView users.

2. Scroll up and down to locate a specific user.
3. Double-click on the desired user. The **Modify IntelliView User** screen appears with user details.

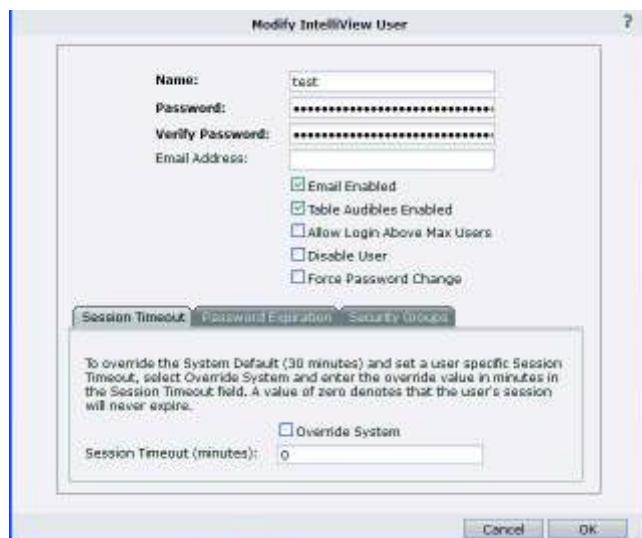


FIGURE 37. Modify IntelliView User screen

4. Click **Cancel** to close the screen without making changes.

Creating User Accounts

To create a new user account:

1. From the main screen toolbar, select **Security > Configuration**.
2. Click **Add**. The **Create IntelliView User** screen appears.

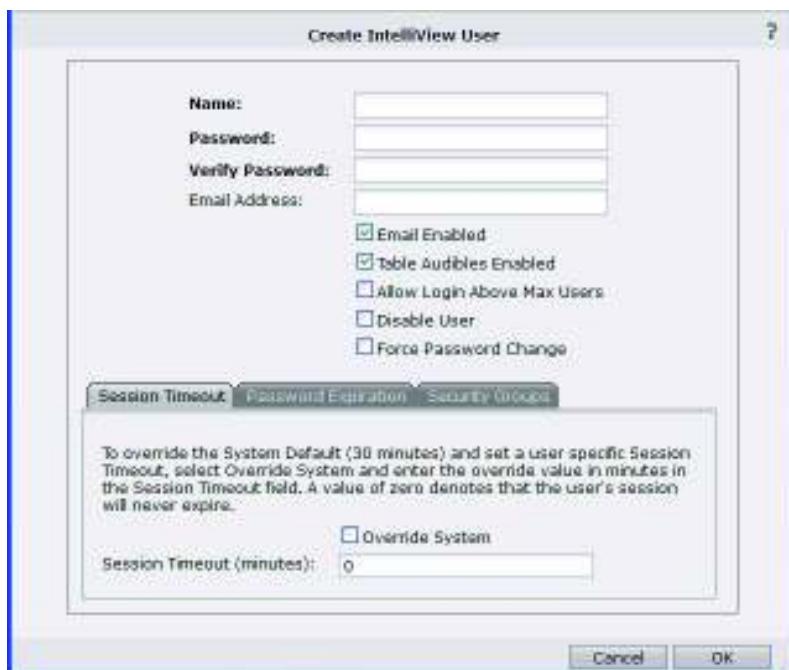


FIGURE 38. Create IntelliView User screen

- Name - Enter the user's name
- Password - Enter password for the USER account being created

Must contain a minimum of one each of the following:

Upper case
Lower case
Numeric
Special character not in first character location

- Verify Password - Re-Enter the password again to verify.
- Email Address - Enter the user's email address. This is optional and only necessary if the user will be receiving notifications.
- Select the user options, if applicable:
 - Email Enabled
 - Table Audibles Enabled - Allows the sounds to be played if a
 - Allow Login Above Max Users
 - Disable User
 - Force Password Change

Configuration Data

- Session Timeout - Session Timeout default is 30 minutes (This will override the System timeout)
 -
 - Password Expiration, and Security Groups information, if desired.
3. Click **OK** when done.
- If you make a mistake with the settings, an error message appears. Click **OK** and make the needed changes.

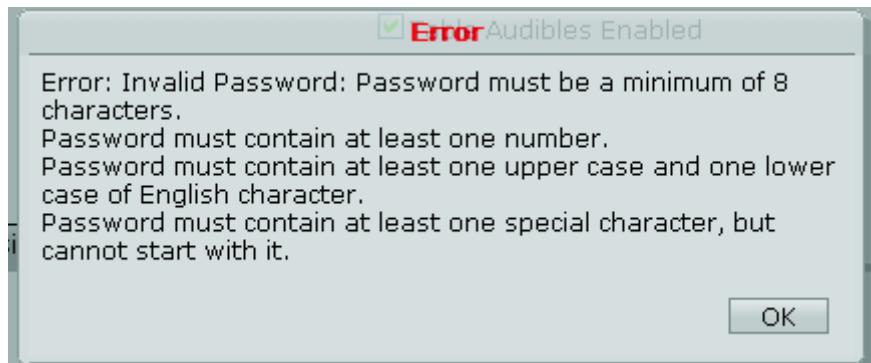


FIGURE 39. User creation error

When successful, a system message appears.



FIGURE 40. User created confirmation

4. Click **OK**. The new user name appears on the IntelliView Users screen.

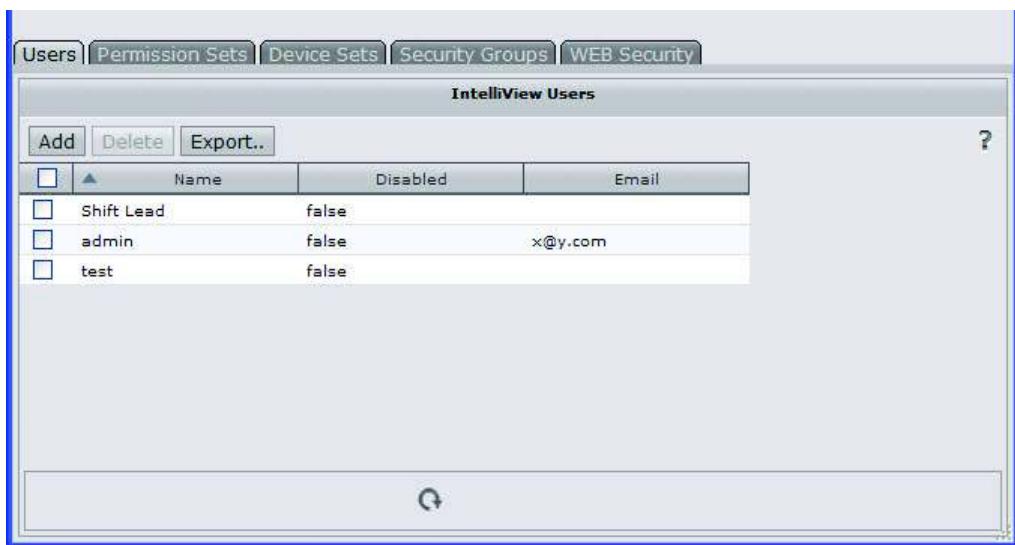


FIGURE 41. Updated list of users

Deleting a User Account

To delete a user account:

1. From the main screen toolbar, select **Security > Configuration**.
2. Highlight the desired user and click **Delete**. The selected user account is removed from the listing and a system message appears confirming the operation.



FIGURE 42. Object deleted confirmation

3. Click **OK**.

Editing User Accounts

To edit/modify a user account:

1. From the main screen toolbar, click **Security > Configuration**.
2. Double-click on the desired user account in the listing. The **Modify IntelliView User** screen appears.

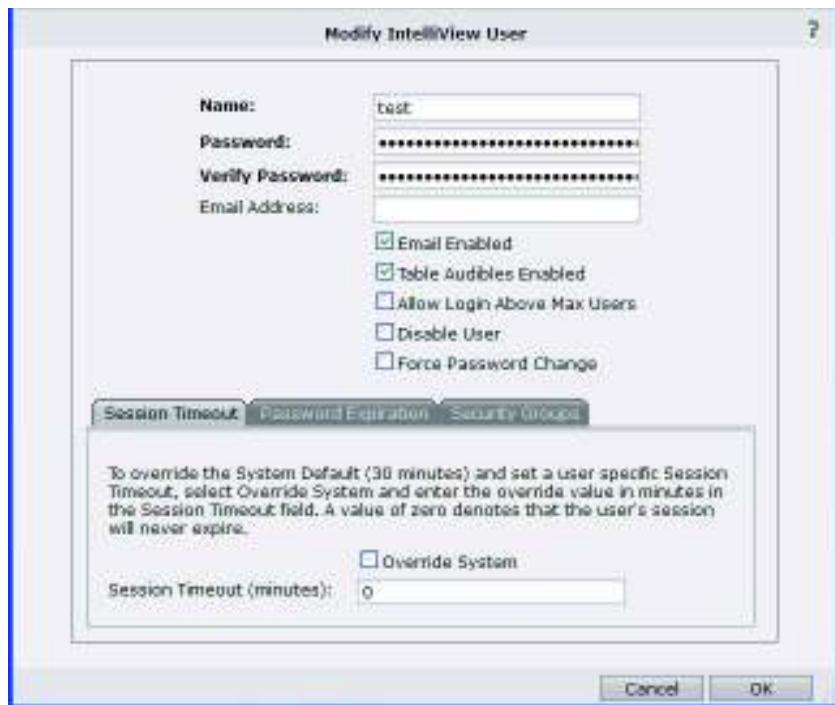


FIGURE 43. Modify IntelliView User screen

3. Make the change(s).
4. Click **OK**. A system message appears.



FIGURE 44. IntelliView User update confirmation

5. Click **OK**. The changes are saved.

Permission Sets

The administrator can create/modify/delete permission sets that can be applied across Security Groups. Changes to permissions have an immediate effect on users of the system.

Adding a Permission Set

A permission set affects all of the groups that use a specific role.

To add a permission set:

1. From the toolbar, click **Security > Configuration**.
2. Click the **Permission Sets** tab. A listing of permission sets appears.



FIGURE 45. Permission Sets screen

3. Click **Add**. The **Create Permission Set** screen opens.

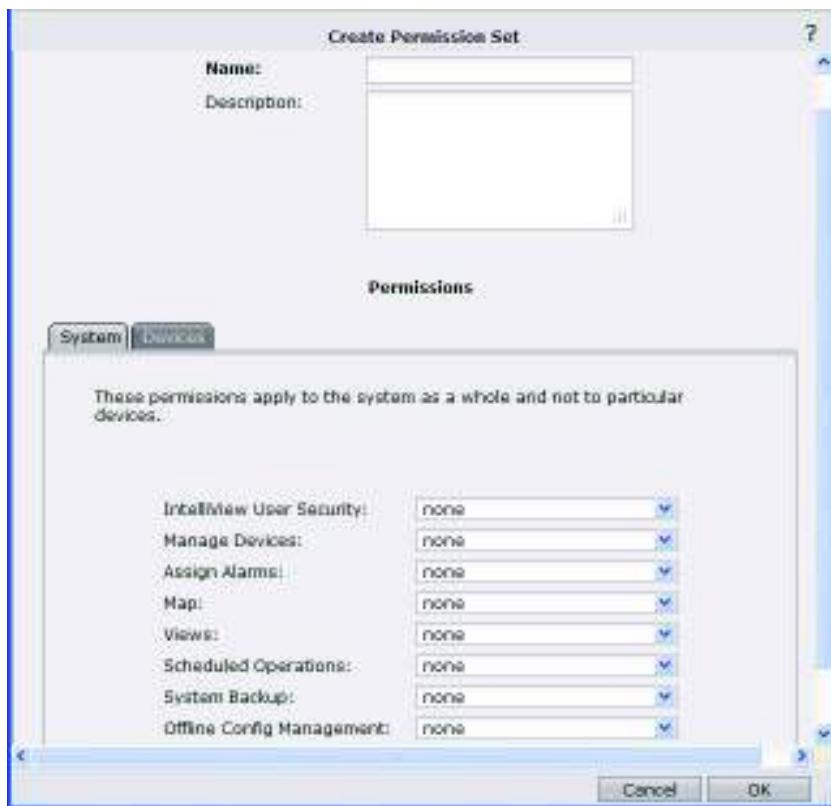


FIGURE 46. Create Permission Set screen

4. Enter the permission set information (name and description).
5. Define the appropriate settings using the related pull-down options.
6. Click **OK**. A system message appears confirming the operation.



FIGURE 47. Permission Set created confirmation

7. Click **OK**. The new permission set appears in the listing.

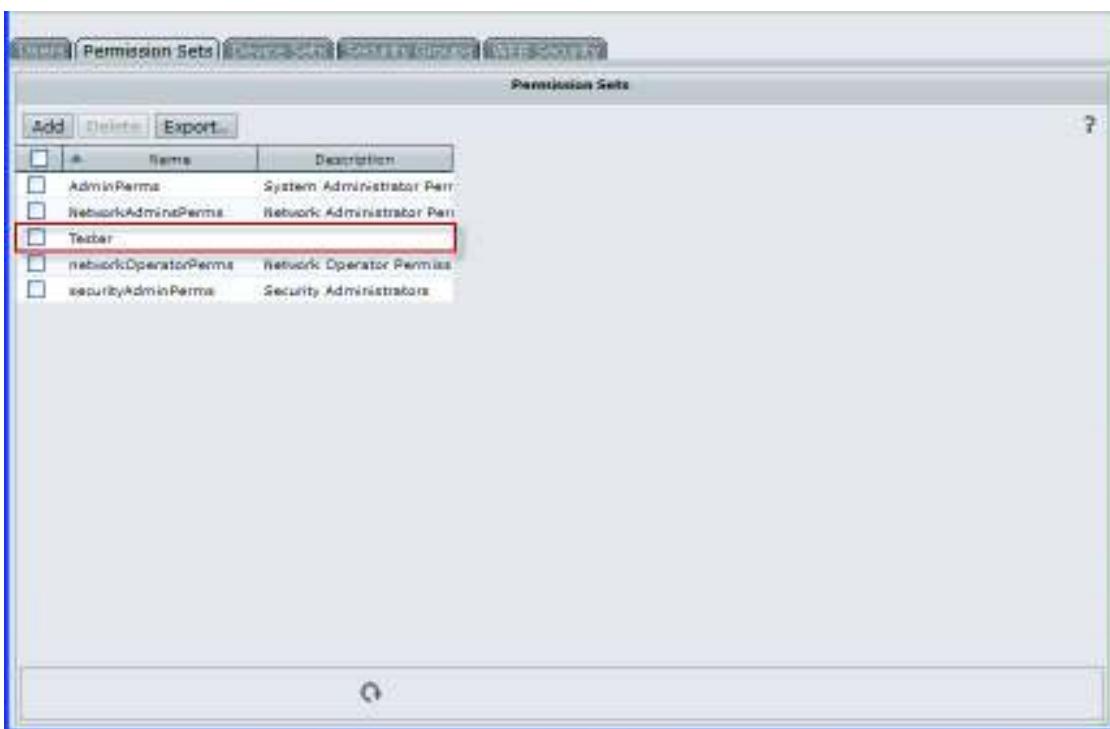


FIGURE 48. Updated list of permission sets

Modifying a Permission Set

To modify a permission set:

1. From the toolbar, select **Security > Configuration**.
2. Click the **Permission Sets** tab. The Permission Sets screen appears.
3. Select the desired permission set and double-click. The **Modify Permission Set** screen appears.

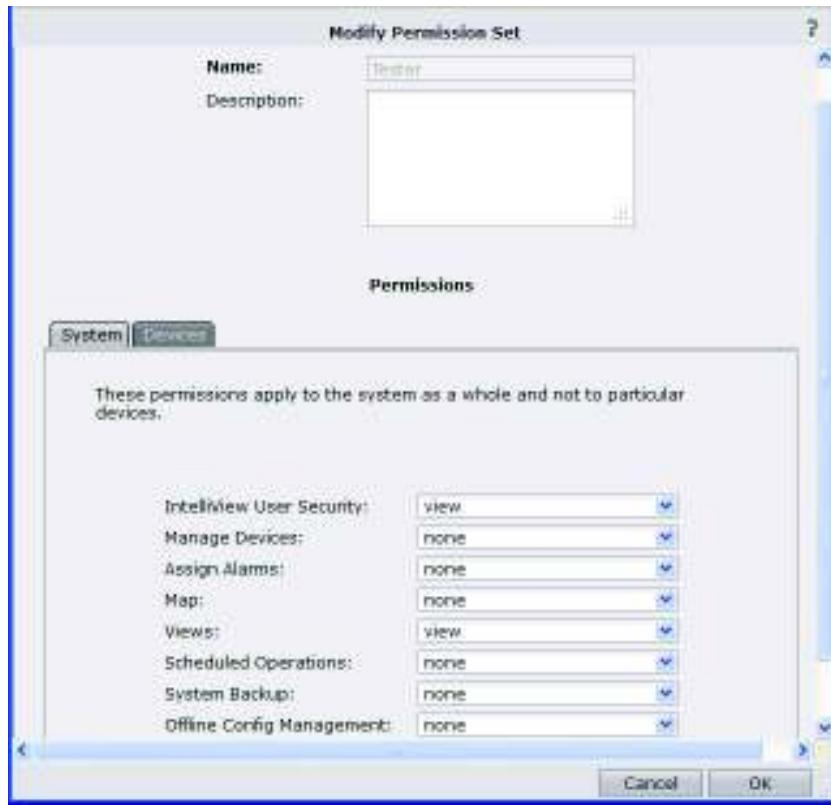


FIGURE 49. Modify Permission Set screen

4. Make change(s) to the settings.
5. Click **OK**. A system message appears confirming the operation.



FIGURE 50. Modify permission set confirmation

6. Click **OK**.

Deleting a Permission Set

To delete a permission set:

1. From the toolbar, select **Security > Configuration**.
2. Click on the **Permission Sets** tab. The **Permission Sets** screen appears.
3. Select the desired permission set.

4. Click **Delete**. The permission set is deleted from the listing and a system message appears confirming the operation.

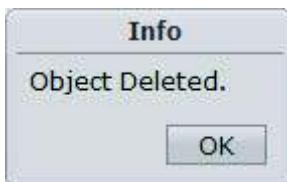


FIGURE 51. Object deleted confirmation

5. Click **OK**.

Device Sets

The System Administrator can create/modify/delete device sets. Device sets are lists of the available devices that can be used in a Security Group.

Creating a Device Set

To create a new device set:

1. From the toolbar, select **Security > Configuration**.
2. Click on the **Device Sets** tab. The **Device Sets** screen appears.

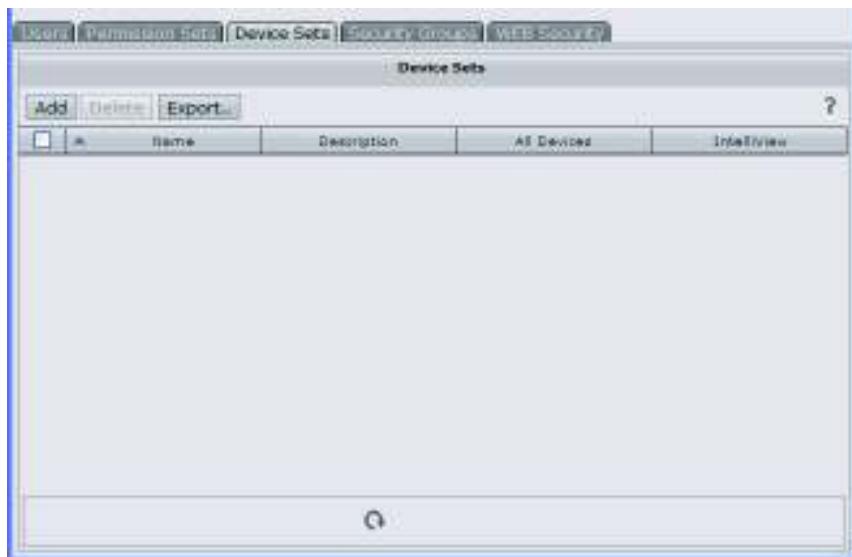


FIGURE 52. Device Sets screen

3. Click **Add**. The **Create Device Set** screen appears.

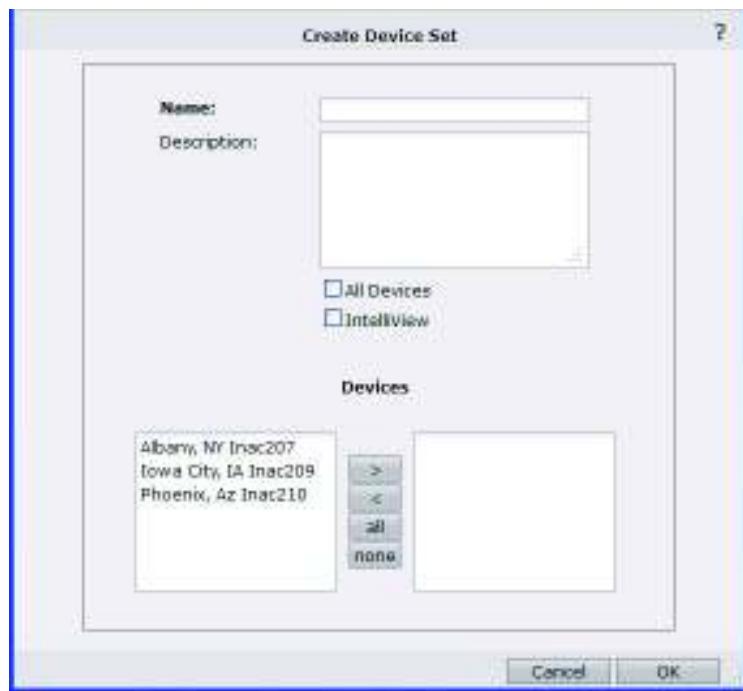


FIGURE 53. Create Device Set screen

4. Enter the device set name and description.
5. Using the right and left arrow buttons, select the devices, moving the defined devices in and out of the final list (on the right). The selected devices (in the right list) are now part of the new device set.

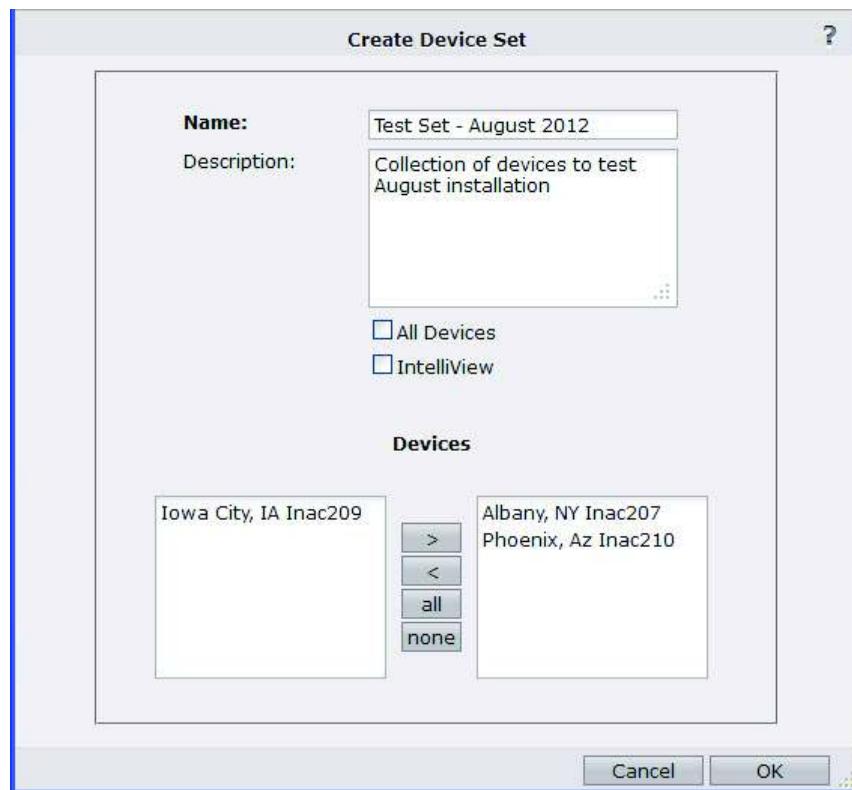


FIGURE 54. Create Device Set screen (filled)

6. Click **OK** when done. A system message appears.



FIGURE 55. Device created confirmation

7. Click **OK**. The new device set appears on the list of device sets.

Modifying a Device Set

To modify a device set:

1. From the toolbar, select **Security > Configuration**.
2. Click on the **Device Sets** tab. The **Device Sets** screen appears.



FIGURE 56. Device Sets screen

3. Double-click on the selected device set. The **Modify Device Set** screen appears.



FIGURE 57. Modify Device Set screen

4. Make changes.
5. Click **OK**. A system message appears.



FIGURE 58. Device set modified confirmation

6. Click **OK**.

Deleting a Device Set

To delete a device set:

1. From the toolbar, select **Security > Configuration**.
2. Click on the **Device Sets** tab. The **Device Sets** screen appears.
3. Select the device set.
4. Click **Delete**. The device set is removed from the list of device sets and a system message appears.



FIGURE 59. Device set deletion confirmed

5. Click **OK**.

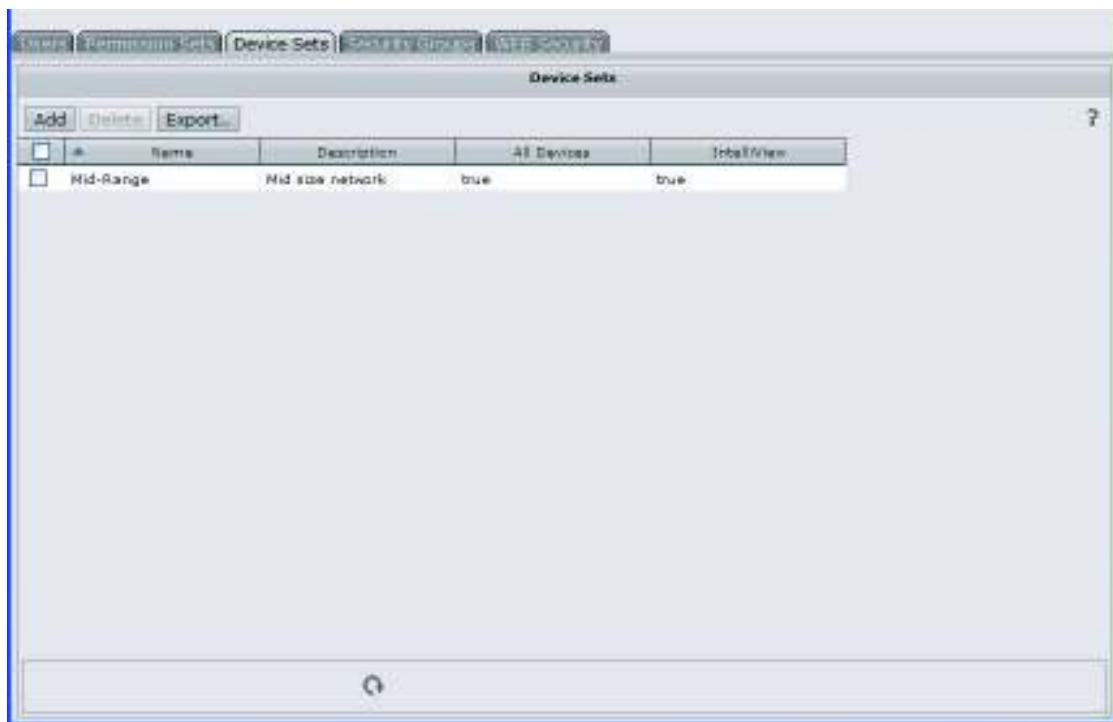


FIGURE 60. Updated list of device sets

System Backup and Restore

The administrator can perform a data backup of IntelliView so that it may be restored at a later time. This is useful if there is a hardware error and the disk have been corrupted. A backup allows the administrator to restore to another machine and quickly be up and running.

Backup Types

There are two types of supported backups:

- System Backup

This type of backup is used when the entire system is backed up. This includes the database, configuration parameters for the database, and uploaded sound and image files. This type of backup is used when the backup file will be used to restore a system.

- Security Export

This type of backup is used to store the users, their permissions, and the devices that are in the system. This backup is used to store off the security information so that it can be used to sync up with another system if desired. Only the security information and devices are copied.

The Security Export backup should only be used when the systems in question only add users, change permissions, and add devices through the export server. If the devices are added into the system through other means, when an import is done, the IntelliView IDs will not be in sync and the views and other references will not be correct.

Since an export only exports the security information, if the administrator wants two machines to be identical, a full restore is required.

Backup Permissions

The Backup/Restore function uses two permissions:

- **System Backup**

This permission allows a user to view/configure the backup configuration parameters, and to perform system backups. A user must have this permission to bring up the System Backup screens.

There are three permission levels:

- **View:** Allows the user to view the files and configuration
- **Backup:** Allows the user to backup/restore the system
- **Configure:** Allows the user to change the configuration parameters

- **Scheduled Operations**

This permission allows a user to schedule backups so they are performed automatically. This permission is necessary in order to see the Scheduler Config, Scheduled Backups, and Run Results tabs.

If the user does not have this permission, but has System Backup permission, they can access the files generated from scheduled backups.

There are two permission levels:

- **View:** Allows the user to view the configuration and scheduled backups
- **Configure:** Allows the user to change the configuration settings as well as schedule operations

System Backup for IntelliView

To backup and restore:

1. From the toolbar, select **Config > System Backup**. The System Backup screens appear. Use the Backups and Configuration tabs to manipulate the backups.
2. On the Backups tab page, If you have permission, you can invoke any of the displayed buttons:
 - **Delete:** Delete the selected backup file
 - **Backup Now:** Start a backup request
 - **Restore:** Prepare the system for a restore, which is accomplished after a server restart
 - **Export:** Currently not supported



FIGURE 61. System backup toolbar

Backup Now

1. Pressing the **Backup Now** button displays the **System Backup** screen.

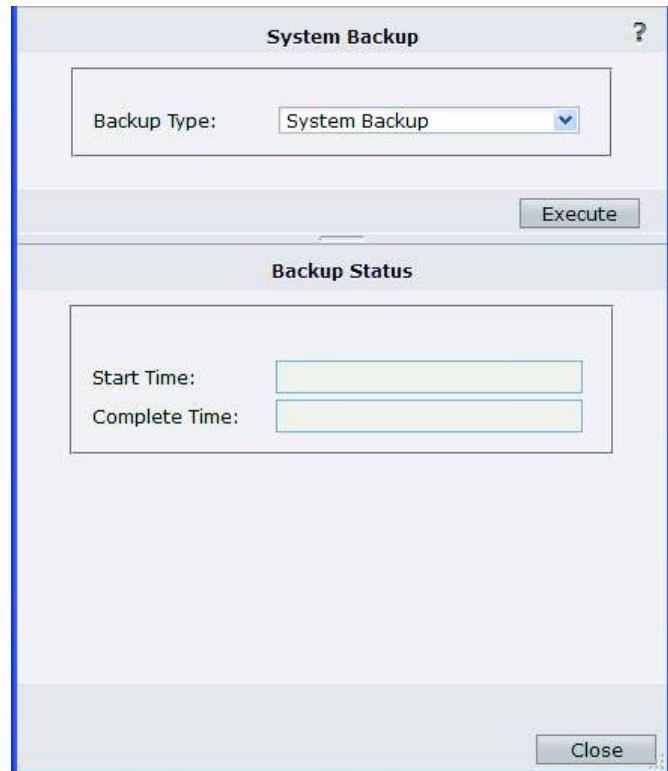


FIGURE 62. System Backup screen

2. Select the backup type (System Backup/Security Export).
3. Press **Execute**. The backup will run and present a screen showing the start and finish time.

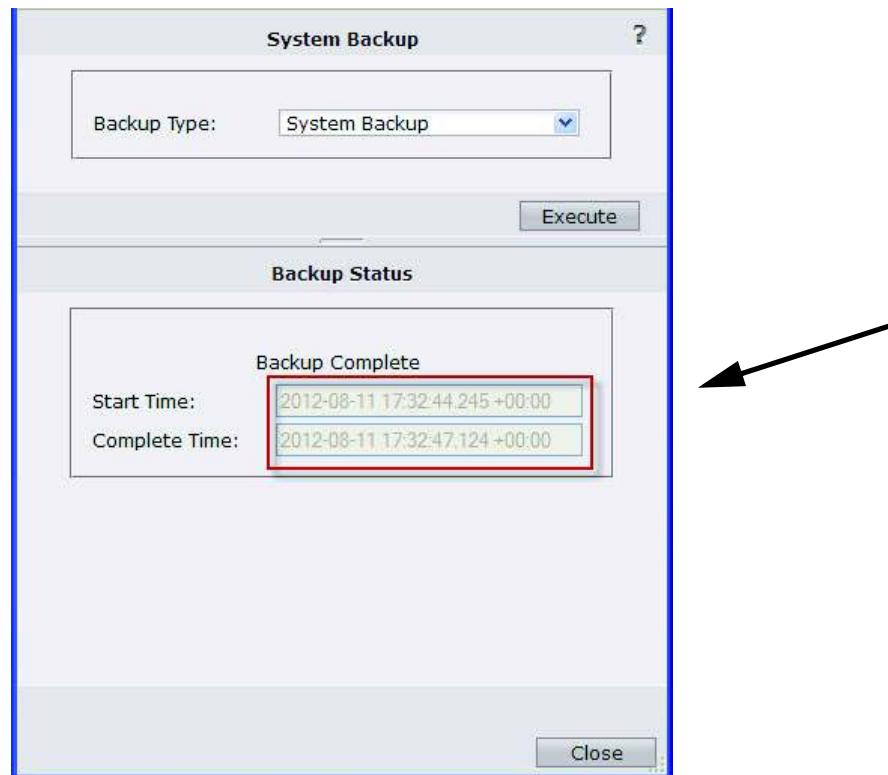


FIGURE 63. Backup Status times

If the backup fails, an error message is displayed.



FIGURE 64. Backup Status Complete

If "Backup Complete" displays, the backup completed successfully.

Restore Button

1. Pressing the **Restore** button displays the **Restore Request** screen.

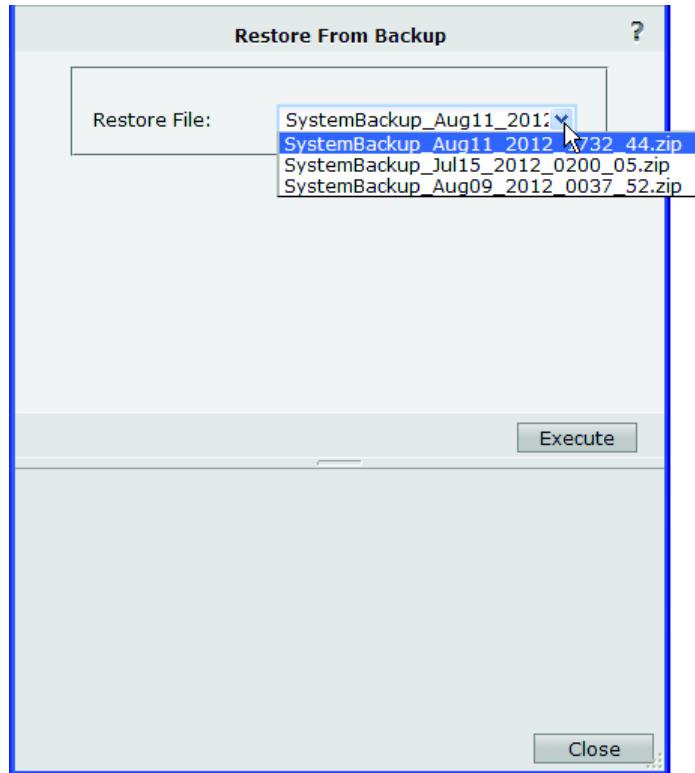


FIGURE 65. Restore from Backup screen

2. Select the file using the pull-down button.
3. Press **Execute**. The restore file is chosen to be a restore point when the system restarts.

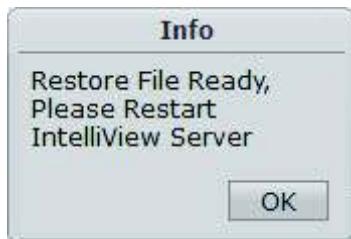


FIGURE 66. System information dialog

Restarting the server restores the server using the selected file. Only one file may be chosen at a time. If a restore is requested when another is already requested, the new request supersedes the other, and the older one is removed.

Export Backup File

Backup Configuration

The **Configuration** tab in the System Backup Config page allows the user to change the configuration parameters for the backup system. System Backup/Configure permission is required to edit the properties.

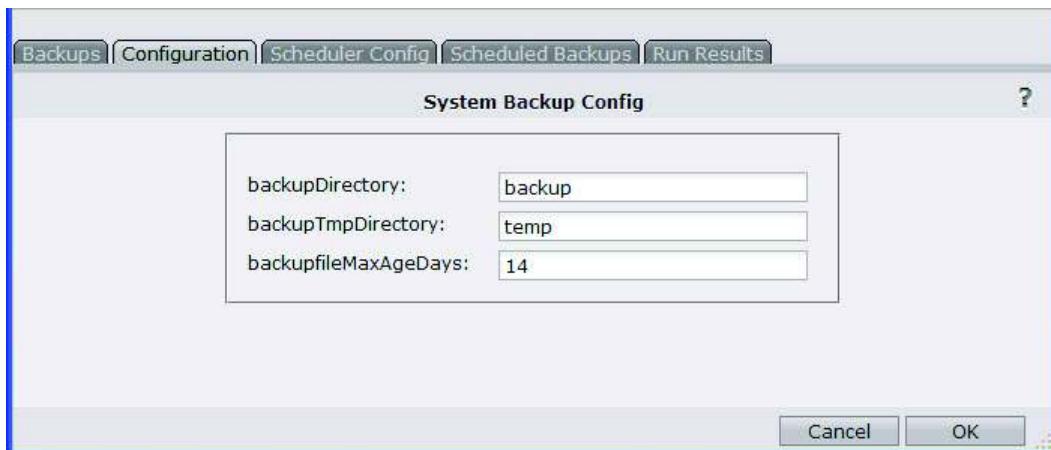


FIGURE 67. System Backup Config screen

If you have the proper permissions, the following attributes are available:

- **backupDirectory**

This directory contains the backup files generated when backups are performed. This directory is used when populating the Backups tab page. If an absolute path to the directory is not specified, it is assumed to belong in the application installation directory.

- **backupTempDirectory**

This directory specifies where the temporary directory is located. The temporary directory is needed when backups and restores are being done to create the zip files or to extract the zip files so that the restore can be processed. If an absolute path to the directory is not specified, it is assumed to belong in the applications installation directory.

- **backupfileMaxAgeDays**

This is the maximum age in days that a backup file can reach before it is deleted.

Scheduled Backups

Scheduled backups utilize the **Scheduler Config**, **Scheduled Backups**, and **Run Results** tab pages. With the addition of the Scheduled Operations permission to the System Backup permission, you have access to the Backup screens. These three tabs are not available if you do not have Scheduled Operations permission.

Scheduler Config

This tab page has only one attribute, which contains the maximum age in days that a run result (the stored result of a scheduled backup) may live before it is archived.

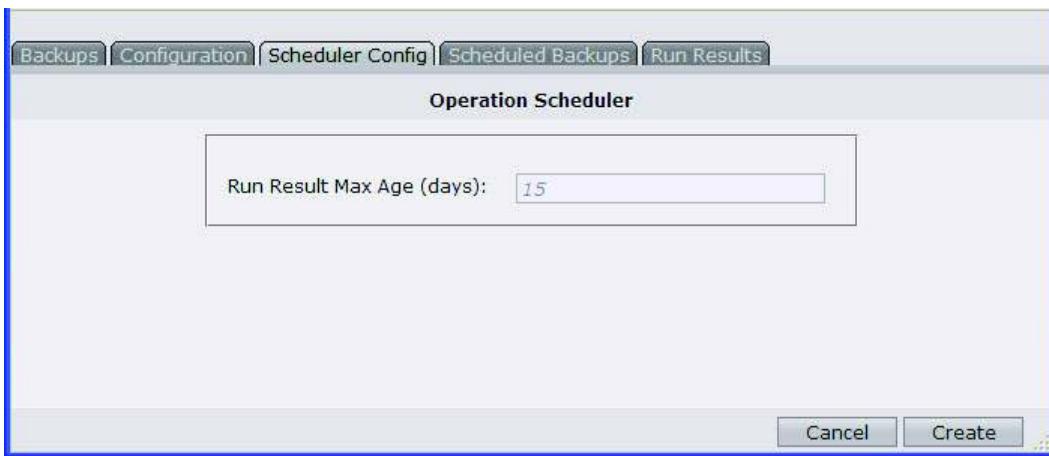


FIGURE 68. Operation Scheduler screen

Scheduled Backups

The Scheduled Operations table displayed on the **Scheduled Backups** tab page contains a listing of backups that are already scheduled. If you have configure permissions, the Add and Delete buttons are available. These buttons allow the user to add another backup or delete ones that are already scheduled.

Scheduled Operations				
	Add	Delete	Export..	
	Operation	Day To Run	Time To Run	Repeat
<input type="checkbox"/>	SystemBackup/BackupOp	Sunday	2:00 AM	false

1 of 1 Operation: SystemBackup/BackupOperation

FIGURE 69. Scheduled Operations screen

Press **Add** to begin a backup request. The Scheduled Operation screen appears:

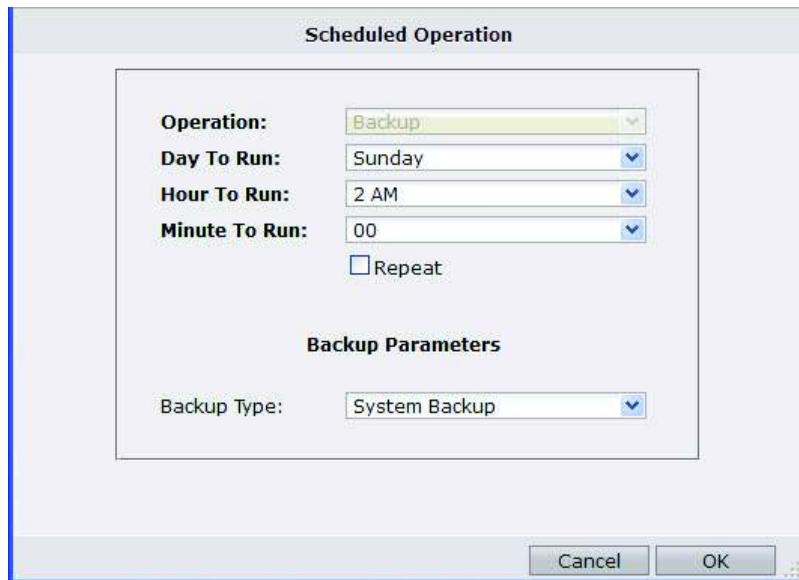


FIGURE 70. Scheduled Operation screen

The following attributes are available:

- **Operation:** This value is always set to Backup when launched from this screen.
- **Day To Run:** This value is the day set to run. The “Every Day” option is available. When the Repeat checkbox is selected, the backup will run every day at the selected time.
- Time to run is specified with two selectors:
 - **Hour To Run:** Specifies which hour to run
 - **Minute to Run:** Specifies the minute to run.
- **Repeat:** Select this checkbox if the backup is meant to run repeatedly. If this option is not selected, the backup will run once, even if “Every Day” is selected.
- **Backup Type:** Specify either System Backup or Security Export.

Run Results

The Run Results tab page displays the backup requests that have run, and states whether or not it was successful. The start and finish times are also available.

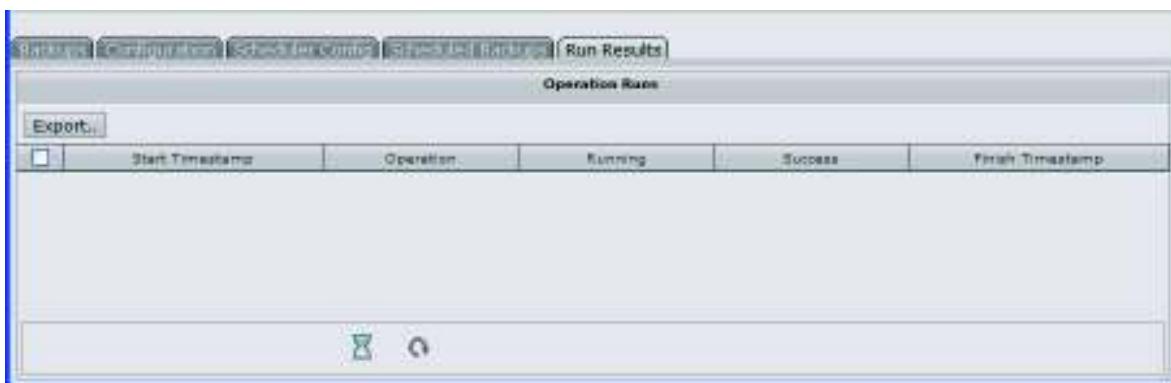


FIGURE 71. Operation Runs screen

If the backup fails, the server log contains the error message. The log can be opened to view the errors.

CHAPTER 4

Configuration

Overview

This section details how to configure IntelliView, the data, and interfaces.

Configure an IntelliNAC Node

Note IntelliNAC Nodes IP address and login credentials must match what was configured during IntelliNAC installation.

To manage an IntelliNAC:

1. On IntelliView Map click on “Devices” icon
2. Click “Manage”
3. Click “Add” button

Enter the IntelliNAC Type

Select Software version

IP address

Description of the device (Node)

Node ID (Enter four digit numerical value - Note if use transaction fail over value must be less than 1000)

SSH Port (Default 830)

SSH username (admin is default)

SSH password (must at least 8 character long, At least one each of the following: Uppercase, Lowercase, numeric and special)

Select a Key (there is a default key, or you can load your under the Devices icon “files”)

Enter and Encryption PassPhrase (if needed)

Remote IntelliVIEW Management Access - IP address (If configuring a Node that is a lower level node in an hierarchical configuration with In-band Management, enter the next level up node management IP port address)

Alternate Remote IntelliVIEW Management Access - IP address (If configuring a Node that is a lower level node in an hierarchical configuration with In-band Management, enter the next level up node management IP port address)

4. The device icon should turn into a spinner, indicating that IntelliView is attempting to connect to the IntelliNAC. When the connection process completes, you should see the node in the Unplaced sidebar (Left side of Map screen). Node icon will show Node status. Note that on initial configuration the indicator ball will be red until all modules and ports in the node are configured.

Note: That if an “! red triangle” appears next to the Node icon the Node credentials are incorrect.

Map Editing

The map can be configured or edited to meet your needs. Right-click on the map to access these functions:

- **Place Device** - removes the selected device from the Unplaced List and places the Map icon for the device so that it belongs to the current submap
- **Add Unmanaged** - creates an unmanaged device icon that is unique to this view; use to represent an unmanaged item in the management domain
- **Add Submap** - creates a new submap within the view
- **Add Link** - creates a new synthetic link that is unique to this view; use to represent network connections to Unmanaged icons and connections that devices do not report
- **Move Device** - move a currently placed device or Unmanaged icon from another submap or within the same submap
- **Properties** - modify the characteristics of the currently viewed submap.

The right-click menu contains choices that affect the map and reflect the specific functions that are also available in the toolbar for the icon if selected:

- **Remove** - removes the selection from the map
- **Add Link** - creates a new synthetic link from this device icon to another
- **Properties** - modify the characteristics of the selected submap.

Place Device

To place a device on the map:

1. Right-click on the map.
2. Select Place Device from the displayed menu. The Add Device dialog box appears.



FIGURE 72. Add Device dialog

3. The pull-down list is populated with the current list of devices that in the Unplaced List. The Unplaced List of devices are those that the user has permissions to view.
4. Click **OK** to accept, or **Cancel** to abort the operation. The map icon for the device is placed on the map where the mouse was located when the menu was selected.

Add Unmanaged

To add an Unmanaged Icon:

1. Right-click on the map.
2. Select **Add Unmanaged** from the displayed menu. The Add Unmanaged dialog box appears.

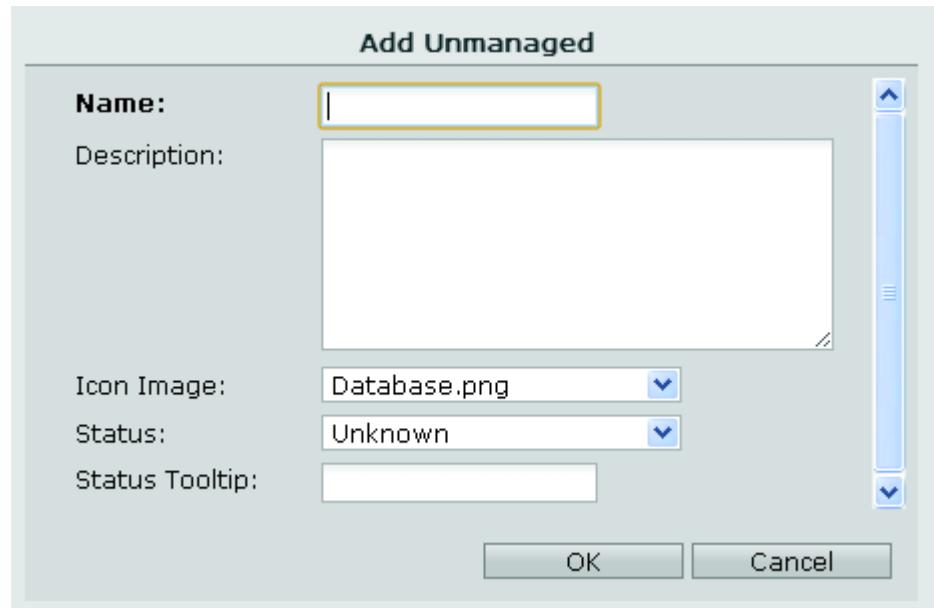


FIGURE 73. Add Unmanaged dialog

3. Enter the following fields:

- **Name** - displayed at the bottom of the icon and provided as a Search suggestion in the View Controls region.
 - **Description** - shown in the View Tree as part of the information on the Unmanaged icon and describes the purpose of the icon. Note that the maximum number of characters in the field allowed is 255 characters.
 - **Image** - any selection from the Icons table
 - **Status** - choice of a status which is reflected by its status color indicator
 - **Status Tooltip** - the text displayed when hovering over the status color indicator of the icon.
4. Click **OK**.

Add Submap

To add a submap icon:

1. Right-click on the map.
2. Select **Add Submap** from the displayed menu. The Add Submap dialog box appears.

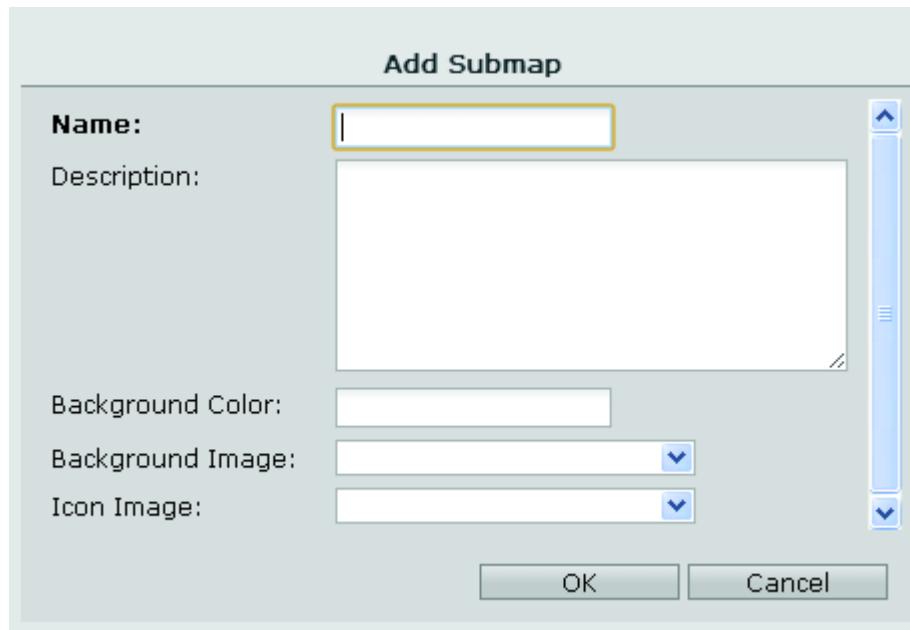


FIGURE 74. Add Submap dialog

3. Enter the following fields:

- **Name** - displayed at the bottom of the icon and provided as a Search suggestion in the View Controls region

- **Description** - shown in the View Tree as part of the information on the submap and describes the purpose of the submap. Note that the maximum number of characters in the field allowed is 255 characters.
- **Background Color** - HTML/CSS specification for a color, e.g., #f00, white, and rgb(0, 0, 255)
- **Background Image** - any selection from the Backgrounds table
- **Icon Image** - any selection from the Icons table

Add Link

Note: A synthetic link is an applied line which indicates a non-WAN physical connection exists between two map objects.

To add a synthetic link:

1. Right-click on the map.
2. Select **Add Link** from the displayed menu. The Add Link dialog box appears.

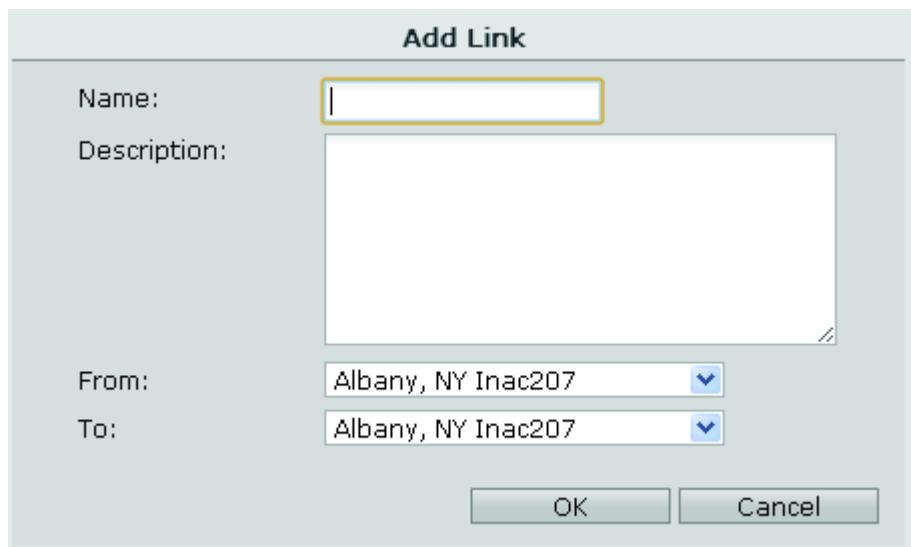


FIGURE 75. Add Link dialog

3. Enter the following fields:

- **Name** - displayed in the View tree as part of the information provided as a Search suggestion in the View Controls region
- **Description** - shown in the View Tree as part of the information on the Unmanaged icon and describes the purpose of the Unmanaged icon. Note that the maximum number of characters in the field allowed is 255 characters.
- **From** - a device or Unmanaged icon that is contained in the view's organization; one end of the link
- **To** - a device or Unmanaged icon that is contained by the view's organization; one end of the link.

Move Device

To move a device or Unmanaged icon from its current map to the map that is currently displayed:

1. Right-click on the map.
2. Select **Move Device** from the displayed menu. The Move Device dialog box appears.



FIGURE 76. Move Device dialog

3. Select the device or Unmanaged icon from the drop-down list.

The moved icon is placed at the mouse location when the right-click menu appears. If the selected device or Unmanaged icon already belongs to the current submap, then it is moved to the mouse location and remains within the submap.

Submap Properties

This function is only available for submaps and Unmanaged icons.

Editing a Submap Icon

To edit the properties of a submap icon:

1. Right-click on the map.
2. Select **Properties** from the displayed menu.
 - If the selected device icon is a submap, the Submap Properties dialog box appears. The fields are the same as those in the Add Submap dialog box.

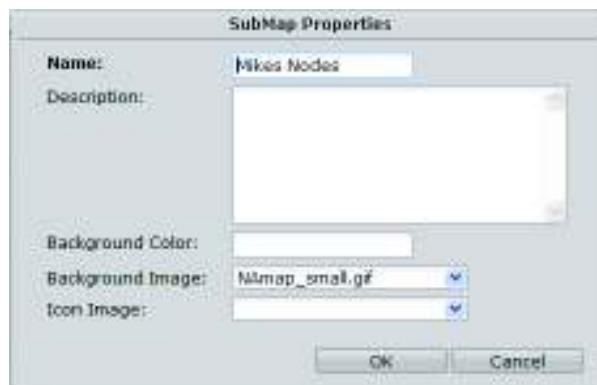


FIGURE 77. Submap Properties dialog

- If the selected device icon is an unmanaged icon, the Unmanaged Properties dialog box appears. The fields are the same as those in the Add Unmanaged dialog box.



FIGURE 78. Unmanaged Properties dialog

Remove

Removing an icon removes the device, unmanaged device, or submap from the view's organization.

- Removing a device icon returns the device to the Unplaced List .
- Removing a submap or unmanaged device permanently deletes the submap or unmanaged device. Submaps must not have any icons belonging to it or the remove operation will fail. To successfully remove a submap, remove or move out all content first.

To remove:

1. Right-click on the device icon located on map.
2. Select **Remove** from the displayed menu. See the above bullets for the resulting actions.

Add Link (Device Icons)

To add a link between device icons:

1. Right-click on the device icon located on the map.
2. Select **Add Link (Device Icons)** from the displayed menu. The **From** selection is already set for the device or unmanaged icon name.
3. Enter the **To** target to complete the synthetic link.

Link Path Details

Clicking on the link's popup badge opens the Link Path Details table.



Status	Endpoint	SubMaps	Endpoint	Actions
	BossMan	EU - System - US	Boston	Delete
	Boston (Robyn)	US - System - EU	Robyn (Boston)	
	Phoenix (Robyn)	US - System - EU	Robyn (Phoenix)	

Displaying 1 - 3 of 3

FIGURE 79. Link Path Details table

Each link shows its current status, submaps through which the link travels, and if it's a synthetic link, the option to delete the link. Automatic links cannot be deleted except when the configuration of one of the endpoint devices is modified (removing the connection that is represented by the link).

Double-clicking on a row in the table produces a Details screen for the specific link.



FIGURE 80. Automatic Link Details screen

Automatic links show a read-only detail about the endpoints and link status.

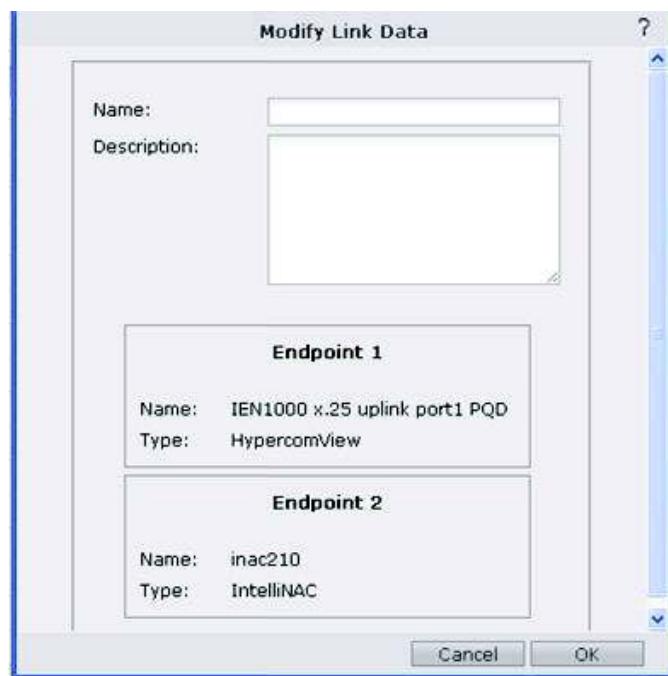


FIGURE 81. Modify Link Data screen

If the link is synthetic, you can also edit the name and description of the link.

NAC to NAC Configuration

The administrator is able to configure the network hierarchy by using intermediate INAC devices as concentrator. See use case example below: (NAC to NAC with transaction fail over, out of band management)

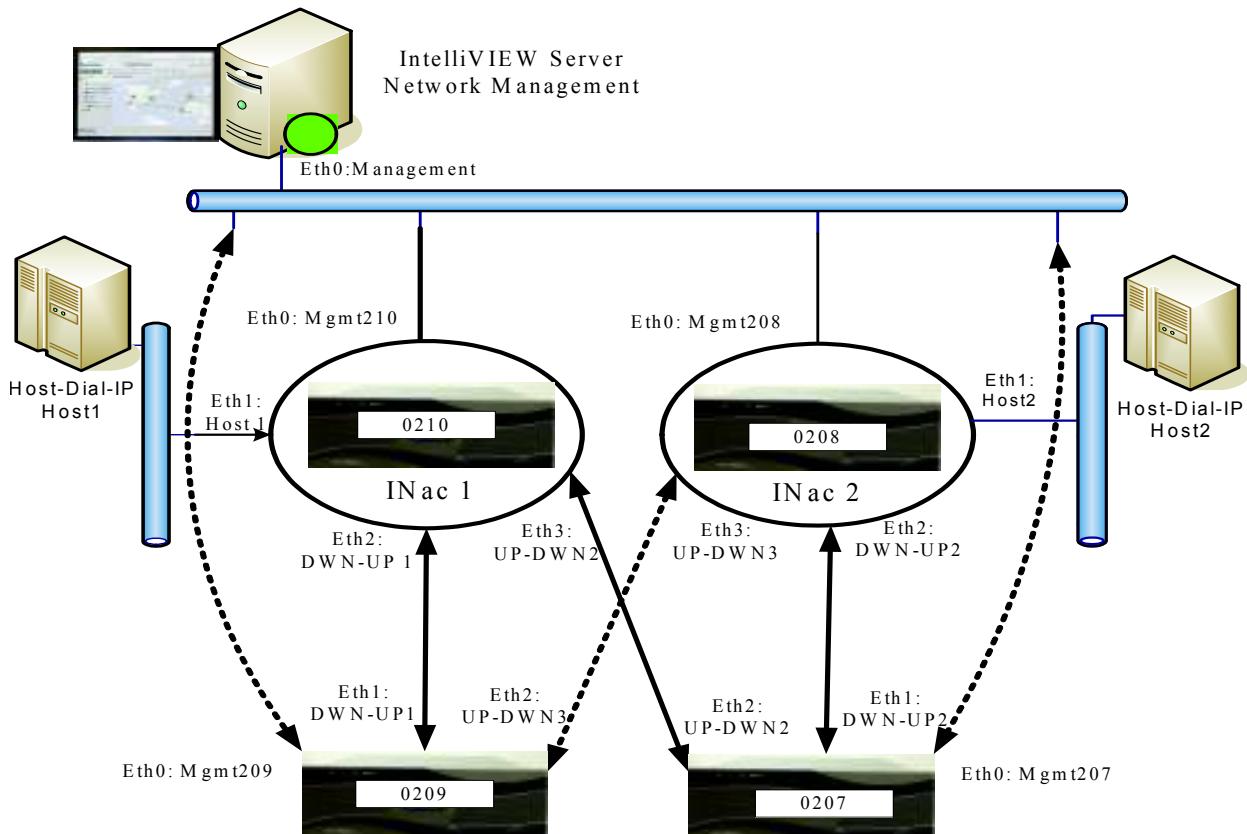


FIGURE 82. Transaction Load Balance and or Fail over example diagram

Device configuration (INAC Deployment)

All INAC's must be deployed (installed) with unique Node ID's and Management port IP address (0207, 0208, 0209, 0210, Mgmt207, Mgmt208, Mgmt209, Mgmt210). For this particular configuration the management port is configured on ETH0 on all the nodes (does not have to be).

Create four Nodes with names of 0207 through 0210, with Node ID's of 1007 through 1010

Ethernet Port configuration for NAC to NAC link configuration

1. Select the device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Ports** under Configuration > Hardware.

NAC to NAC Configuration

3. In the configure screen click on **Ethernet** tab
4. The Ethernet screen appears.

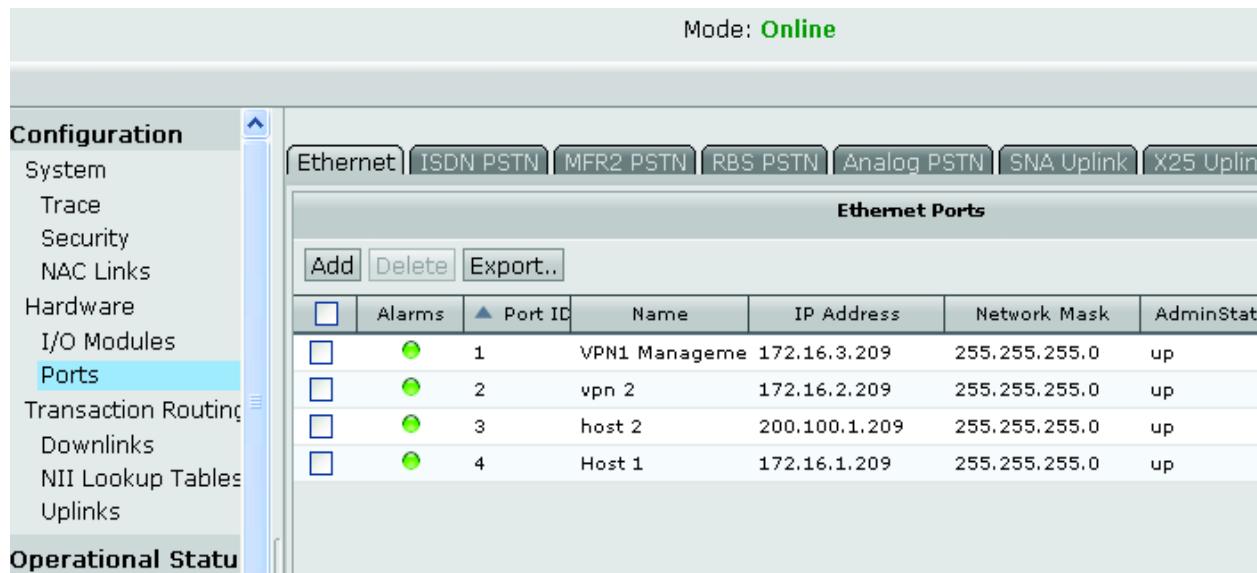


FIGURE 83. Ports configuration screen (Ethernet)

5. Click on Add to configure that nodes Ethernet Ports
 6. Repeat on each node in the NAC to NAC configuration
- Note Port ID: 1 = ETH0, 2 = ETH1, etc...

Configuration

Node 0210 Ethernet port configuration

210 ETH0 port configuration

Ethernet Port

Port ID:	1
Name:	Management 210
IP Address:	Mgmt210
Network Mask:	255.255.255.0
Warning:	This is management port!
Admin State:	up
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; height: 150px; width: 100%;"><div style="border-bottom: 1px solid #ccc; height: 10px;"></div><div style="text-align: right; margin-top: -5px;">+</div><div style="text-align: left; margin-top: -5px;">-</div></div>
Dedicated Downlink:	<input type="checkbox"/> Default: false

FIGURE 84. Node 0210 Ethernet Port 1 Configuration screen

210 ETH1 port configuration

Ethernet Port

Port ID:	2
Name:	Host 210
IP Address:	Host.1.210
Network Mask:	255.255.255.0
Warning:	
Admin State:	up
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; height: 150px; width: 100%;"></div> <div style="text-align: right; margin-top: -10px;">+ -</div>
Dedicated Downlink:	<input type="checkbox"/> Default: false

FIGURE 85. Node 0210 Ethernet Port 2 Configuration screen

210 ETH2 port configuration

Ethernet Port

Port ID:	<input type="text" value="3"/>
Name:	<input type="text" value="DWN-UP1"/>
IP Address:	<input type="text" value="DWN-UP1-210"/>
Network Mask:	<input type="text" value="255.255.255.0"/>
Warning:	
Admin State:	<input style="width: 100px; height: 20px; border: 1px solid #ccc; padding: 2px;" type="text" value="up"/> ▼
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 150px; margin-top: 10px;">+ -</div>
Dedicated Downlink:	<input style="width: 200px; height: 25px; border: 1px solid #ccc; padding: 2px;" type="text" value="Default: false"/> ▼

FIGURE 86. Node 0210 Ethernet Port 3 Configuration screen

210 ETH3 port configuration

Ethernet Port

Port ID:	<input type="text" value="4"/>
Name:	<input type="text" value="UP-DWN2"/>
IP Address:	<input type="text" value="UP-DWN2-210"/>
Network Mask:	<input type="text" value="255.255.255.0"/>
Warning:	
Admin State:	<input style="width: 100px; height: 20px; border: 1px solid #ccc; padding: 2px;" type="text" value="up"/> ▼
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 150px; margin-top: 10px;">+ -</div>
Dedicated Downlink:	<input style="width: 200px; height: 25px; border: 1px solid #ccc; padding: 2px;" type="text" value="Default: false"/> ▼

FIGURE 87. Node 0210 Ethernet Port 4 Configuration screen

Configuration

Node 0208 Ethernet port configuration

208 ETH0 port configuration

Ethernet Port

Port ID:	1
Name:	Management 208
IP Address:	Mgmt208
Network Mask:	255.255.255.0
Warning:	This is management port!
Admin State:	up
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; height: 150px; width: 100%;"><div style="border-bottom: 1px solid #ccc; height: 10px;"></div><div style="text-align: right; margin-top: -5px;">+</div><div style="text-align: left; margin-top: -5px;">-</div></div>
Dedicated Downlink:	<input type="checkbox"/> Default: false

FIGURE 88. Node 0208 Ethernet Port 1 Configuration screen

208 ETH1 port configuration

Ethernet Port

Port ID:	2				
Name:	Host 208				
IP Address:	Host.2.208				
Network Mask:	255.255.255.0				
Warning:					
Admin State:	up				
Static Routes:	<table border="1" style="width: 100%;"><tr><td style="padding: 5px;"> </td><td style="text-align: right; padding: 5px;">+</td></tr><tr><td style="padding: 5px;"> </td><td style="text-align: right; padding: 5px;">-</td></tr></table>		+		-
	+				
	-				
Dedicated Downlink:	<input type="checkbox"/> Default: false				

FIGURE 89. Node 0208 Ethernet Port 2 Configuration screen

208 ETH2 port configuration

Ethernet Port

Port ID:	<input type="text" value="3"/>
Name:	<input type="text" value="DWN-UP2"/>
IP Address:	<input type="text" value="DWN-UP-208"/>
Network Mask:	<input type="text" value="255.255.255.0"/>
Warning:	<input type="text" value=""/>
Admin State:	<input style="background-color: #e0ffe0; color: green; font-weight: bold; font-style: italic; font-size: 1em; padding: 2px 5px; border: 1px solid #ccc; border-radius: 3px; width: 100px; height: 1.2em; vertical-align: middle;" type="text" value="up"/> ▼
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; width: 400px; height: 300px; margin-top: 10px; position: relative; border-radius: 5px;"><div style="position: absolute; right: -10px; top: -10px; width: 20px; height: 20px; background-color: #e0e0e0; border-radius: 50%; display: flex; align-items: center; justify-content: center; font-size: 1.5em; font-weight: bold; color: #ccc;">+</div><div style="position: absolute; right: -10px; bottom: -10px; width: 20px; height: 20px; background-color: #e0e0e0; border-radius: 50%; display: flex; align-items: center; justify-content: center; font-size: 1.5em; font-weight: bold; color: #ccc;">-</div><div style="position: absolute; left: 10px; top: 10px; width: 10px; height: 10px; background-color: #e0e0e0; border-radius: 5px; display: flex; align-items: center; justify-content: center; font-size: 0.8em; font-weight: bold; color: #ccc;">◀</div><div style="position: absolute; right: 10px; top: 10px; width: 10px; height: 10px; background-color: #e0e0e0; border-radius: 5px; display: flex; align-items: center; justify-content: center; font-size: 0.8em; font-weight: bold; color: #ccc;">▶</div><div style="position: absolute; left: 50%; top: 50%; width: 10px; height: 10px; background-color: #e0e0e0; border-radius: 5px; display: flex; align-items: center; justify-content: center; font-size: 0.8em; font-weight: bold; color: #ccc;">III</div></div>
Dedicated Downlink:	<input style="width: 200px; border: 1px solid #ccc; border-radius: 3px; padding: 2px 5px; font-size: 0.9em;" type="text" value="Default: false"/> ▼

FIGURE 90. Node 0208 Ethernet Port 3 Configuration screen

208 ETH3 port configuration

Ethernet Port

Port ID:	4
Name:	UP-DWN3
IP Address:	UP-DWN3-208
Network Mask:	255.255.255.0
Warning:	
Admin State:	up
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; width: 400px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> + - </div> <div style="margin-top: 10px; border: 1px solid #ccc; height: 10px; background-color: #f0f0f0;"></div> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> < > </div> </div>
Dedicated Downlink:	Default: false

FIGURE 91. Node 0208 Ethernet Port 4 Configuration screen

Configuration

Node 0209 Ethernet port configuration

209 ETH0 port configuration

Ethernet Port

Port ID:	<input type="text" value="1"/>
Name:	<input type="text" value="Management 209"/>
IP Address:	<input type="text" value="Mgmt209"/>
Network Mask:	<input type="text" value="255.255.255.0"/>
Warning:	This is management port!
Admin State:	<input style="background-color: #e0ffe0; color: green; font-weight: bold; font-style: italic; font-size: 1em; padding: 2px 5px; border: 1px solid #ccc; border-radius: 3px; width: 100px; height: 1.2em; vertical-align: middle;" type="text" value="up"/> ▼
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; width: 400px; height: 200px; margin-top: 10px; position: relative; border-radius: 5px;">+-<div style="border: 1px solid #ccc; width: 100%; height: 100%; position: absolute; left: 0; top: 0; background: #f0f0f0; border-radius: 5px;"></div><div style="position: absolute; bottom: 10px; left: 10px; width: 100%; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; left: 50%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 10px; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 50%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 75%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 90%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 95%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 100%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 105%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 110%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 115%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 120%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 125%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 130%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 135%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 140%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 145%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 150%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 155%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 160%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 165%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 170%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 175%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 180%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 185%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 190%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 195%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 200%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 205%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 210%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 215%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 220%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 225%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 230%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 235%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 240%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 245%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 250%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 255%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 260%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 265%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 270%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 275%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 280%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 285%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 290%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 295%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 300%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 305%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 310%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 315%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 320%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 325%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 330%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 335%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 340%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 345%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 350%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 355%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 360%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 365%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 370%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 375%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 380%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 385%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 390%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 395%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 400%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 405%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 410%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 415%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 420%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 425%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 430%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 435%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 440%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 445%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 450%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 455%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 460%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 465%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 470%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 475%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 480%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 485%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 490%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 495%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 500%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 505%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 510%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 515%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 520%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 525%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 530%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 535%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 540%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 545%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 550%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 555%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 560%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 565%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 570%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 575%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 580%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 585%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 590%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 595%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 600%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 605%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 610%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 615%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 620%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 625%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 630%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 635%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 640%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 645%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 650%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 655%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 660%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 665%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 670%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 675%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 680%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 685%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 690%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 695%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 700%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 705%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 710%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 715%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 720%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 725%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 730%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 735%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 740%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 745%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 750%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 755%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 760%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 765%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 770%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 775%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 780%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 785%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 790%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 795%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 800%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 805%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 810%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 815%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 820%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 825%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 830%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 835%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 840%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 845%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 850%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 855%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 860%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 865%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 870%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 875%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 880%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 885%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 890%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 895%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 900%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 905%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 910%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 915%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 920%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 925%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 930%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 935%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 940%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 945%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position: absolute; bottom: 10px; right: 950%; width: 10px; height: 10px; background: #f0f0f0; border-radius: 5px; z-index: 1;"></div><div style="position:</div>

209 ETH1 port configuration

Ethernet Port

Port ID:	2				
Name:	DWN-UP1				
IP Address:	DWN-UP1-209				
Network Mask:	255.255.255.0				
Warning:					
Admin State:	up				
Static Routes:	<table border="1" style="width: 100%;"><tr><td style="padding: 5px;"> </td><td style="text-align: right; padding: 5px;">+</td></tr><tr><td style="padding: 5px;"> </td><td style="text-align: right; padding: 5px;">-</td></tr></table>		+		-
	+				
	-				
Dedicated Downlink:	<i>Default: false</i>				

FIGURE 93. Node 0209 Ethernet Port 2 Configuration screen

209 ETH2 port configuration

Ethernet Port

Port ID:	<input type="text" value="3"/>
Name:	<input type="text" value="UP-DWN3"/>
IP Address:	<input type="text" value="UP-DWN3-209"/>
Network Mask:	<input type="text" value="255.255.255.0"/>
Warning:	<input type="text"/>
Admin State:	<input style="width: 100px; height: 20px; border: 1px solid #ccc; padding: 2px;" type="text" value="up"/> ▼
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 150px; width: 100%;">+ -</div>
Dedicated Downlink:	<input style="width: 100px; height: 20px; border: 1px solid #ccc; padding: 2px;" type="text" value="Default: false"/> ▼

FIGURE 94. Node 0209 Ethernet Port 3 Configuration screen

Node 0207 Ethernet port configuration

207 ETH0 port configuration

Ethernet Port

Port ID:	1
Name:	Management 207
IP Address:	Mgmt207
Network Mask:	255.255.255.0
Warning:	This is management port!
Admin State:	up
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; height: 150px; width: 100%;"><p style="margin: 0;">(Empty Static Routes list)</p><div style="text-align: right; margin-top: -10px;">+-</div></div>
Dedicated Downlink:	<input type="checkbox"/> Default: false

FIGURE 95. Node 0207 Ethernet Port 1 Configuration screen

207 ETH1 port configuration

Ethernet Port

Port ID:	<input type="text" value="2"/>
Name:	<input type="text" value="DWN-UP2"/>
IP Address:	<input type="text" value="DWN-UP2-207"/>
Network Mask:	<input type="text" value="255.255.255.0"/>
Warning:	<input type="text"/>
Admin State:	<input style="width: 100px; height: 20px; border: 1px solid #ccc; padding: 2px;" type="text" value="up"/> ▼
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 150px; width: 100%;">+ -</div>
Dedicated Downlink:	<input style="width: 100px; height: 20px; border: 1px solid #ccc; padding: 2px;" type="text" value="Default: false"/> ▼

FIGURE 96. Node 0207 Ethernet Port 2 Configuration screen

207 ETH2 port configuration

Ethernet Port

Port ID:	<input type="text" value="3"/>
Name:	<input type="text" value="UP-DWN2"/>
IP Address:	<input type="text" value="UP-DWN2-207"/>
Network Mask:	<input type="text" value="255.255.255.0"/>
Warning:	<input type="text"/>
Admin State:	<input style="width: 100px; height: 20px; border: 1px solid #ccc; padding: 2px;" type="text" value="up"/> ▼
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; width: 400px; height: 150px; margin-top: 10px;"></div> <div style="display: flex; justify-content: space-around; width: 100%;">+-</div>
Dedicated Downlink:	<input style="width: 200px; height: 20px; border: 1px solid #ccc; padding: 2px;" type="text" value="Default: false"/> ▼

FIGURE 97. Node 0207 Ethernet Port 3 Configuration screen

Configuration

IntelliVIEW device NAC to NAC link configuration

1. Select the device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **NAC Links** under Configuration > System.

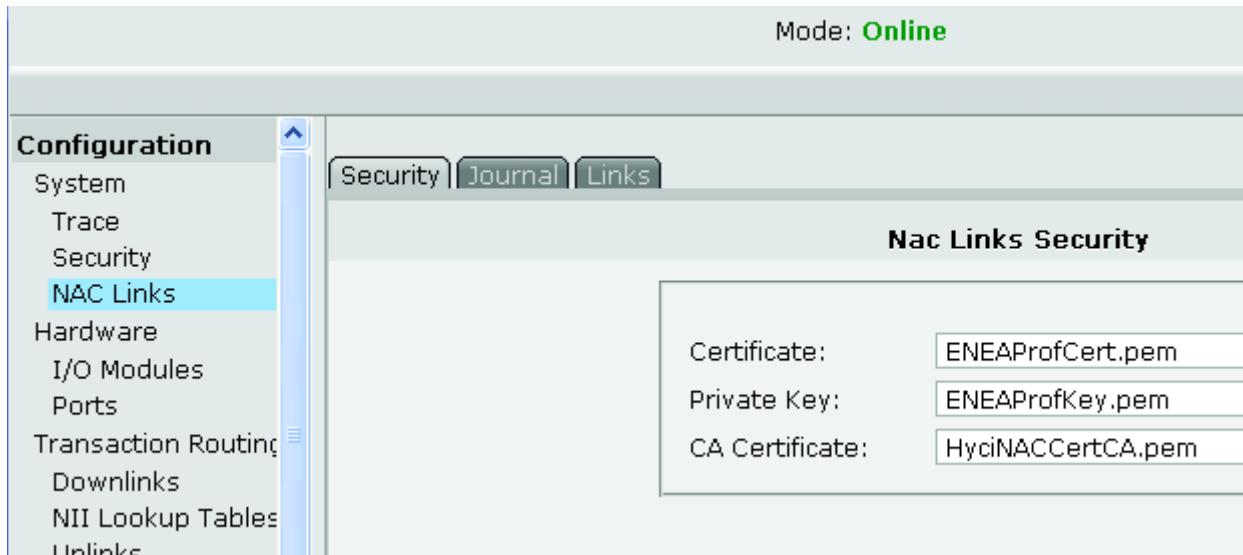


FIGURE 98. NAC links screen

3. In the configure screen click on **Links** tab
4. The NAC links screen appears.



FIGURE 99. NAC links Configuration screen

5. Click on Add to configure that nodes NAC to NAC link
6. Repeat on each node in the NAC top NAC configuration

Node 0210 configuration

NAC Link

Link Name:	210 to 209
Enable:	true
Local Address:	UP-DWN1-210
Local Gateway:	UP-DWN1-210
Remote Address:	UP-DWN1-209
Remote Gateway:	UP-DWN1-209
priority:	<i>Default: false</i>

NAC Link

Link Name:	210 to 207
Enable:	true
Local Address:	DWN-UP2-210
Local Gateway:	DWN-UP2-210
Remote Address:	DWN-UP2-207
Remote Gateway:	DWN-UP2-207
priority:	<i>Default: false</i>

FIGURE 100. Node 0210 NAC links Configuration screens

Node 0208 Configuration

NAC Link

Link Name:	208 to 207
Enable:	true
Local Address:	DWN-UP2-208
Local Gateway:	DWN-UP2-208
Remote Address:	DWN-UP2-207
Remote Gateway:	DWN-UP2-207
priority:	<i>Default: false</i>

NAC Link

Link Name:	208 to 209
Enable:	true
Local Address:	UP-DWN3-208
Local Gateway:	UP-DWN3-208
Remote Address:	UP-DWN3-209
Remote Gateway:	UP-DWN3-209
priority:	<i>Default: false</i>

FIGURE 101. Node 0208 NAC links Configuration screens

NAC to NAC Configuration

Node0209 Configuration

NAC Link

Link Name:	209 to 210
Enable:	true
Local Address:	DWN-UP1-209
Local Gateway:	DWN-UP1-209
Remote Address:	DWN-UP1-210
Remote Gateway:	DWN-UP1-210
priority:	<i>Default: false</i>

NAC Link

Link Name:	209 to 208
Enable:	true
Local Address:	UP-DWN3-209
Local Gateway:	UP-DWN3-209
Remote Address:	UP-DWN3-208
Remote Gateway:	UP-DWN3-209
priority:	<i>Default: false</i>

FIGURE 102. Node 0209 NAC links Configuration screens

Node 207 Configuration

NAC Link

Link Name:	207 to 210
Enable:	true
Local Address:	UP-DWN2-207
Local Gateway:	UP-DWN2-207
Remote Address:	UP-DWN2-210
Remote Gateway:	UP-DWN2-210
priority:	<i>Default: false</i>

NAC Link

Link Name:	207 to 208
Enable:	true
Local Address:	DWN-UP2-207
Local Gateway:	DWN-UP2-207
Remote Address:	DWN-UP2-208
Remote Gateway:	DWN-UP2-208
priority:	<i>Default: false</i>

FIGURE 103. Node 0207 NAC links Configuration screens

Configure the NII's for load balance or fail over.

Fail over

Configure node name 0210 TCP/IP Uplinks

Configure Primary host

1. Select the 0210 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

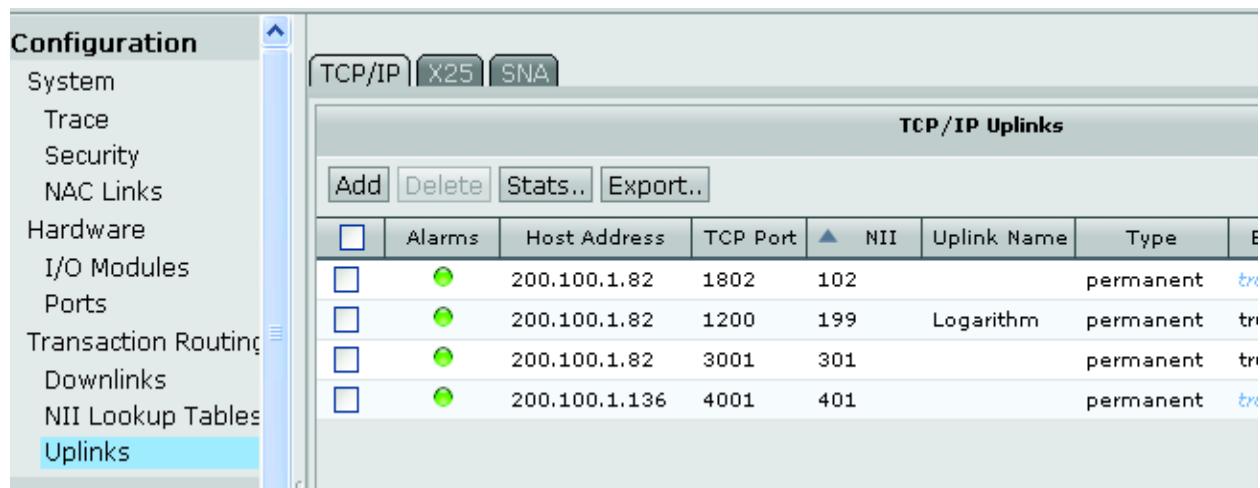


FIGURE 104. Node Configuration (Uplinks)

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	HOST1
TCP Port:	1400
NII:	500
Uplink Name:	Host1 Primary
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 105. Node 0210 Host1 TCP/IP Uplink Primary Configuration screens

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (a value lower than 1000 for primary NII is required for fail over configurations)
10. Enter any other configuration settings
11. Click **OK**

Now on node 0210 configure fail over host

1. Select the 0210 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.

3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

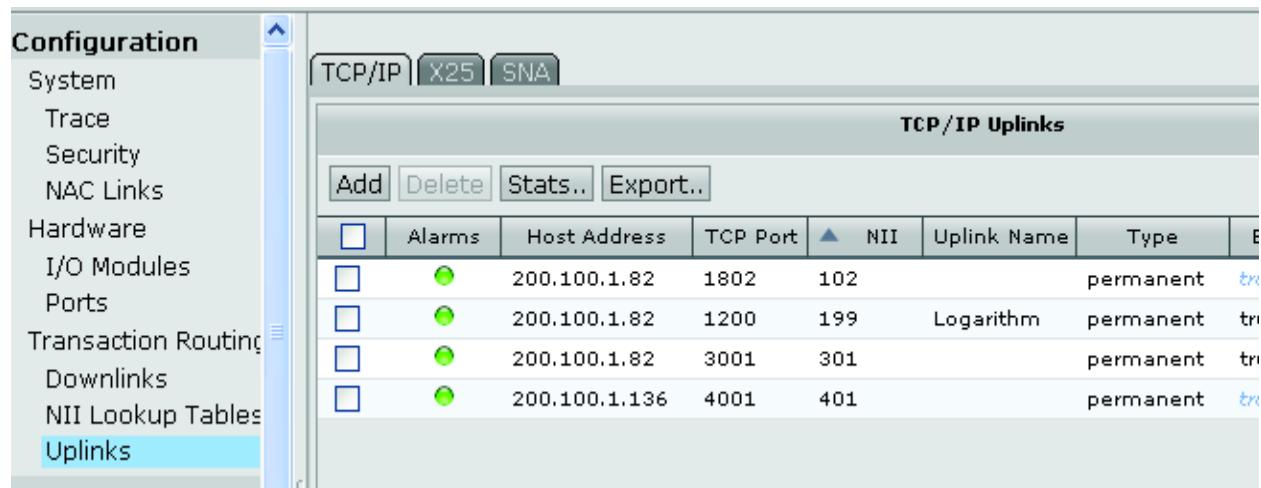


FIGURE 106. Node Configuration (Uplinks)

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

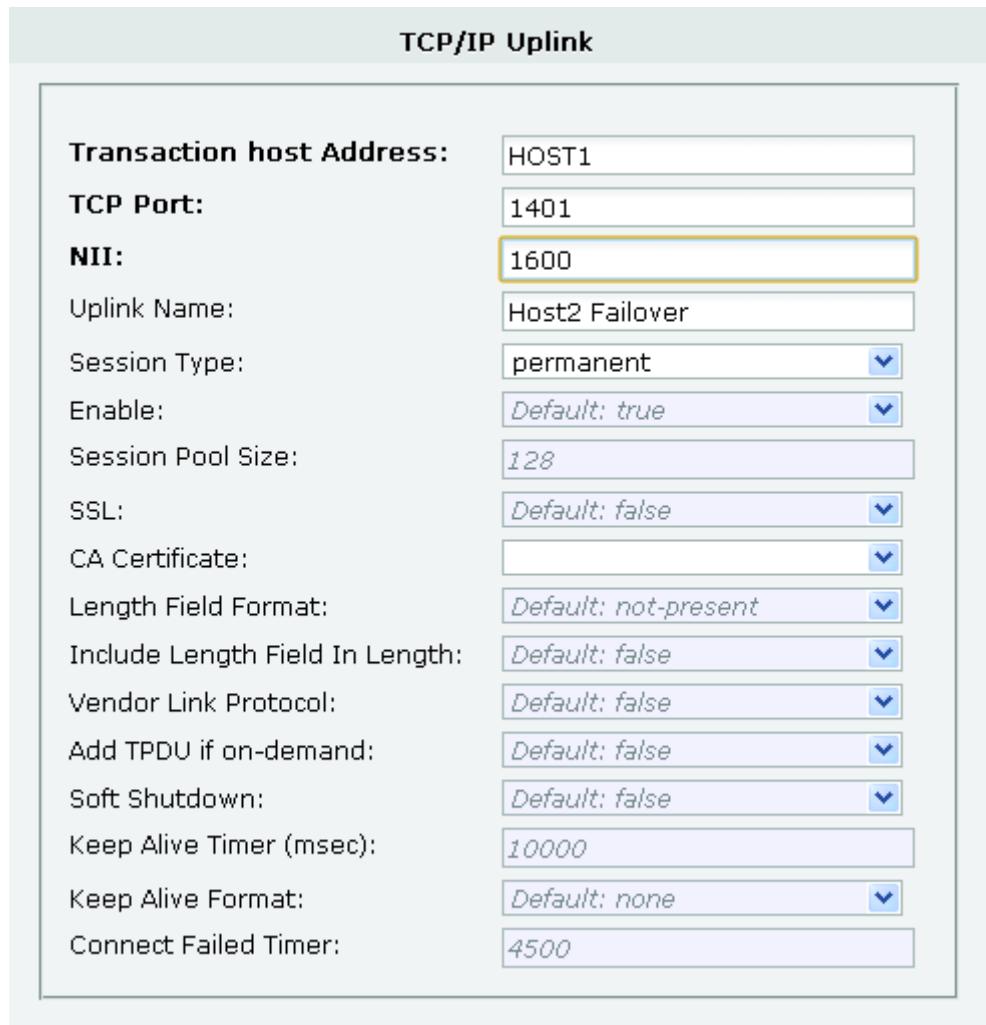


FIGURE 107. Node 0210 Host 1 TCP/IP Uplink Fail over Configuration screens

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (a value of exact 1000 more for fail over NII is required for fail over configurations. If Primary NII was 600 then the failover NII will be 1600)
10. Enter any other configuration settings
11. Click **OK**

Configure node name 0208 TCP/IP Uplinks

Configure Primary host

1. Select the 0208 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

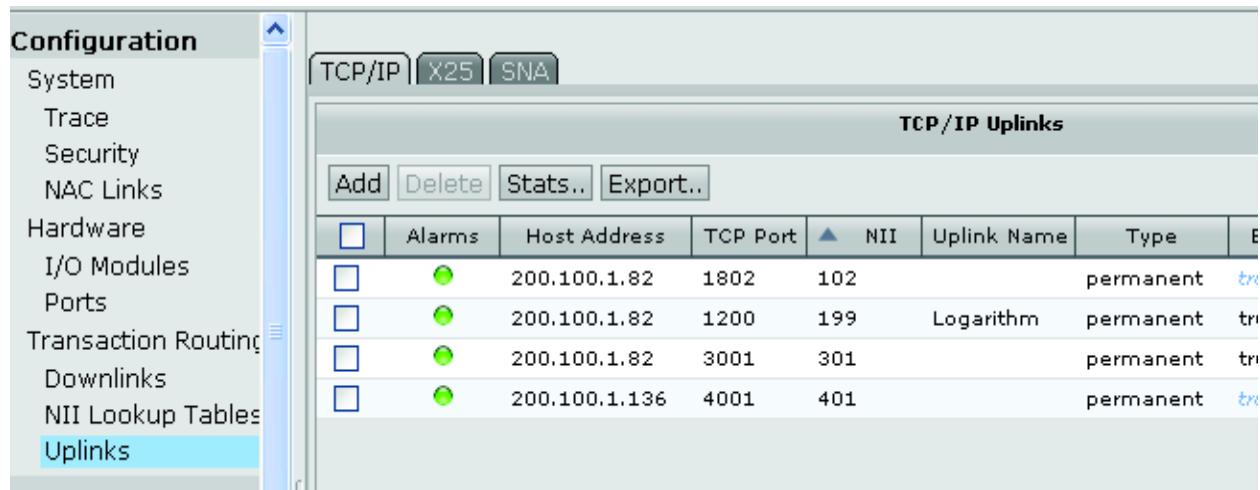


FIGURE 108. Node Configuration (Uplinks)

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	HOST2
TCP Port:	1400
NII:	600
Uplink Name:	Host2 Primary
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 109. Node 0208 Host2 TCP/IP Uplink Primary Configuration screens

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (a value lower than 1000 for primary NII is required for fail over configurations)
10. Enter any other configuration settings
11. Click **OK**

Now on node 0208 configure fail over host

1. Select the 0208 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

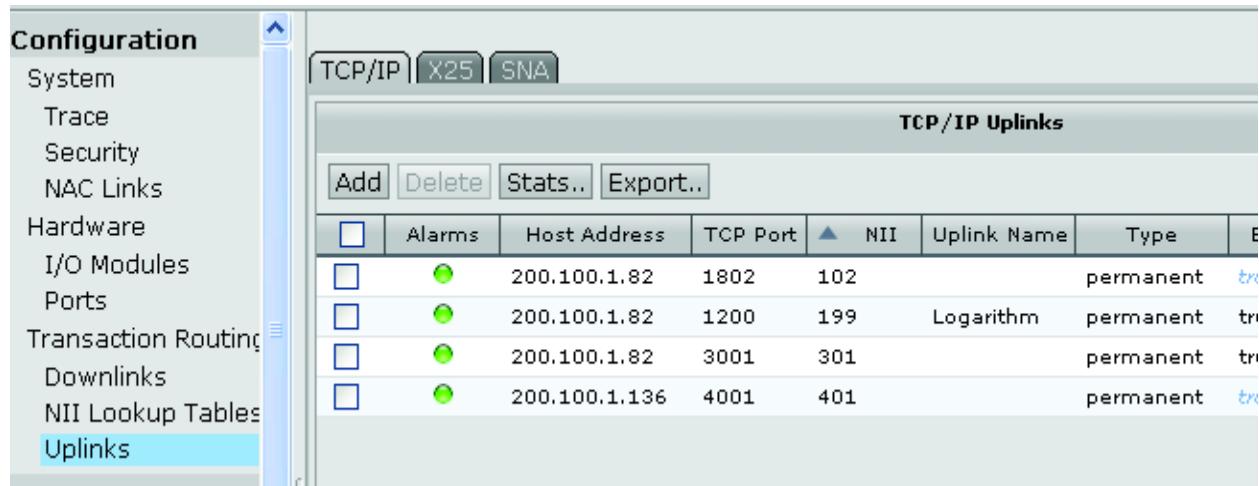


FIGURE 110. Node Configuration (Uplinks)

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	HOST2
TCP Port:	1401
NII:	1500
Uplink Name:	Host1 Failover
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 111. Node 0208 Host2 TCP/IP Uplink Fail over Configuration screens

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (a value of exact 1000 more for fail over NII is required for fail over configurations. If Primary NII was 600 then the failover NII will be 1600)
10. Enter any other configuration settings
11. Click **OK**

Configure node name 0209 TCP/IP Host Uplinks

Configure Primary host uplink

1. Select the 0209 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

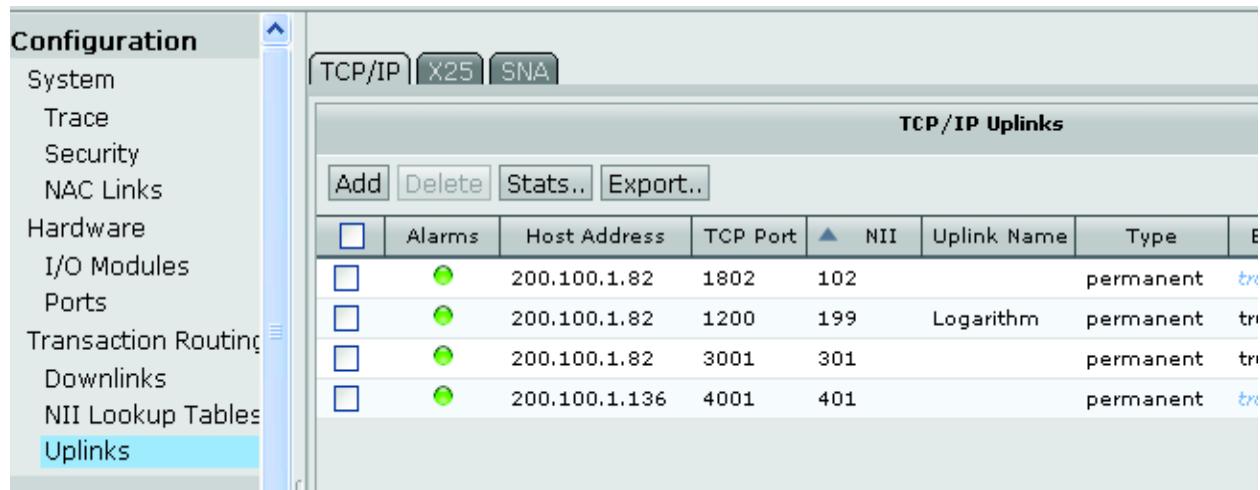


FIGURE 112. Node Configuration (Uplinks)

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	Host 1
TCP Port:	1400
NII:	500
Uplink Name:	Host1 Pri-uplink
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 113. Node 0209 Host1 TCP/IP Uplink Primary Configuration screens

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (value must match Host1 NII in node 0210)
10. Enter any other configuration settings
11. Click **OK**

Now on node 0209 configure fail over host uplink

1. Select the 0209 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

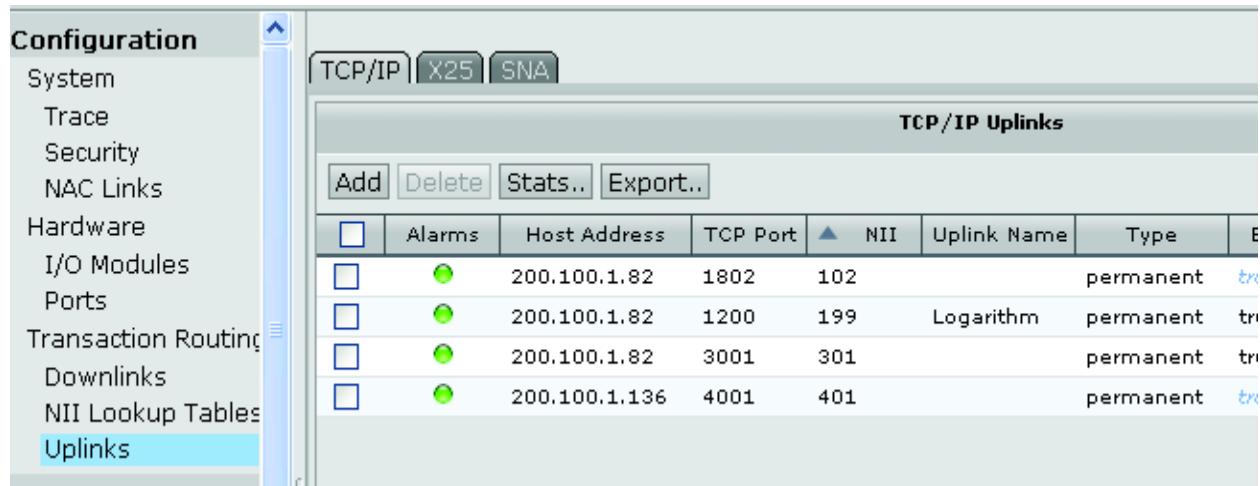


FIGURE 114. Node Configuration (Uplinks)

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	Host 2
TCP Port:	1401
NII:	1500
Uplink Name:	Host2 Alt-uplink
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 115. Node 0209 Host2 TCP/IP Uplink Fail over Configuration screens

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (value must match Host 2 fail over NII)
10. Enter any other configuration settings
11. Click **OK**

Configure node name 0207 TCP/IP Host Uplinks

Configure Primary host uplink

1. Select the 0207 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

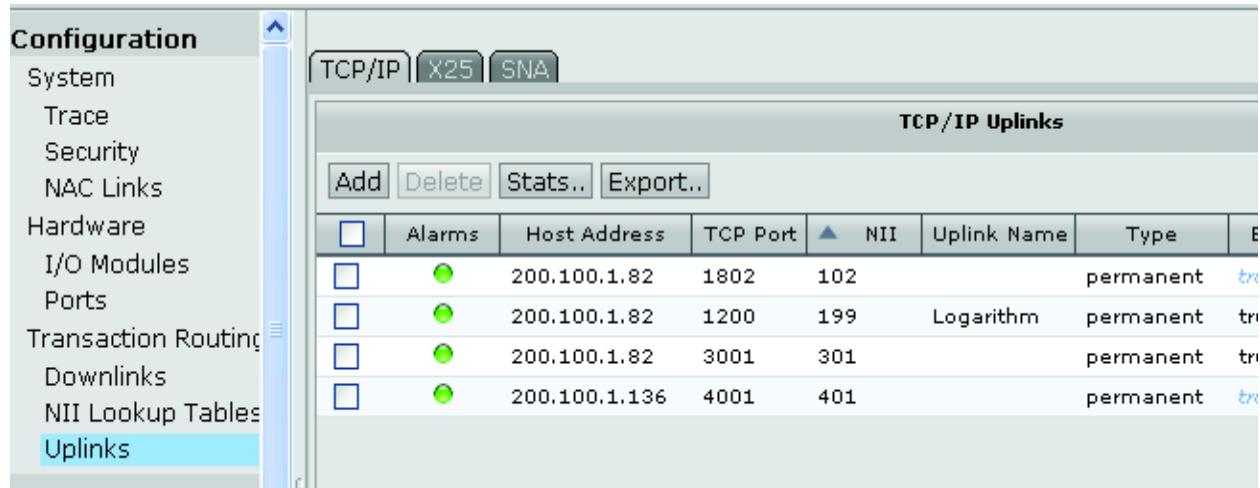


FIGURE 116. Node Configuration (Uplinks)

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	Host 2
TCP Port:	1400
NII:	600
Uplink Name:	Host2 Pri uplink
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 117. Node 0207 Host2 TCP/IP Uplink Primary Configuration screens

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (value must match Host2 NII in node 0208)
10. Enter any other configuration settings
11. Click **OK**

Now on node 0207 configure fail over host uplink

1. Select the 0207 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

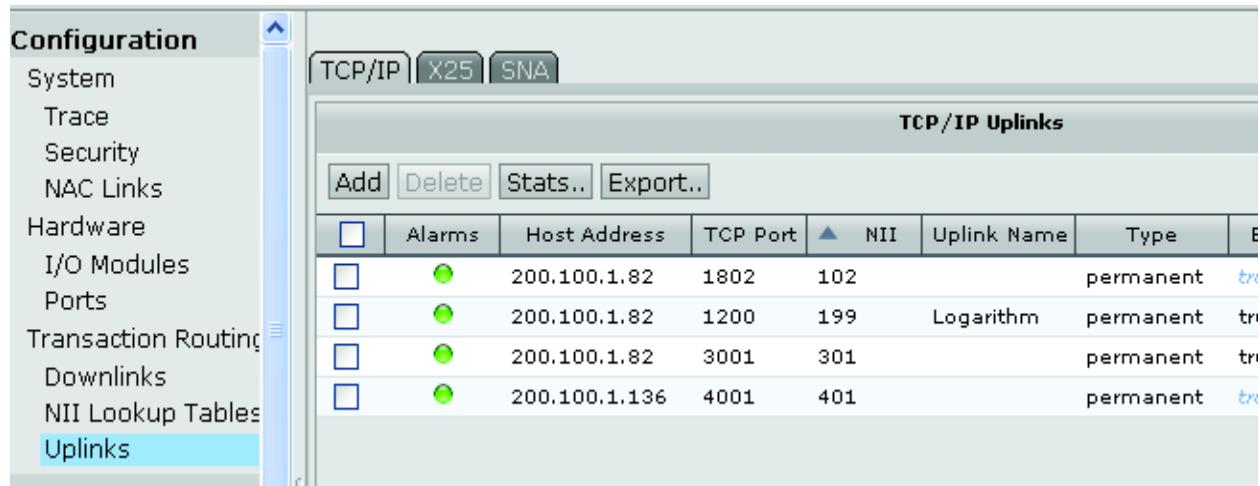


FIGURE 118. Node Configuration (Uplinks)

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	Host 1
TCP Port:	1401
NII:	1600
Uplink Name:	Host1 Alt-uplink
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 119. Node 0207 Host1 TCP/IP Uplink Fail over Configuration screens

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (value must match Host 1 fail over NII)
10. Enter any other configuration settings
11. Click **OK**

The NAC to NAC links and routing are complete for this fail over configuration.

For Nodes 0207 and 0209 any downlinks will have to have the NII tables built for proper routing IE. the downlinks on node 0207 use NII 600 for Host2 and downlinks on node 0209 use NII 500 for Host1. The fail over is handled automatically by use of the NII primary and plus 1000 NII for the alternate.

Note: The transactions will use the Alternate only if the Primary NII is not responsive. Every transaction tries the Primary first. This is the same for all downlink types.

Load Balance

Configure node name 0210 TCP/IP Uplinks

Configure Primary host

1. Select the 0210 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

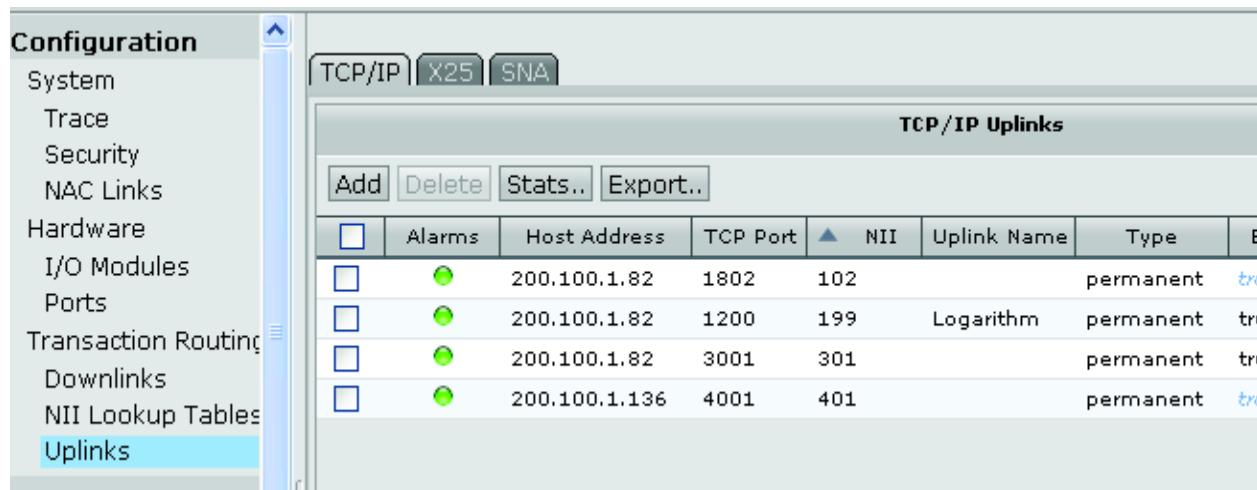


FIGURE 120. Node Configuration (Uplinks)

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	Host1
TCP Port:	1400
NII:	500
Uplink Name:	0209 host bal-conn
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 121. Node 0210 Host1 TCP/IP Uplink load Balance for node 0209

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (must be the same value as node 0208 Host2, port 1401)
10. Enter any other configuration settings
11. Click **OK**

Now on node 0210 configure cross over load balance host

1. Select the 0210 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

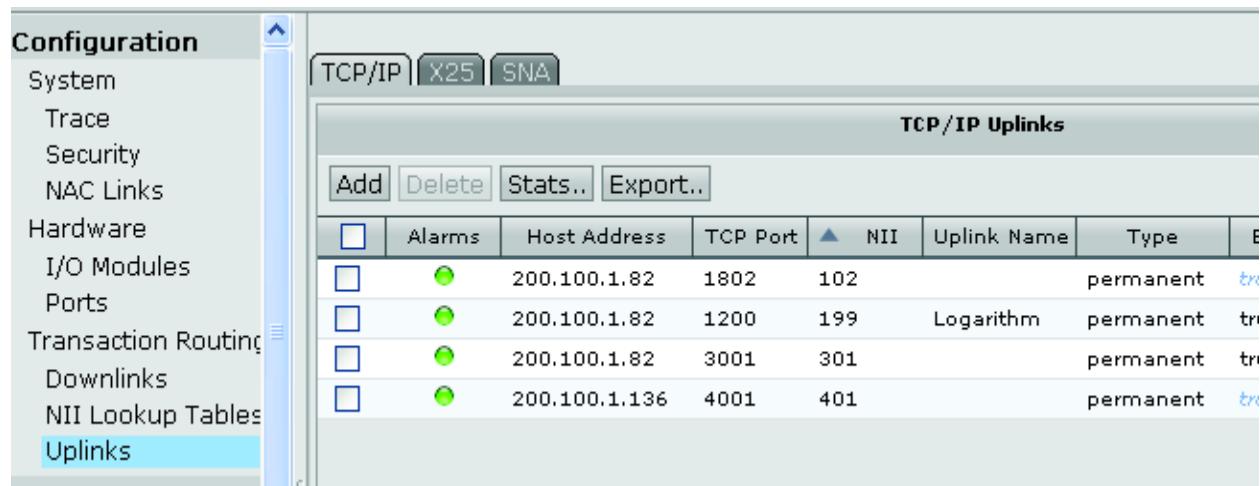


FIGURE 122. Node Configuration (Uplinks)

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	Host1
TCP Port:	1401
NII:	600
Uplink Name:	0207 host bal-conn
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 123. Node 0210 Host1 TCP/IP Uplink load Balance for node 0207

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (must be the same value as node 0208 Host2, port 1400)
10. Enter any other configuration settings
11. Click **OK**

Configure node name 0208 TCP/IP Uplinks

Configure Primary host

1. Select the 0208 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

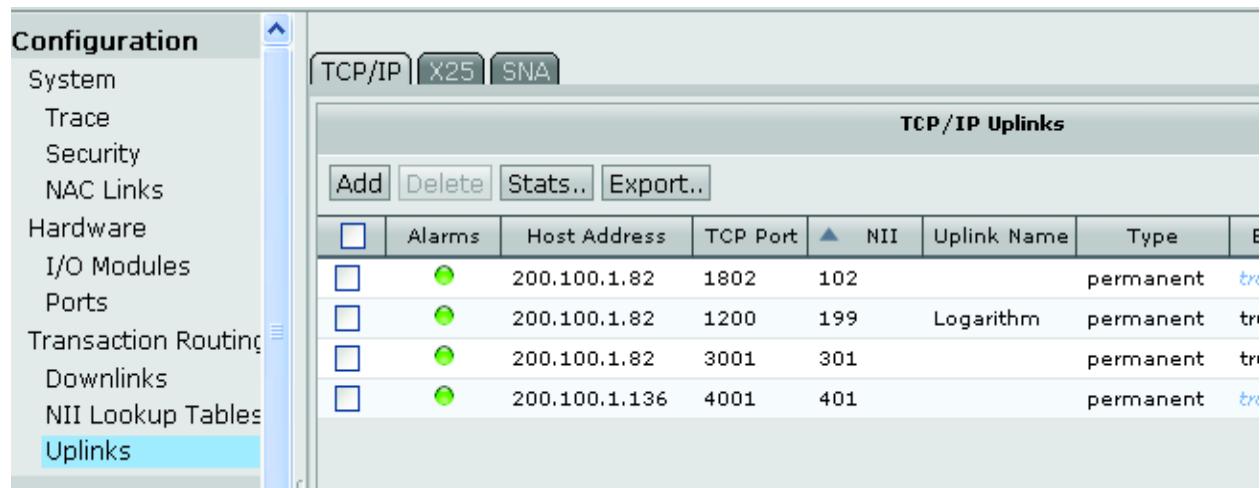


FIGURE 124. Node Configuration (Uplinks)

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	Host2
TCP Port:	1400
NII:	600
Uplink Name:	0207 host bal-conn
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 125. Node 0208 Host2 TCP/IP Uplink load Balance for node 0207

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (must be the same value as node 0210 Host2, port 1401)
10. Enter any other configuration settings
11. Click **OK**

Now on node 0208 configure cross over load balance host

1. Select the 0208 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

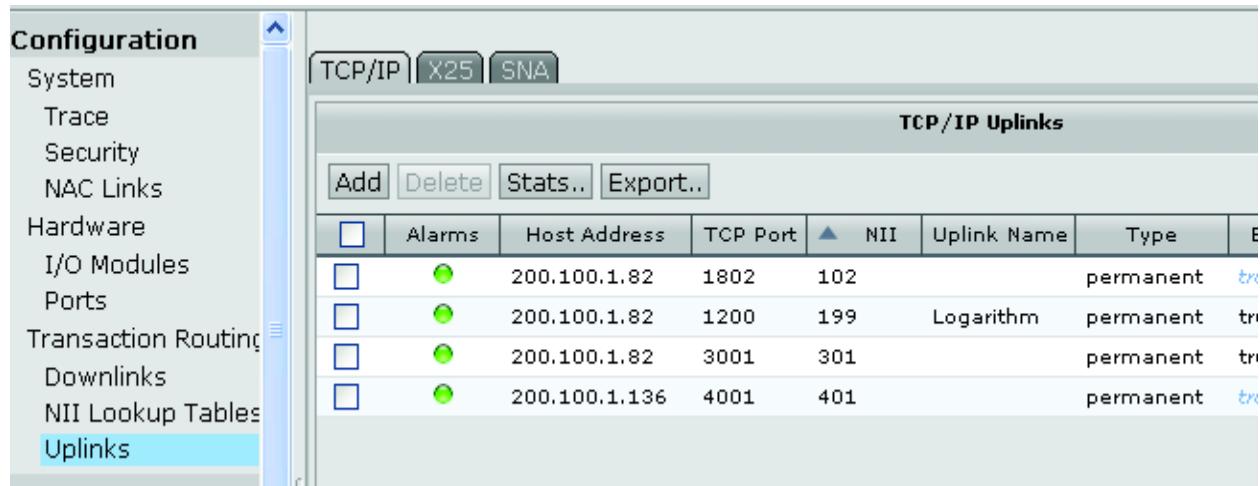


FIGURE 126. Node Configuration (Uplinks)

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	Host2
TCP Port:	1401
NII:	500
Uplink Name:	0209 host bal-conn
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 127. Node 0208 Host2 TCP/IP Uplink load Balance for node 0209

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (must be the same value as node 0210 Host1, port 1400)
10. Enter any other configuration settings
11. Click **OK**

Configure node name 0209 TCP/IP Host Uplinks

Configure Primary host uplink

1. Select the 0209 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

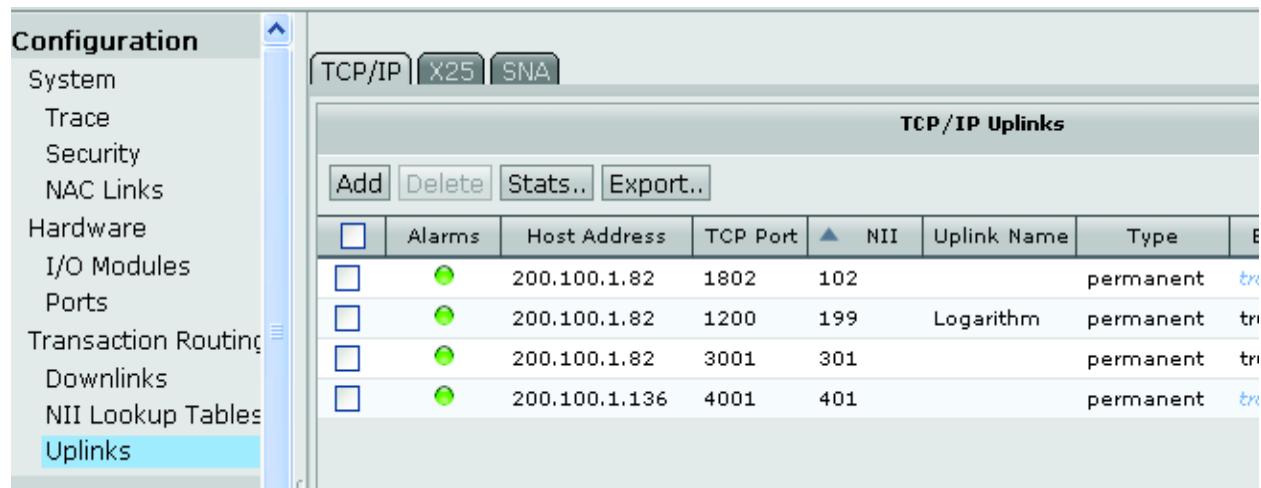


FIGURE 128. Node Configuration (Uplinks)

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	Host1
TCP Port:	1400
NII:	500
Uplink Name:	0209 host bal-conn
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 129. Node 0209 Host1 TCP/IP Uplink load Balance for node 0209

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (value must match Host1 NII in node 0210)
10. Enter any other configuration settings
11. Click **OK**

Now on node 0209 configure Load balance host uplink

1. Select the 0209 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

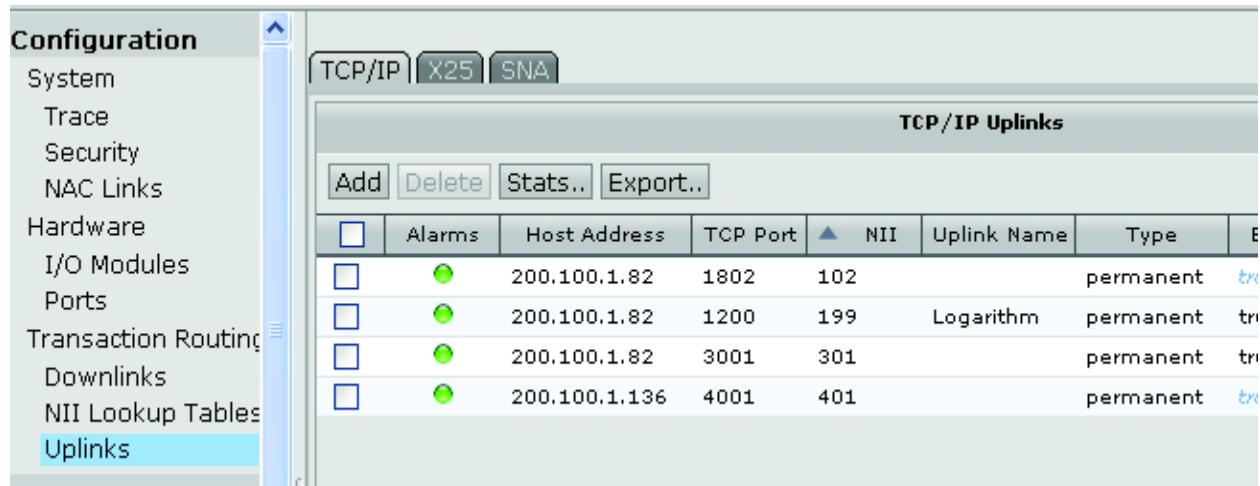


FIGURE 130. Node Configuration (Uplinks)

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	Host2
TCP Port:	1401
NII:	500
Uplink Name:	0209 host bal-conn
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 131. Node 0209 Host2 TCP/IP Uplink load Balance for node 0209

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (value must match Host 2 fail over NII)
10. Enter any other configuration settings
11. Click **OK**

Configure node name 0207 TCP/IP Host Uplinks

Configure Primary host uplink

1. Select the 0207 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

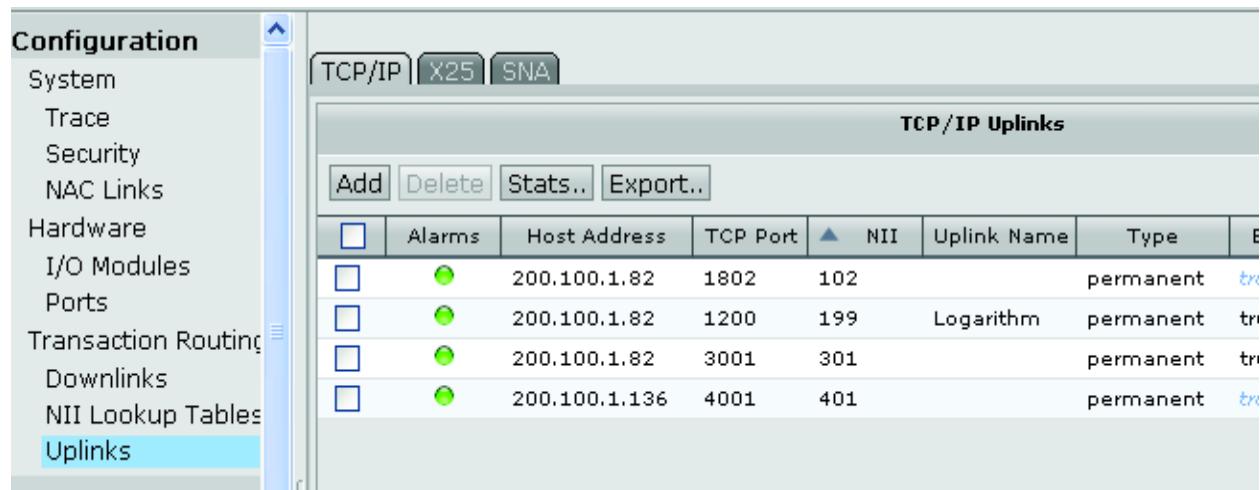


FIGURE 132. Node Configuration (Uplinks)

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	Host 2
TCP Port:	1400
NII:	600
Uplink Name:	Host2 Pri uplink
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 133. Node 0207 Host2 TCP/IP Uplink load Balance for node 0207

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (value must match Host2 NII in node 0208)
10. Enter any other configuration settings
11. Click **OK**

Now on node 0207 configure fail over host uplink

1. Select the 0207 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

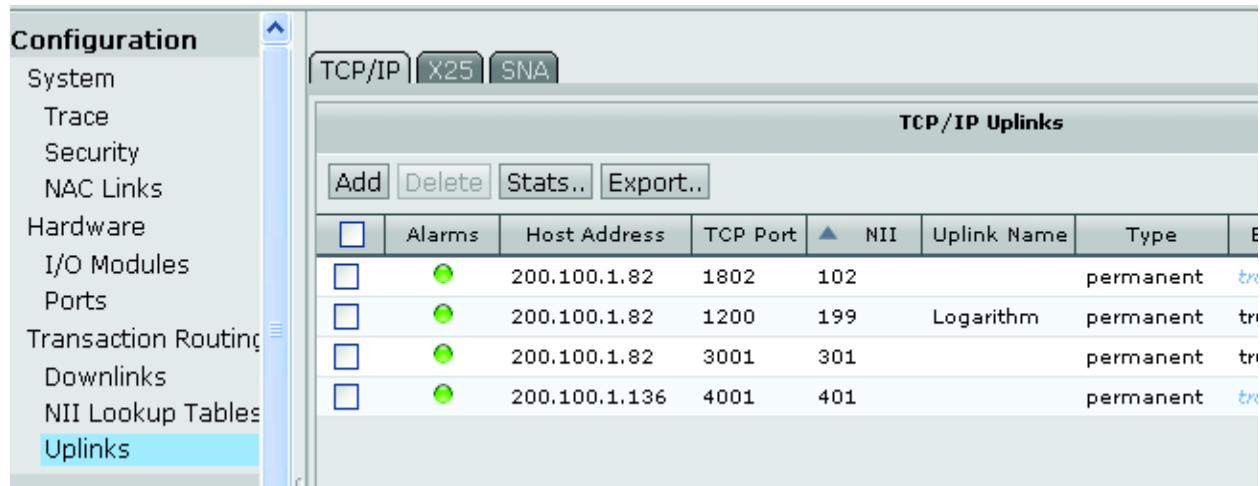


FIGURE 134. Node Configuration (Uplinks)

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	Host1
TCP Port:	1401
NII:	600
Uplink Name:	0207 host bal-conn
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 135. Node 0207 Host1 TCP/IP Uplink load Balance for node 0207

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (value must match Host 1 fail over NII)
10. Enter any other configuration settings
11. Click **OK**

The NAC to NAC links and routing are complete for this load balance configuration.

For Nodes 0207 and 0209 any downlinks will have to have the NII tables built for proper routing IE. the downlinks on node 0207 use NII 600 for Host2 and downlinks on node 0209 use NII 500 for Host1. The load balance is handled automatically by round robin or ping pong operation

NAC to NAC with In-Band Management Configuration

The administrator is able to configure the network hierarchy by using intermediate INAC devices as concentrator. See use case example below: (NAC to NAC with in-band management redundancy and transaction load balancing)

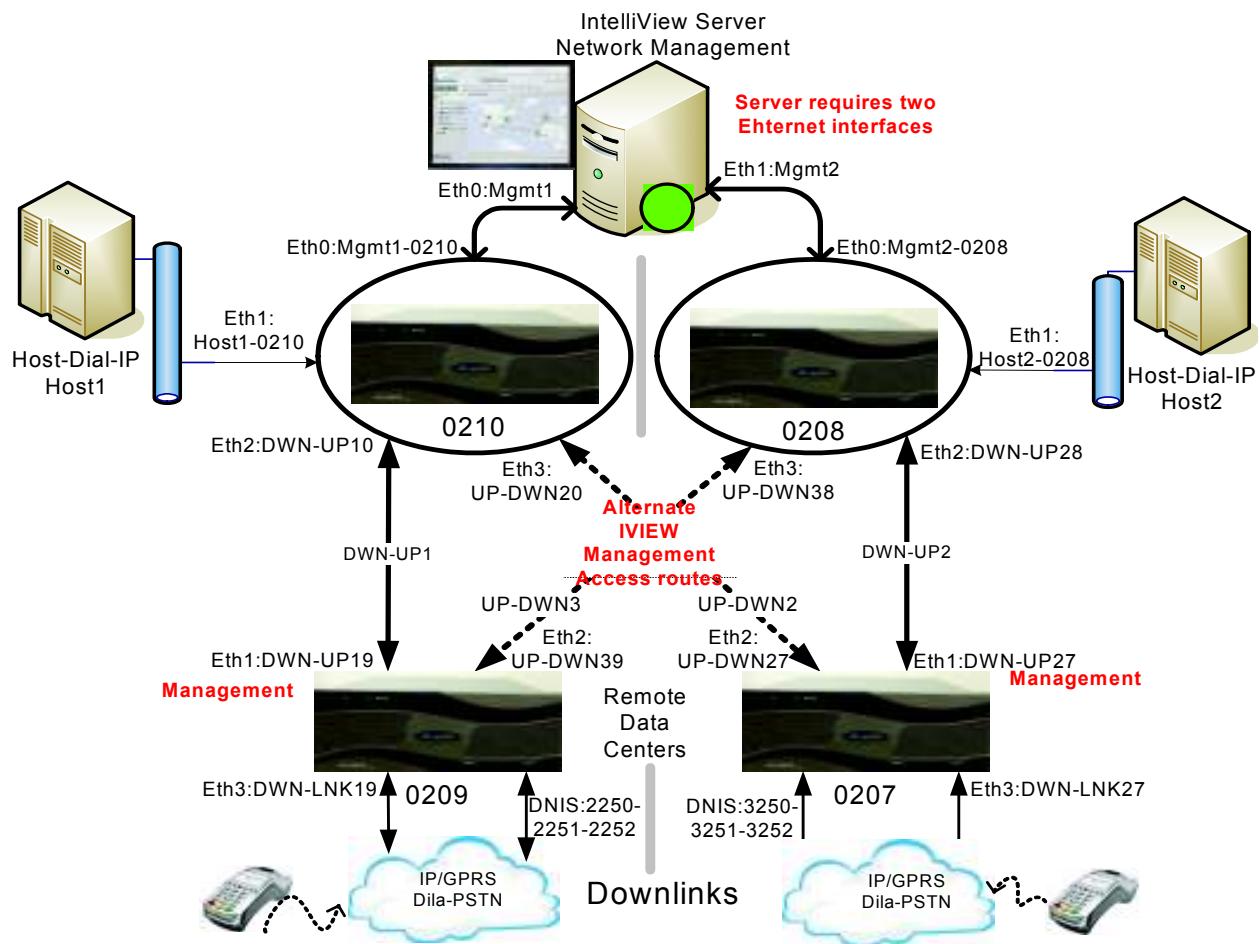


FIGURE 136. NAC to NAC link with in band management configuration

Device configuration (INAC Deployment)

All INAC's must be deployed (installed) with unique Node ID's and Management port IP address (0207, 0208, 0209, 0210, Eth1:DWN-UP27 (Node 0207), ETH0:Mgmt2-0208 (Node 0208), Eth1:DWN-UP19 (Node 0209), Eth0:Mgmt1-0210 (Node 0210)). For this particular configuration the management port is configured on ETH0 (port 1) on all upper level (does not have to be).

Create four Nodes with names of 0207 through 0210, with Node ID's of 1007 through 1010

See IntelliNAC Installation Guide for the installation of the INAC's

Note - During the INAC installation process Port 1 = Eht1, Port 2 = Eth2, Port 3 = Eth3, Port 4 = Eth4.

For Remote node 0207 deploy values are:

Node ID = 1007

Port for IntelliVIEW management = 2

Management port IP Address = Eth1:DWN-UP27

Netmask = 255.255.255.0

Add static route = Yes

Destination IP address = Eth1:Mgmt2

Netmask = 255.255.255.255

GW IP address = Eth2:DWN-UP28

For Remote node 0209 deploy values are:

Node ID = 1009

Port for IntelliVIEW management = 2

Management port IP Address = Eth1:DWN-UP19

Netmask = 255.255.255.0

Add static route = Yes

Destination IP address = Eth0:Mgmt1

Netmask = 255.255.255.255

GW IP address = Eth2:DWN-UP10

For Remote node 0208 deploy values are:

Node ID = 1008

Port for IntelliVIEW management = 1

Management port IP Address = Eth0:Mgmt2-0208

Netmask = 255.255.255.0

Add static route = No

For Remote node 0210 deploy values are:

Node ID = 1010

Port for IntelliVIEW management = 1

Management port IP Address = Eth0:Mgmt1-0210

Configuration

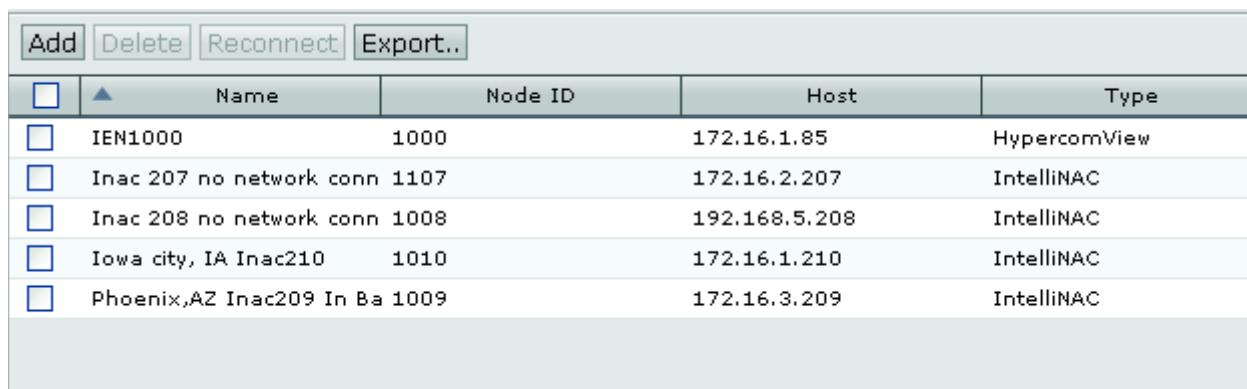
Netmask = 255.255.255.0

Add static route = No

Configure the Devices (Node)

Manage (Create) Devices

1. Right Click on “Map View”
2. Click **Devices** on the toolbar. From pull down menu select **Manage**



The screenshot shows a software interface titled "Device Manager". At the top, there is a toolbar with four buttons: "Add", "Delete", "Reconnect", and "Export..". Below the toolbar is a table with five columns: "Name", "Node ID", "Host", and "Type". The table contains five rows of data:

	Name	Node ID	Host	Type
<input type="checkbox"/>	IEN1000	1000	172.16.1.85	HypercomView
<input type="checkbox"/>	Inac 207 no network conn	1107	172.16.2.207	IntelliNAC
<input type="checkbox"/>	Inac 208 no network conn	1008	192.168.5.208	IntelliNAC
<input type="checkbox"/>	Iowa city, IA Inac210	1010	172.16.1.210	IntelliNAC
<input type="checkbox"/>	Phoenix,AZ Inac209 In Ba	1009	172.16.3.209	IntelliNAC

FIGURE 137. Device Manage screen

3. Click **Add**, The Managed Element screen appears

Managed Element

Type:	IntelliNAC i6
Version:	2013.3.26
Name:	<input type="text"/>
IP/DNS Address:	<input type="text"/>
Description:	<input type="text"/>
<input type="checkbox"/> Maintenance	

Details

Node ID:	<input type="text"/>
SSH Port:	830
SSH User Name:	admin
SSH Password:	<input type="text"/>
Private Key:	<input type="text"/>
Encryption PassPhrase:	<input type="text"/>
Warning:	Enable In-Band management in device config->system
Gateway:	<input type="text"/>
Alternate Gateway:	<input type="text"/>

Trace Collection

<input checked="" type="checkbox"/> Collecting Traces	
Interval (minutes):	15

FIGURE 138. Device Configuration screen

4. For Node 0207 the follow information is used, Then click **OK** when complete

Name - 0207

Configuration

IP address - Eth2:DWN-UP27

Description - Remote node 207

Node ID - 1007

Remote IntelliVIEW Access - Eth0:Mgmt2-0208

Alternate Remote IntelliVIEW Access - Eth0:Mgmt1-0210

5. Repeat for Node 0209 the follow information is used, Then click **OK** when complete

Name - 0209

IP address - Eth2:DWN-UP19

Description - Remote node 209

Node ID - 1009

Remote IntelliVIEW Access - Eth0:Mgmt1-0210

Alternate Remote IntelliVIEW Access - Eth0:Mgmt2-0208

6. Repeat for Node 0210 the follow information is used, Then click **OK** when complete

Name - 0210

IP address - Eth0:Mgmt1-0210

Description - Remote node 210

Node ID - 1010

Remote IntelliVIEW Access - BLANK

Alternate Remote IntelliVIEW Access - BLANK

7. Repeat for Node 0208 the follow information is used, Then click **OK** when complete

Name - 0208

IP address - Eth0:Mgmt2-0208

Description - Remote node 208

Node ID - 1008

Remote IntelliVIEW Access - BLANK

Alternate Remote IntelliVIEW Access - BLANK

Configuring Nodes for In-Band Management

The four node created will be located in the left side bar under **Unplaced**



FIGURE 139. Device unplaced side bar

1. Select the device and either right click and select **Config App** or click **Config App** from the tool bar.
2. Select **System** under the **Configuration** in the right side menu bar.

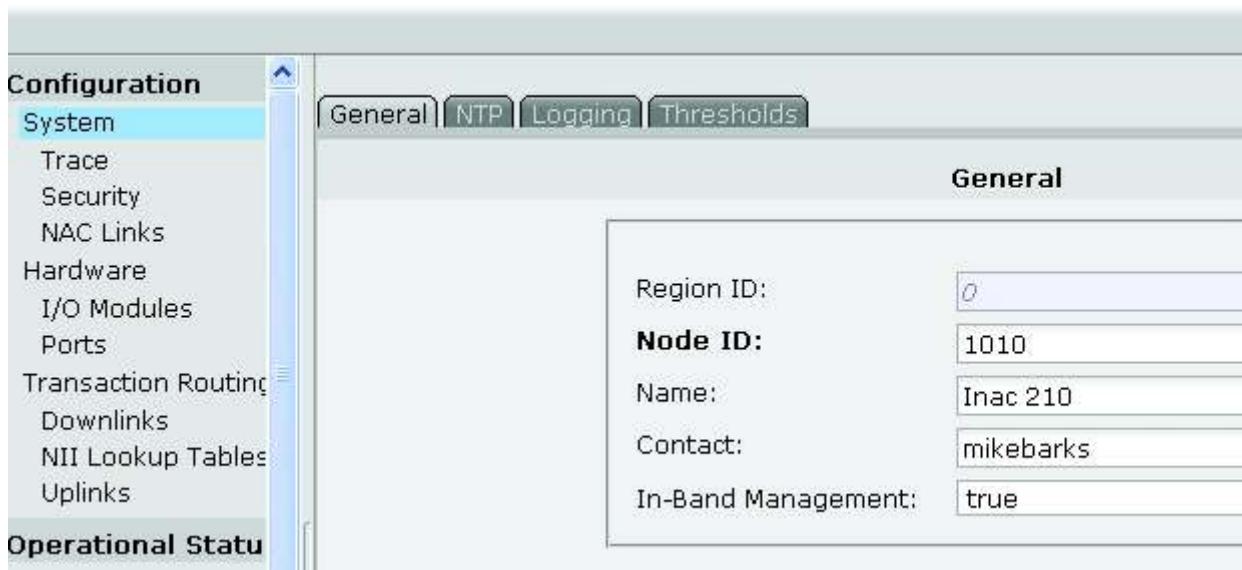


FIGURE 140. Device System Configuration screen

3. For Nodes 0208 and 0210 set the **In-Band Management** field to **True**.
4. For Nodes 0209 and 0207 set the **In-Band Management** field to **False**.

Ethernet Port configuration for NAC to NAC link and In-Band Management configuration

1. Select the device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Ports** under Configuration > Hardware.
3. In the configure screen click on **Ethernet** tab
4. The Ethernet screen appears.



FIGURE 141. Port Configuration screen

5. Click on Add to configure that nodes Ethernet Ports
6. Repeat on each node in the NAC to NAC configuration

Configuration

Node 0210 Ethernet port configuration

210 ETH0 port configuration

Ethernet Port

Port ID:	1
Name:	Management1
IP Address:	Eth0:Mgmt1-0210
Network Mask:	255.255.255.0
Warning:	This is management port!
Admin State:	up
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 150px; margin-top: 10px;"><div style="border-bottom: 1px solid #ccc; height: 10px;"></div><div style="display: flex; justify-content: space-between; align-items: center; margin-top: 5px;">+-</div><div style="display: flex; justify-content: space-around; margin-top: 10px;"><></div></div>
Dedicated Downlink:	<i>Default: false</i>

FIGURE 142. Ethernet Port 1 Configuration screen - node 0210

210 ETH1 port configuration

Ethernet Port

Port ID:	2
Name:	Host1 0210
IP Address:	Eth1:Host1-0210
Network Mask:	255.255.255.0
Admin State:	up
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; height: 150px; width: 100%;"></div> <div style="text-align: right; margin-top: -10px;">+</div> <div style="text-align: right; margin-top: -10px;">-</div>
Dedicated Downlink:	<i>Default: false</i>

FIGURE 143. Ethernet Port 2 Configuration screen - node 0210

210 ETH2 port configuration

210 ETH3 port configuration

Ethernet Port

Port ID:	3
Name:	DWN-UP1
IP Address:	Eth2:DWN-UP10
Network Mask:	255.255.255.0
Admin State:	up
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; height: 200px; width: 100%;"></div> <div style="display: flex; justify-content: space-around; margin-top: 5px;">+-</div>
Dedicated Downlink:	<i>Default: false</i>

FIGURE 144. Ethernet Port 3 Configuration screen - node 0210

Ethernet Port

Port ID:	4
Name:	UP-DWN2
IP Address:	Eth3:UP-DWN20
Network Mask:	255.255.255.0
Admin State:	up <input type="button" value="▼"/>
Static Routes:	Eth1:DWN-UP27 255.255.255.255 Eht2:UP-DWN27 <input style="float: right; margin-right: 10px;" type="button" value="+"/> <input style="float: right; margin-right: 10px;" type="button" value="-"/>
Dedicated Downlink:	<i>Default: false</i> <input type="button" value="▼"/>

FIGURE 145. Ethernet Port 4 Configuration screen - node 0210

Add a static route for the alternate management path to node 0207

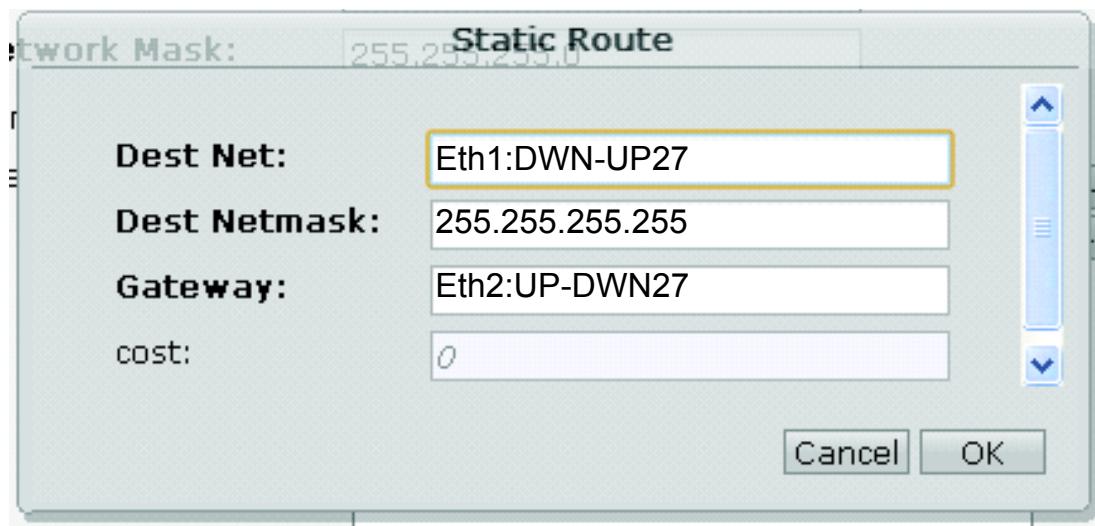


FIGURE 146. Ethernet Port 4 Static Route Configuration - node 0210

Configuration

Node 0208 Ethernet port configuration

208 ETH0 port configuration

Ethernet Port

Port ID:	1
Name:	Management2
IP Address:	Eth0:Mgmt2-0208
Network Mask:	255.255.255.0
Warning:	This is management port!
Admin State:	up
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 150px; margin-top: 10px;"><div style="border-bottom: 1px solid #ccc; height: 10px;"></div><div style="display: flex; justify-content: space-between; align-items: center; margin-top: 5px;">+-</div><div style="display: flex; justify-content: space-around; margin-top: 10px;"><></div></div>
Dedicated Downlink:	<i>Default: false</i>

FIGURE 147. Ethernet Port 1 Configuration screen - node 0208

208 ETH2 port configuration

Ethernet Port

Port ID:	2
Name:	Host2 0208
IP Address:	Eth1:Host2-0208
Network Mask:	255.255.255.0
Admin State:	up 
Static Routes:	<div style="border: 1px solid #ccc; padding: 10px; min-height: 200px; margin-bottom: 10px;"></div> <div style="display: flex; align-items: center; justify-content: flex-end;"> </div>
Dedicated Downlink:	<i>Default: false</i> 

FIGURE 148. Ethernet Port 2 Configuration screen - node 0208

208 ETH3 port configuration

Ethernet Port

Port ID:	3
Name:	DWN-UP2
IP Address:	Eth2:DWN-UP28
Network Mask:	255.255.255.0
Admin State:	up <input type="button" value="▼"/>
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 150px; margin-bottom: 10px;"></div> <div style="display: flex; align-items: center; justify-content: flex-end;"><input style="margin-right: 10px;" type="button" value="+"/><input type="button" value="-"/></div>
Dedicated Downlink:	<i>Default: false</i> <input type="button" value="▼"/>

FIGURE 149. Ethernet Port 3 Configuration screen - node 0208

208 ETH4 port configuration

Ethernet Port

Port ID:	4
Name:	UP-DWN3
IP Address:	Eth3:UP-DWN38
Network Mask:	255.255.255.0
Admin State:	up <input type="button" value="▼"/>
Static Routes:	Eth2:DWN-UP19 255.255.255.255 Eht3:UP-DWN39 <input style="float: right; margin-right: 10px;" type="button" value="+"/> <input style="float: right; margin-right: 10px;" type="button" value="-"/>
Dedicated Downlink:	<i>Default: false</i> <input type="button" value="▼"/>

FIGURE 150. Ethernet Port 4 Configuration screen - node 0208

Add a static route for the alternate management path to Node 0209

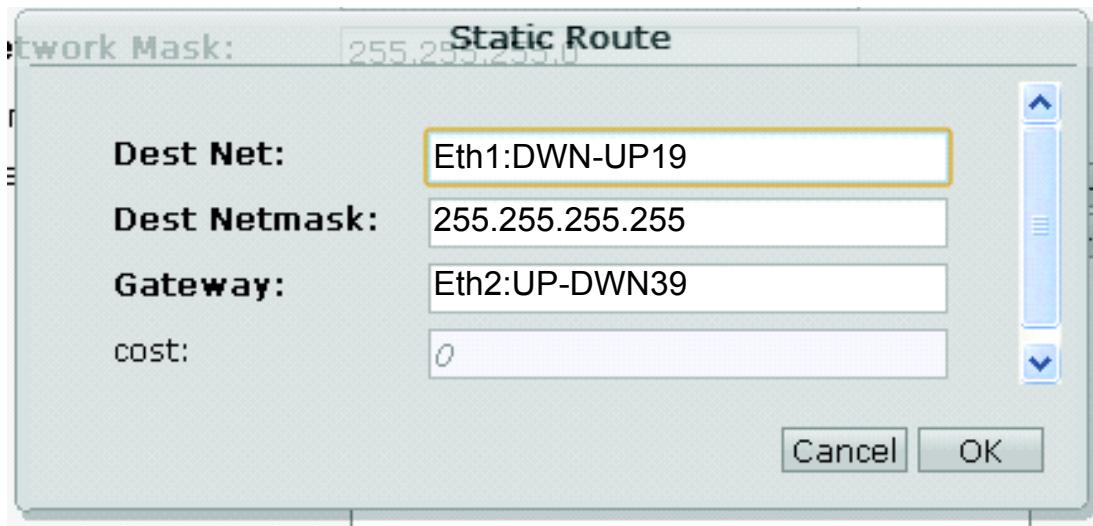


FIGURE 151. Ethernet Port 4 Static Route Configuration - node 0208

Node 0209 Ethernet port configuration

209 ETH1 port configuration

Ethernet Port

Port ID:	2
Name:	Management1
IP Address:	Eth1:DWN-UP19
Network Mask:	255.255.255.0
Warning:	This is management port!
Admin State:	up
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 200px; margin-top: 10px;"><div style="border-bottom: 1px solid #ccc; height: 15px;"></div><div style="text-align: right; margin-top: -5px;">+</div><div style="text-align: right; margin-top: 5px;">-</div></div>
Dedicated Downlink:	<i>Default: false</i>

FIGURE 152. Ethernet Port 2 Configuration screen - node 0209

Configuration

209 ETH2 port configuration

Ethernet Port

Port ID:	3
Name:	UP-DWN3
IP Address:	Eth2:UP-DWN39
Network Mask:	255.255.255.0
Admin State:	up <input type="button" value="▼"/>
Static Routes:	Eth1:Mgmt2 255.255.255.255 Eht3:UP-DWN38 <input style="float: right; margin-right: 10px;" type="button" value="+"/> <input style="float: right; margin-right: 10px;" type="button" value="-"/>
Dedicated Downlink:	<i>Default: false</i> <input type="button" value="▼"/>

FIGURE 153. Ethernet Port 3 Configuration screen - node 0209

Add a static route for the alternate management path from node 0209

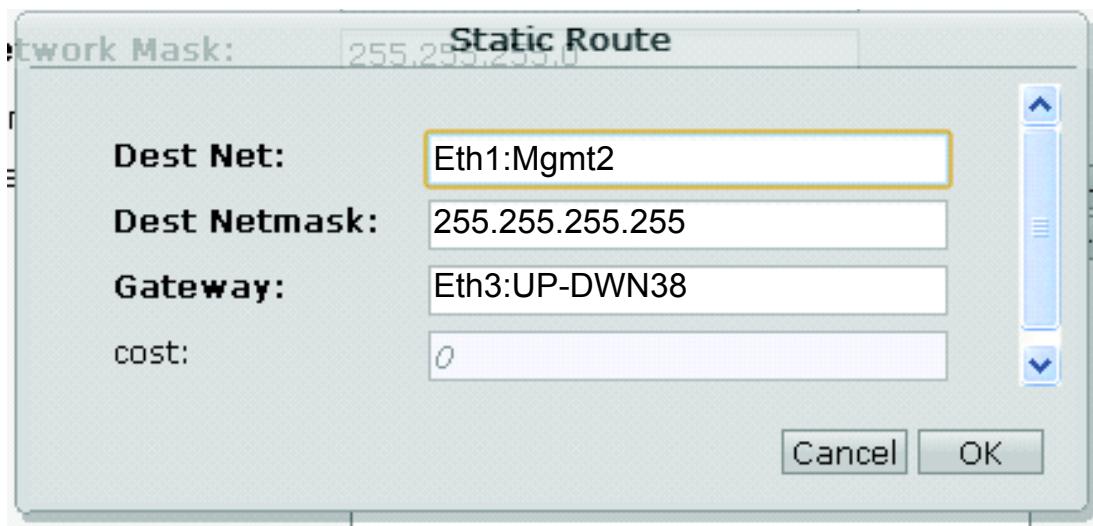


FIGURE 154. Ethernet Port 3 Static Route Configuration - node 0209

209 ETH3 port configuration

Ethernet Port

Port ID:	4
Name:	DWN-LNK1
IP Address:	Eth3:DWN-LNK19
Network Mask:	255.255.255.0
Admin State:	up 
Static Routes:	<div style="border: 1px solid #ccc; padding: 10px; min-height: 200px;"></div> <div style="text-align: right; margin-top: -10px;"> </div>
Dedicated Downlink:	<i>Default: false</i> 

FIGURE 155. Ethernet Port 4 Configuration screen - node 0209

Node 0207 Ethernet port configuration

207 ETH1 port configuration

Ethernet Port

Port ID:	2
Name:	Management2
IP Address:	Eth1:DWN-UP27
Network Mask:	255.255.255.0
Warning:	This is management port!
Admin State:	up
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; height: 200px; width: 100%;"><p style="margin: 0;">+ -</p><p style="margin: 0; text-align: center;">< ></p></div>
Dedicated Downlink:	<i>Default: false</i>

FIGURE 156. Ethernet Port 2 Configuration screen - node 0207

Configuration

207 ETH2 port configuration

Ethernet Port

Port ID:	3
Name:	UP-DWN2
IP Address:	Eth2:UP-DWN27
Network Mask:	255.255.255.0
Admin State:	up <input type="button" value="▼"/>
Static Routes:	Eth0:Mgmt1 (255.255.255.255) Eth3:UP-DWN20 <input style="float: right; margin-right: 10px;" type="button" value="+"/> <input style="float: right; margin-right: 10px;" type="button" value="-"/>
Dedicated Downlink:	<i>Default: false</i> <input type="button" value="▼"/>

FIGURE 157. Ethernet Port 3 Configuration screen - node 0207

Add a static route for the alternate management path from node 0207

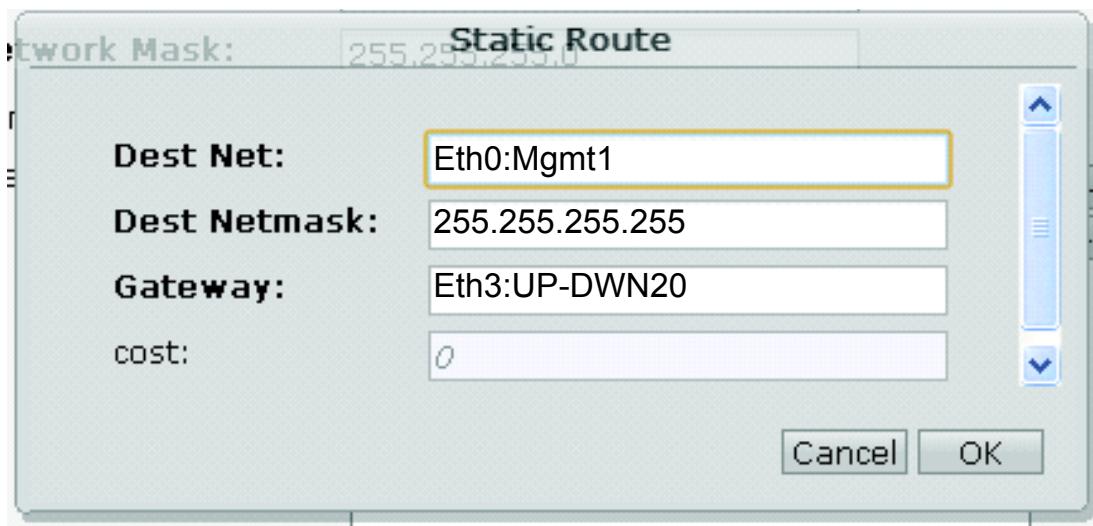


FIGURE 158. Ethernet Port 3 Static Route Configuration - node 0207

Configuration

207 ETH3 port configuration

Ethernet Port

Port ID:	4
Name:	DWN-LNK2
IP Address:	Eth3:DWN-LNK27
Network Mask:	255.255.255.0
Admin State:	up <input type="button" value="▼"/>
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 150px; margin-bottom: 10px;"></div> <div style="display: flex; align-items: center; justify-content: flex-end;"><input style="margin-right: 10px;" type="button" value="+"/><input type="button" value="-"/></div>
Dedicated Downlink:	<i>Default: false</i> <input type="button" value="▼"/>

FIGURE 159. Ethernet Port 4 Configuration screen - node 0207

IntelliVIEW device NAC to NAC link configuration

1. Select the device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **NAC Links** under Configuration > System.



FIGURE 160. NAC Links Configuration screen

3. In the configure screen click on **Links** tab
4. The NAC links screen appears.

NAC Links								
	Add	Delete	Export..	Alarms	LinkName	Enable	Local Address	Local Gateway
				●	210 to 207	true	172.16.2.210	172.16.2.210
				●	210 to 209	true	172.16.3.210	172.16.3.210

FIGURE 161. NAC Links status screen

5. Click on Add to configure that nodes NAC to NAC link
6. Repeat on each node in the NAC top NAC configuration

Configuration

Node 0210 configuration

NAC Link

Link Name:	DWN-UP1
Enable:	True
Local Address:	Eth2:DWN-UP10
Local Gateway:	Eth2:DWN-UP10
Remote Address:	Eth1:DWN-UP19
Remote Gateway:	Eth1:DWN-UP19
priority:	<i>Default: false</i>

NAC Link

Link Name:	UP-DWN2
Enable:	True
Local Address:	Eth3:UP-DWN20
Local Gateway:	Eth3:UP-DWN20
Remote Address:	Eth2:UP-DWN27
Remote Gateway:	Eth2:UP-DWN27
priority:	<i>Default: false</i>

FIGURE 162. NAC to NAC links configuration screens - node 0210

Node 0208 Configuration

NAC Link

Link Name:	DWN-UP2
Enable:	True
Local Address:	Eth2:DWN-UP28
Local Gateway:	Eth2:DWN-UP28
Remote Address:	Eth1:DWN-UP27
Remote Gateway:	Eth1:DWN-UP27
priority:	<i>Default: false</i>

NAC Link

Link Name:	UP-DWN3
Enable:	True
Local Address:	Eth3:UP-DWN38
Local Gateway:	Eth3:UP-DWN38
Remote Address:	Eth2:UP-DWN39
Remote Gateway:	Eth2:UP-DWN39
priority:	<i>Default: false</i>

FIGURE 163. NAC to NAC links configuration screens - node 0208

Configuration

Node 0209 Configuration

NAC Link	
Link Name:	DWN-UP1
Enable:	True
Local Address:	Eth1:DWN-UP19
Local Gateway:	Eth1:DWN-UP19
Remote Address:	Eth2:DWN-UP10
Remote Gateway:	Eth2:DWN-UP10
priority:	<i>Default: false</i>

NAC Link	
Link Name:	UP-DWN3
Enable:	True
Local Address:	Eth2:UP-DWN39
Local Gateway:	Eth2:UP-DWN39
Remote Address:	Eth3:UP-DWN38
Remote Gateway:	Eth3:UP-DWN38
priority:	<i>Default: false</i>

FIGURE 164. NAC to NAC links configuration screens - node 0209

Node 207 Configuration

NAC Link	
Link Name:	DWN-UP2
Enable:	True
Local Address:	Eth1:DWN-UP27
Local Gateway:	Eth1:DWN-UP27
Remote Address:	Eth2:DWN-UP28
Remote Gateway:	Eth2:DWN-UP28
priority:	<i>Default: false</i>

NAC Link	
Link Name:	UP-DWN2
Enable:	True
Local Address:	Eth2:UP-DWN27
Local Gateway:	Eth2:UP-DWN27
Remote Address:	Eth3:UP-DWN20
Remote Gateway:	Eth3:UP-DWN20
priority:	<i>Default: false</i>

FIGURE 165. NAC to NAC links configuration screens - node 0207

Configure the NII's for load balance

Load Balance

Configure node name 0210 TCP/IP Uplinks

Configure Primary host

1. Select the 0210 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

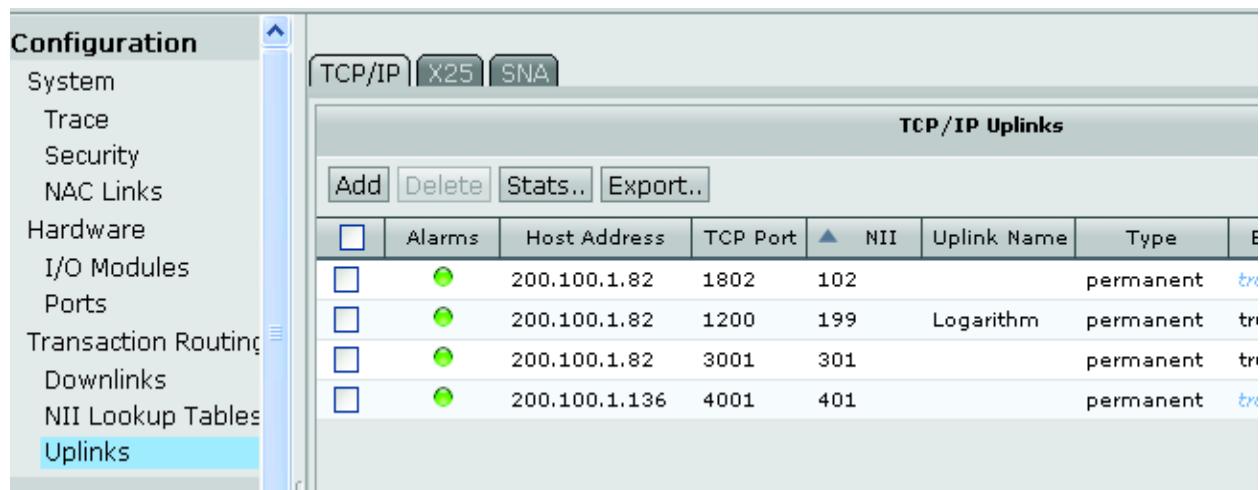


FIGURE 166. Uplinks configuration screens

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	Host1
TCP Port:	1400
NII:	500
Uplink Name:	0209 host bal-conn
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 167. Host1 TCP/IP Uplink load Balance node 0210 for node 0209

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (must be the same value as node 0208 Host2, port 1401)
10. Enter any other configuration settings
11. Click **OK**

Now on node 0210 configure cross over load balance host

1. Select the 0210 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

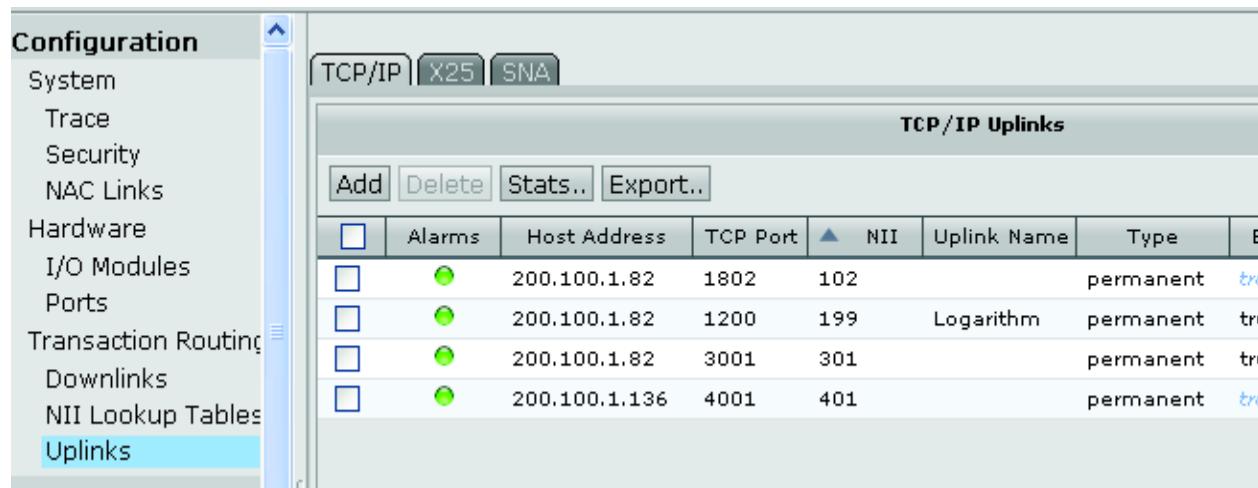


FIGURE 168. Uplinks configuration screens

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	Host1
TCP Port:	1401
NII:	600
Uplink Name:	0207 host bal-conn
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 169. Host1 TCP/IP Uplink load Balance node 0210 for node 0207

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (must be the same value as node 0208 Host2, port 1400)
10. Enter any other configuration settings
11. Click **OK**

Configure node name 0208 TCP/IP Uplinks

Configure Primary host

1. Select the 0208 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

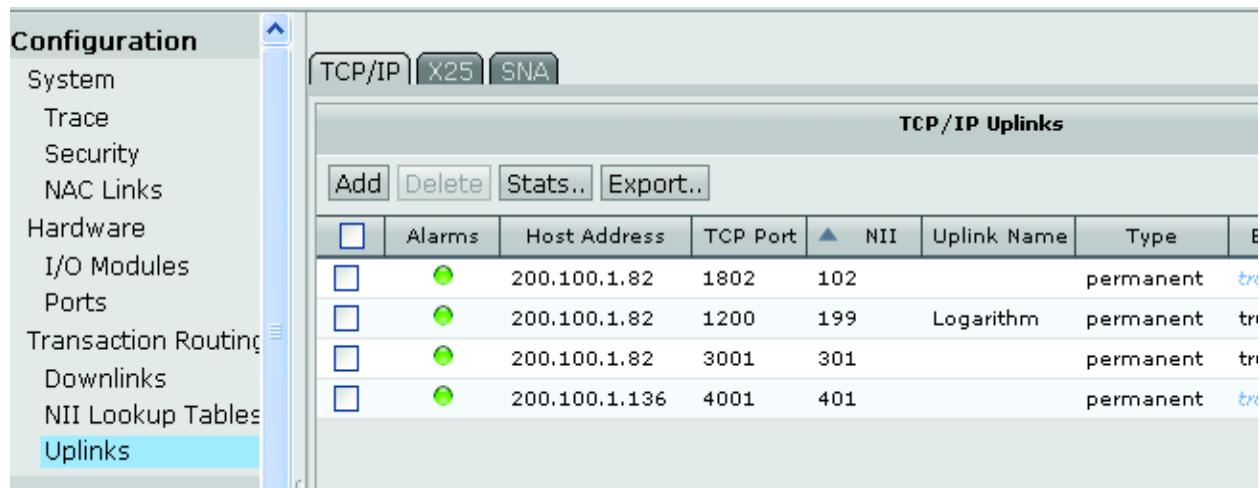


FIGURE 170. Uplinks configuration screens

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	Host2
TCP Port:	1400
NII:	600
Uplink Name:	0207 host bal-conn
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 171. Host2 TCP/IP Uplink load Balance node 0208 for node 0209

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (must be the same value as node 0210 Host2, port 1401)
10. Enter any other configuration settings
11. Click **OK**

Now on node 0208 configure cross over load balance host

1. Select the 0208 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

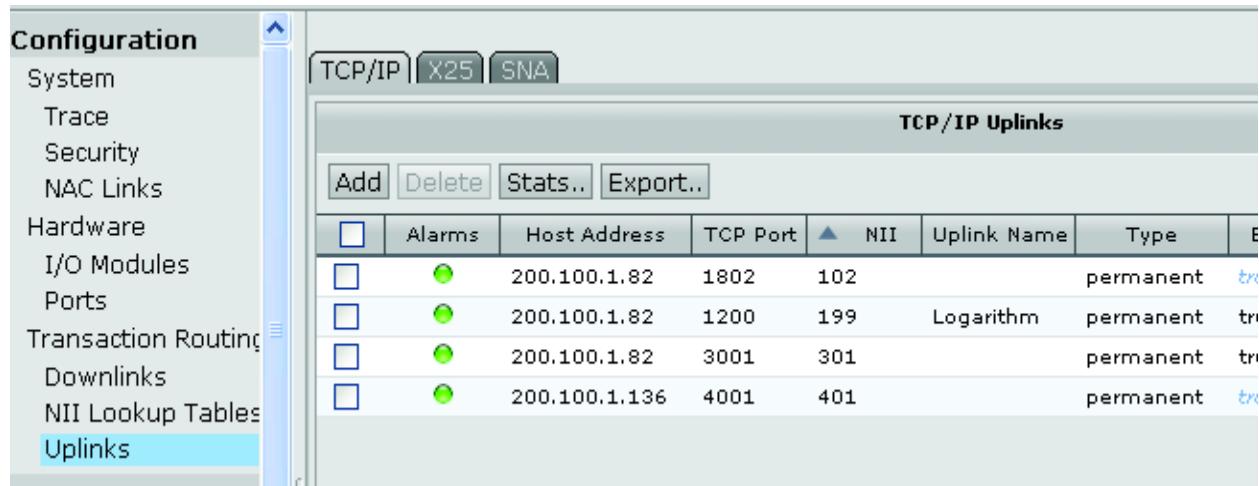


FIGURE 172. Uplinks configuration screens

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	Host2
TCP Port:	1401
NII:	500
Uplink Name:	0209 host bal-conn
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 173. Host2 TCP/IP Uplink load Balance node 0208 for node 0207

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (must be the same value as node 0210 Host1, port 1400)
10. Enter any other configuration settings
11. Click **OK**

Configure node name 0209 TCP/IP Host Uplinks

Configure Primary host uplink

1. Select the 0209 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

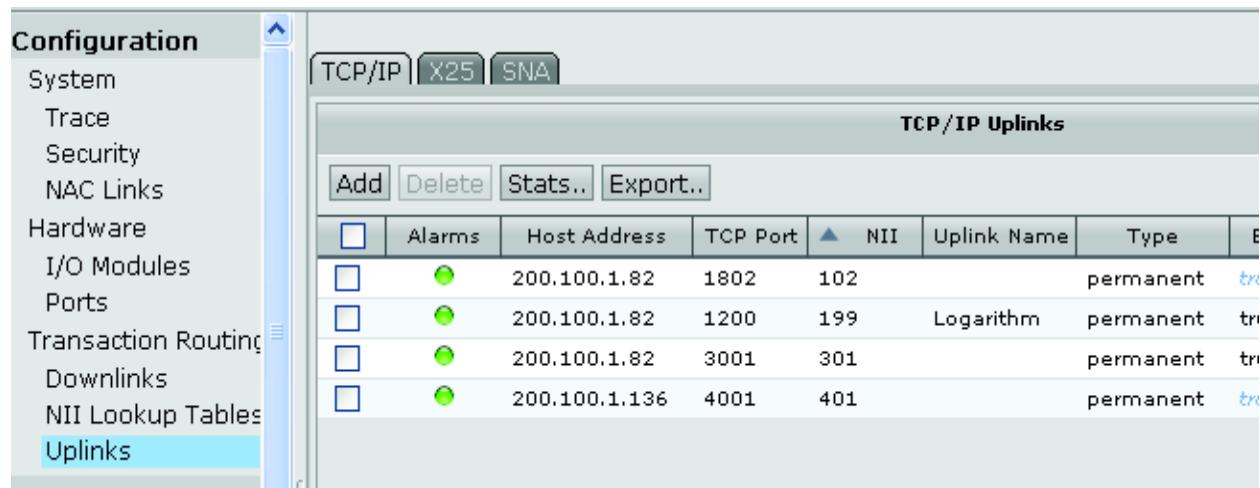


FIGURE 174. Uplinks configuration screens

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	Host1
TCP Port:	1400
NII:	500
Uplink Name:	0209 host bal-conn
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 175. Host1 TCP/IP Uplink load Balance on node 0209 for node 0209

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (value must match Host1 NII in node 0210)
10. Enter any other configuration settings
11. Click **OK**

Now on node 0209 configure fail over host uplink

1. Select the 0209 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

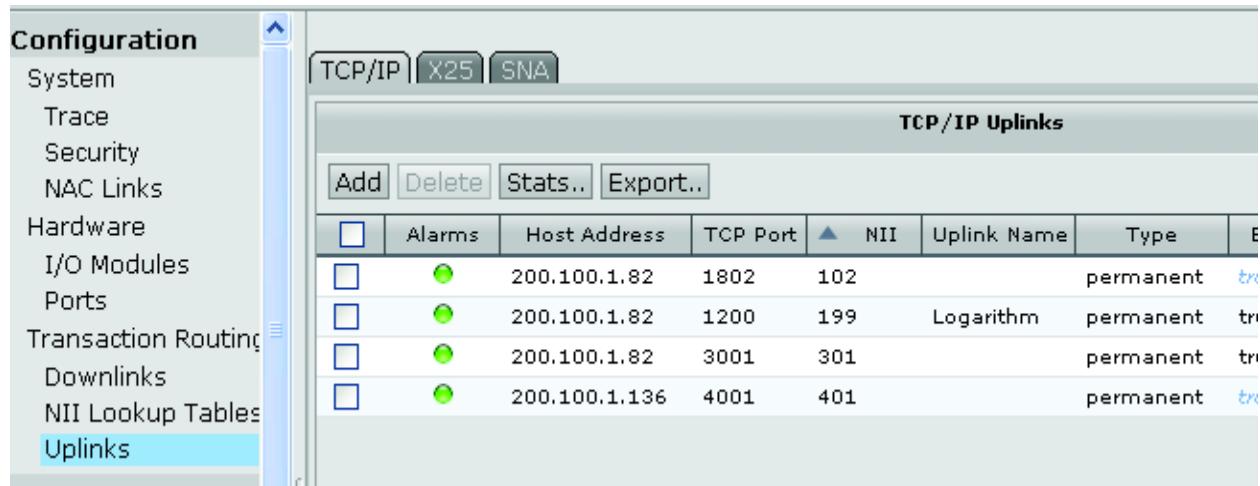


FIGURE 176. Uplinks configuration screens

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	Host2
TCP Port:	1401
NII:	500
Uplink Name:	0209 host bal-conn
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 177. Host2 TCP/IP Uplink load Balance on node 0209 for node 0209

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (value must match Host 2 fail over NII)
10. Enter any other configuration settings
11. Click **OK**

Configuration

Configure node name 0207 TCP/IP Host Uplinks

Configure Primary host uplink

1. Select the 0207 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

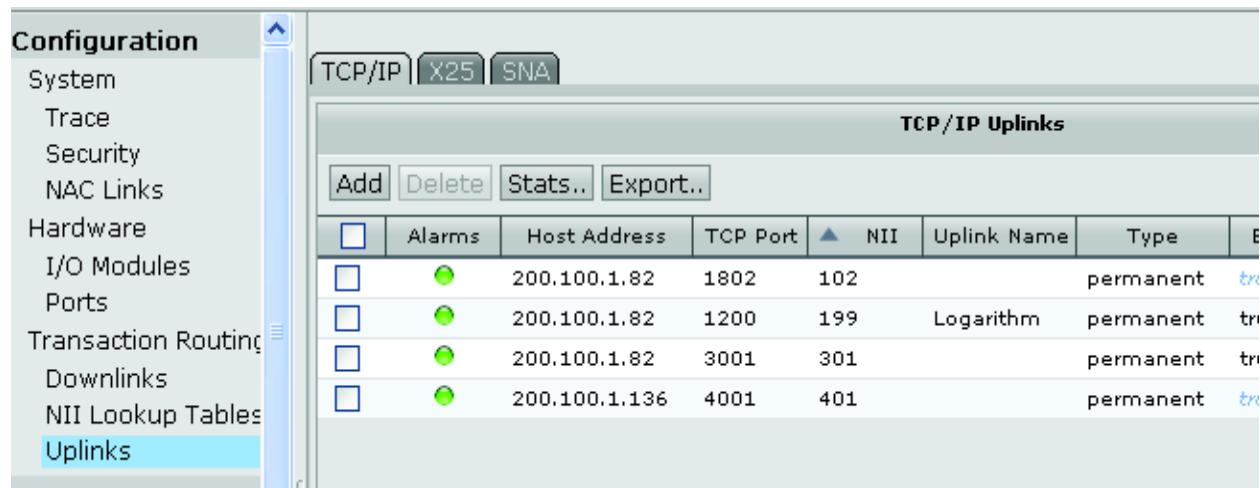


FIGURE 178. Uplinks configuration screens

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	Host 2
TCP Port:	1400
NII:	600
Uplink Name:	Host2 Pri uplink
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 179. Host2 TCP/IP Uplink load Balance on node 0207 for node 0207

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (value must match Host2 NII in node 0208)
10. Enter any other configuration settings
11. Click **OK**

Now on node 0207 configure fail over host uplink

1. Select the 0207 device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Uplinks** under Configuration > Transaction routing.
3. In the configure screen click on **TCP/IP** tab
4. The TCP/IP Uplink screen appears.

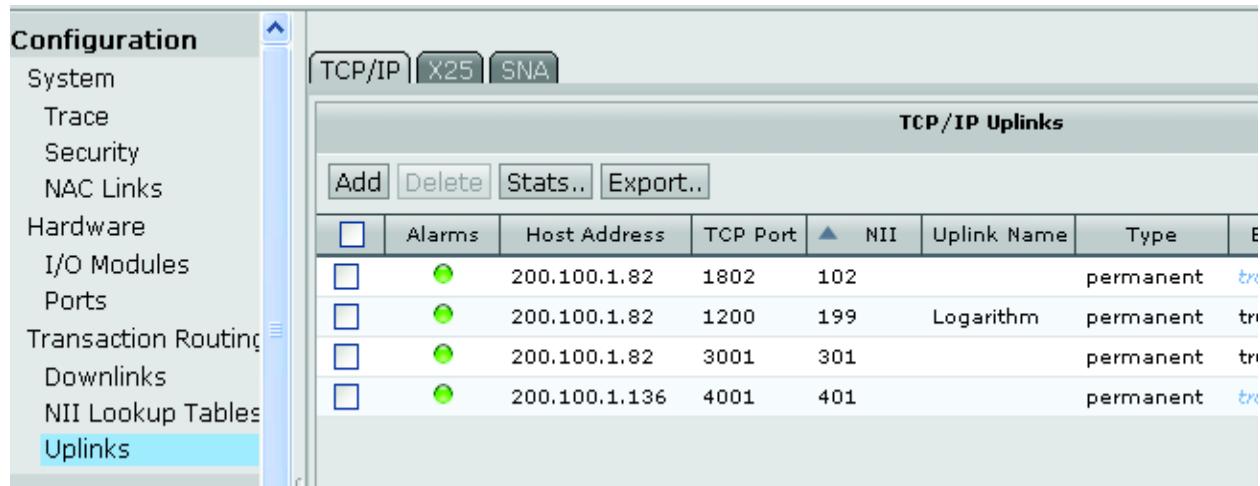


FIGURE 180. Uplinks configuration screens

5. Click **ADD** button
6. TCP/IP uplink configuration screen appears

TCP/IP Uplink

Transaction host Address:	Host1
TCP Port:	1401
NII:	600
Uplink Name:	0207 host bal-conn
Session Type:	permanent
Enable:	Default: true
Session Pool Size:	128
SSL:	Default: false
CA Certificate:	
Length Field Format:	Default: not-present
Include Length Field In Length:	Default: false
Vendor Link Protocol:	Default: false
Add TPDU if on-demand:	Default: false
Soft Shutdown:	Default: false
Keep Alive Timer (msec):	10000
Keep Alive Format:	Default: none
Connect Failed Timer:	4500

FIGURE 181. Host1 TCP/IP Uplink load Balance on node 0207 for node 0207

7. Enter “Transaction host Address” IP address (use actual IP address format xxx.xxx.xxx.xxx)
8. Enter Host “TCP Port” Value
9. Enter port “NII” value (value must match Host 1 fail over NII)
10. Enter any other configuration settings
11. Click **OK**

The NAC to NAC links and routing are complete for this load balance configuration.

For Nodes 0207 and 0209 any downlinks will have to have the NII tables built for proper routing IE. the downlinks on node 0207 use NII 600 for Host2 and downlinks on node 0209 use NII 500 for Host1. The load balance is handled automatically by round robin or ping pong operation

Alarm Configuration

The administrator is able to configure the alarm system utilizing the Alarm System Configuration screen. Accessible from the Config option in the IntelliView toolbar, it allows the administrator to configure Alarm Overrides, Alarm Rules, and specify notification properties.

Alarm Configuration Data

The Alarm system provides a level of configuration which is available to users through the IntelliView configuration screen.

Alarm Overrides

An Alarm Overrides configuration allows the administrator to override alarm settings and information.

1. On Main screen click on **Config**,
2. Click on **Alarm System** on pull down menu. the following screen appears

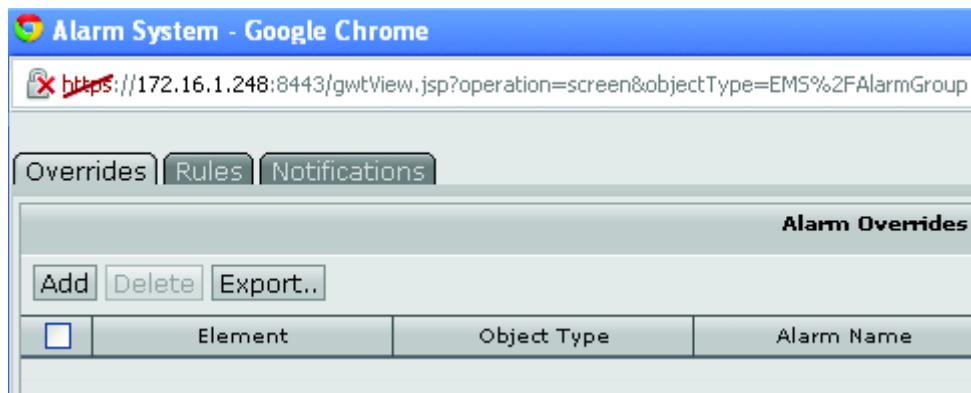


FIGURE 182. Alarm System screen

3. Select the **Overrides** Tab

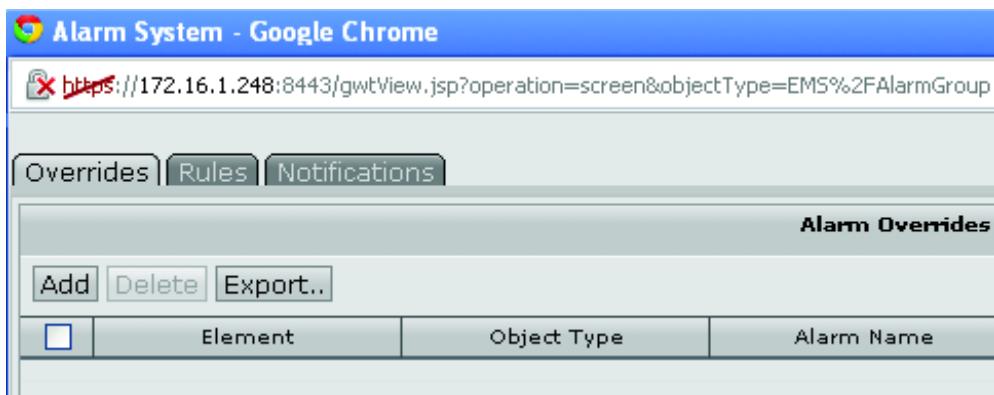


FIGURE 183. Alarm Override screen

4. Click on **Add** to add an Override

Alarm Override

Element:	IEN1000
Object Type:	
Alarm Name:	
<hr/>	
Severity:	
<input type="checkbox"/> Ignore Alarm (Do Not Raise)	
<input type="checkbox"/> Auto Acknowledge	
<input type="checkbox"/> Enable User Clearable	
 Info	
Reason Set:	
Reason Cleared:	
Recommended Actions:	

FIGURE 184. Alarm Override screen

The top portion of the Alarm Override screen contains four fields. They are used primarily to apply an alarm override to an alarm as it is being processed or viewed.

Alarm Configuration

Note: Event Name and Element must be specified. The Object Type can be left blank as a wild card.

- Element - Select device from pull down menu that the alarm will be received from
- Object Type - Select from pull down menu Device, Port, interface or EMS (Leave blank to apply to all)

Device
EMS
IntelliNAC/Intellinac_configuration_downlinks_tcpip
IntelliNAC/Intellinac_configuration_ioModules_ioModule
IntelliNAC/Intellinac_configuration_ports_etherenet
IntelliNAC/Intellinac_configuration_ports_pstnAnalog
IntelliNAC/Intellinac_configuration_ports_pstnIsdn
IntelliNAC/Intellinac_configuration_ports_x25Uplink
IntelliNAC/Intellinac_configuration_system_nacLinks_nacLink
IntelliNAC/Intellinac_configuration_uplinks_tcpip
IntelliNAC/Intellinac_configuration_uplinks_x25

Alarm Name - Select event from pull down menu (Leave blank to apply to all alarms)

Device Disconnected
ETHERNET_PORT_DOWN
HW_MODULE_CONFIG_BUT_NOT_PRESENT
HW_MODULE_CONFIG_MISMATCH
HW_MODULE_NO_CONFIG_BUT_PRESENT
Invalid License
License has expired
NAC_LINK_DISCONNECTED
NO_NIIS_AVAILABLE
PSTN_ANALOG_PORT_DOWN
PSTN_ISDN_PORT_DOWN
System ID mismatch
TCPPIP_DOWNLINK_UNAVAILABLE
TCPPIP_UPLINK_UNAVAILABLE
X25_UPLINK_PORT_DOWN
X25_UPLINK_UNAVAILABLE
valid License

- Severity - (Will be display in alarms and event just like the built in events and alarms) - Select from pull down menu

Critical
Major
Minor
Clear
Info
Maintenance

- Ignore Alarm (Do Not Raise) - If this is selected, the alarm will not be raised when the raising event is encountered. The event is still saved in log and statistic

- Auto Acknowledge - If this is selected, the alarm is raised and acknowledged immediately. It will not affect the Alarm Summary counters in the upper left corner of the Main screens
- User Clearable - Enable or disable the ability to clear the alarm. If User Clearable is selected, the alarm will be able to be cleared using the **Clear** button in the Alarm table.
- Info - The values specified here override the values from the alarms log file. Only the fields that are specified will override the default value. A blank field allows the default value to be used.

An alarm will map to either one or no alarm override. If two or more alarm overrides map to an alarm, the most specific one will be used.

Alarm Rules

Alarm rules are used to raise and clear alarms based on events. This allows an administrator to raise alarms on any event that is placed into the Event system. The alarm is named with the value specified in the **Alarm Name** field. The severity must also be specified or the alarm will be created in the Cleared state.

1. On Main screen click on **Config**,
2. Click on **Alarm System** on pull down menu. the following screen appears

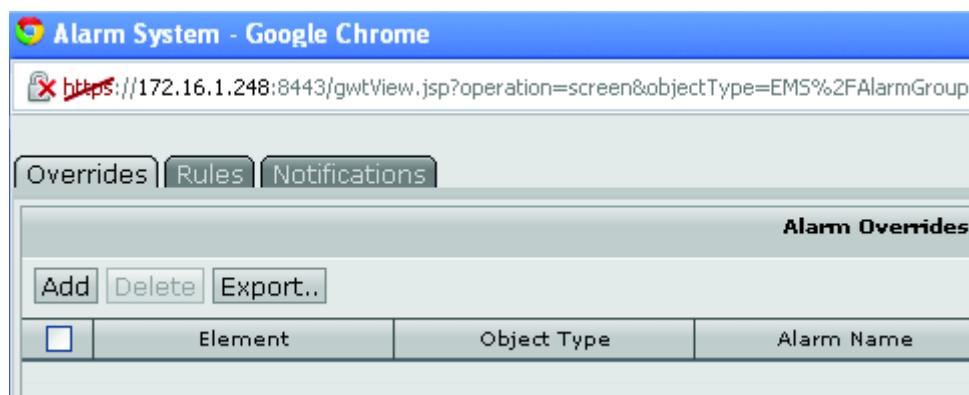
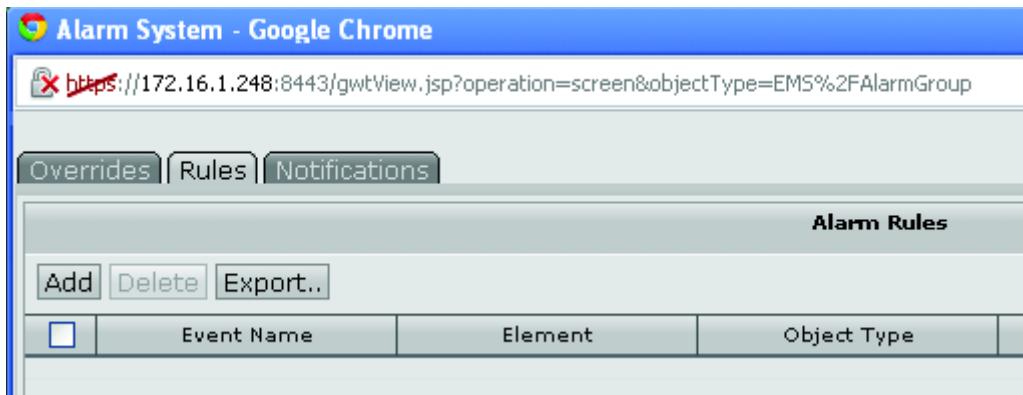


FIGURE 185. Alarm System screen

3. Select the **Rules** Tab

**FIGURE 186.** Alarm Rule screen

4. Click on **Add** to add a rule

A screenshot of a configuration dialog box titled "Alarm Rule". The dialog has several input fields:

- "Event Name:" dropdown menu
- "Element:" dropdown menu set to "IEN1000"
- "Object Type:" dropdown menu
- A section titled "Resulting Alarm" containing:
 - "Alarm Name:" dropdown menu
 - "Severity:" dropdown menu
 - A checked checkbox labeled "User Clearable"

FIGURE 187. Alarm Rule screen

Note: Event Name and Element must be specified. The Object Type can be left blank as a wild card.

- Event Name - Select event from pull down menu

Device Disconnected
ETHERNET_PORT_DOWN
HW_MODULE_CONFIG_BUT_NOT_PRESENT
HW_MODULE_CONFIG_MISMATCH
HW_MODULE_NO_CONFIG_BUT_PRESENT
Invalid License
License has expired
NAC_LINK_DISCONNECTED
NO_NIIS_AVAILABLE
PSTN_ANALOG_PORT_DOWN
PSTN_ISDN_PORT_DOWN
System ID mismatch
TCPIP_DOWNLINK_UNAVAILABLE
TCPIP_UPLINK_UNAVAILABLE
X25_UPLINK_PORT_DOWN
X25_UPLINK_UNAVAILABLE
valid License

- Element - Select device from pull down menu that the alarm will be received from
- Object Type - Select from pull down menu Device, Port, interface or EMS

Device
EMS
IntelliNAC/Intellinac_configuration_downlinks_tcpip
IntelliNAC/Intellinac_configuration_ioModules_ioModule
IntelliNAC/Intellinac_configuration_ports_ethernet
IntelliNAC/Intellinac_configuration_ports_pstnAnalog
IntelliNAC/Intellinac_configuration_ports_pstnIsdn
IntelliNAC/Intellinac_configuration_ports_x25Uplink
IntelliNAC/Intellinac_configuration_system_nacLinks_nacLink
IntelliNAC/Intellinac_configuration_uplinks_tcpip
IntelliNAC/Intellinac_configuration_uplinks_x25

- Alarm Name - (Name of resultant alarm) Select from pull down menu

Device Disconnected
ETHERNET_PORT_DOWN
HW_MODULE_CONFIG_BUT_NOT_PRESENT
HW_MODULE_CONFIG_MISMATCH
HW_MODULE_NO_CONFIG_BUT_PRESENT
Invalid License
License has expired
NAC_LINK_DISCONNECTED
NO_NIIS_AVAILABLE
PSTN_ANALOG_PORT_DOWN
PSTN_ISDN_PORT_DOWN
System ID mismatch
TCPIP_DOWNLINK_UNAVAILABLE
TCPIP_UPLINK_UNAVAILABLE
X25_UPLINK_PORT_DOWN
X25_UPLINK_UNAVAILABLE
valid License

Alarm Configuration

- Severity - (Will be display in alarms and event just like the built in events and alarms) - Select from pull down menu

Critical
Major
Minor
Clear
Info
Maintenance

- User Clearable - Enable or disable the ability to clear the alarm. If User Clearable is selected, the alarm will be able to be cleared using the **Clear** button in the Alarm table.

Alarm Notifications

Most alarms are raised and cleared based on Alarm-type events. The system contains a correlation engine that looks at events and applies them to the alarm system. The correlation is based on the following fields: Name, Element, Source Type, and Source ID.

The Alarms screen shows generic text for the alarm describing what typically caused this alarm, how it is cleared, and actions the user might take to remedy the alarm condition.

An administrator can set up a Notification Policy. There is only one notification policy per system and it applies to all alarms. The **Alarm Notification** screen is used for its configuration.

1. On Main screen click on **Config**,
2. Click on **Alarm System** on pull down menu. the following screen appears

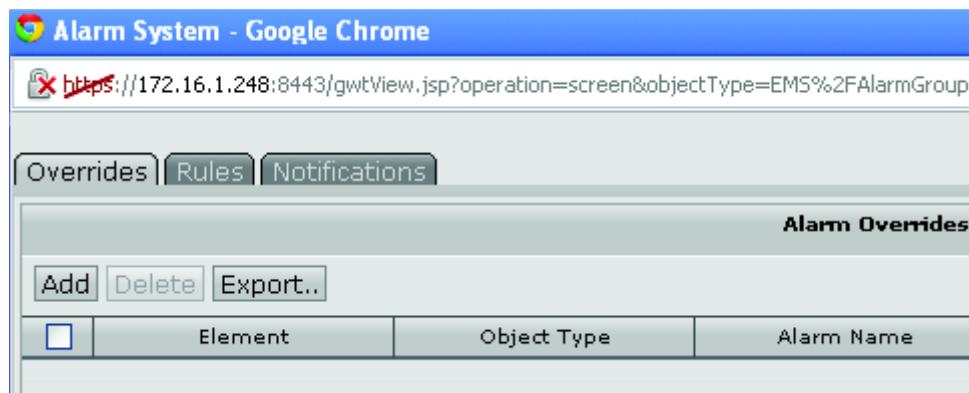


FIGURE 188. Alarm System screen

3. Select the **Notifications** Tab



FIGURE 189. Alarm Notification screen

A screenshot of the "Alarm Notification Properties" screen, specifically the "Level 1" tab. The tab bar at the top includes "Level 1", "Level 2", "Alarm Clear", "Alarm Ack", and "Audibles".

Level 1

Open Alarms
 Unacked Alarms

Trigger (minutes):

The E-Mail Recipients field may be specified with a comma separated list of email address such as (not including the double quotes): "a@company.com, g@gmail.com, y@yahoo.com".

E-Mail Recipients:

Available

Admin
admin
ilan
mike
rick

>
<
all
none

Assigned

FIGURE 190. Alarm Notification Properties screen - Level 1 tab

The five tab pages are described below:

Level 1

- Open Alarms - Notifications are sent to the email recipients and users specified when an alarm has been in the state specified by the Open Alarms
- Unacked Alarms - Notifications are sent to the email recipients and users specified when an alarm has been in the state specified by the Unacked Alarms
- Trigger (minutes) - Notifications are sent to the email recipients and users specified in the time specified in the trigger. If Open Alarms is selected, the email notifications are sent when the alarm has been open for the trigger minutes. If Unacked Alarms is selected, the email notifications are sent when the alarm has been unacknowledged for the trigger minutes. If both are selected, only one email message is sent, but it will be sent if the trigger time is exceeded for either setting.

Level 2

Level 2 is options and is used for escalation in the event Level 1 notifications are not acknowledged.

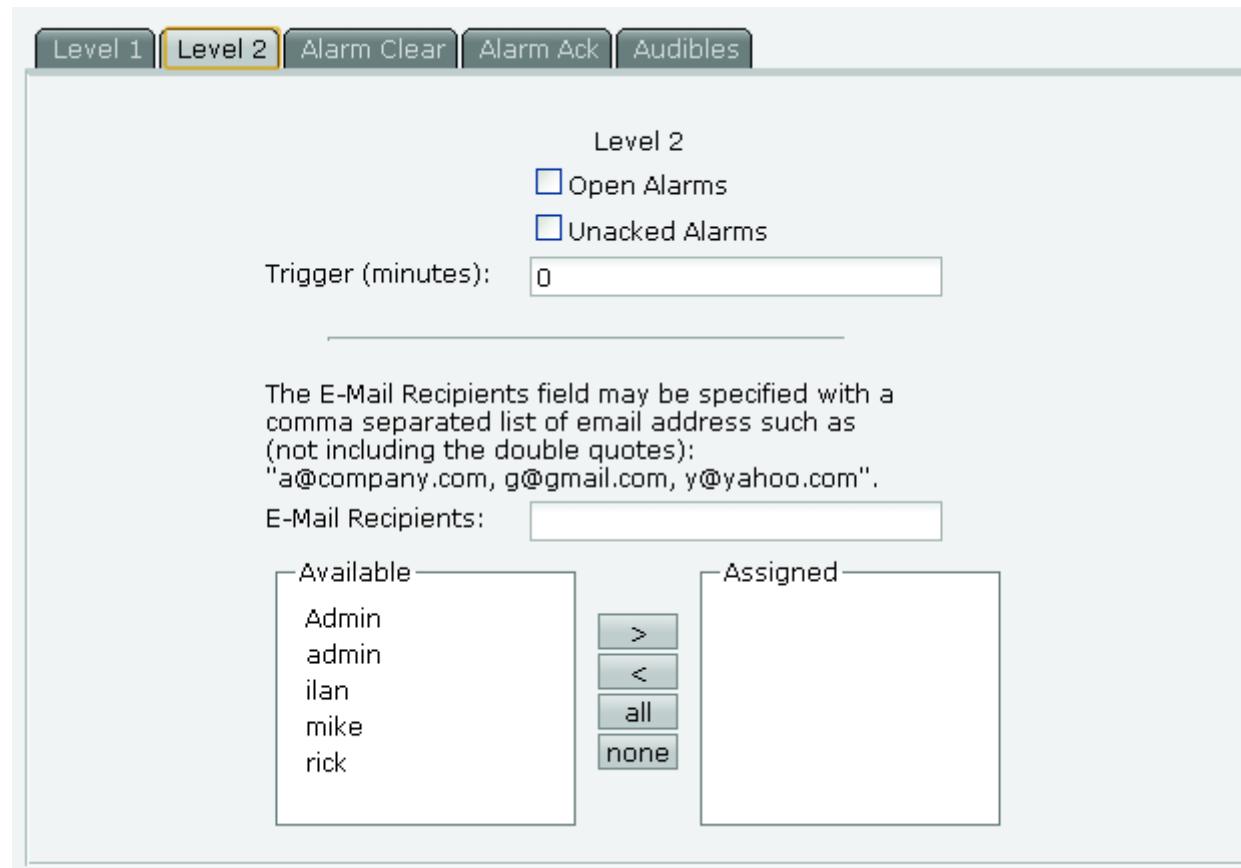


FIGURE 191. Alarm Notification Properties screen - Level 2 tab

- Open Alarms - Notifications are sent to the email recipients and users specified when an alarm has been in the state specified by the Open Alarms

Configuration

- Unacked Alarms - Notifications are sent to the email recipients and users specified when an alarm has been in the state specified by the Unacked Alarms
- Trigger (minutes) - Notifications are sent to the email recipients and users specified in the time specified in the trigger. If Open Alarms is selected, the email notifications are sent when the alarm has been open for the trigger minutes. If Unacked Alarms is selected, the email notifications are sent when the alarm has been unacknowledged for the trigger minutes. If both are selected, only one email message is sent, but it will be sent if the trigger time is exceeded for either setting.

Alarm Clear

This tab allows the administrator to send email notifications when an alarm is cleared.

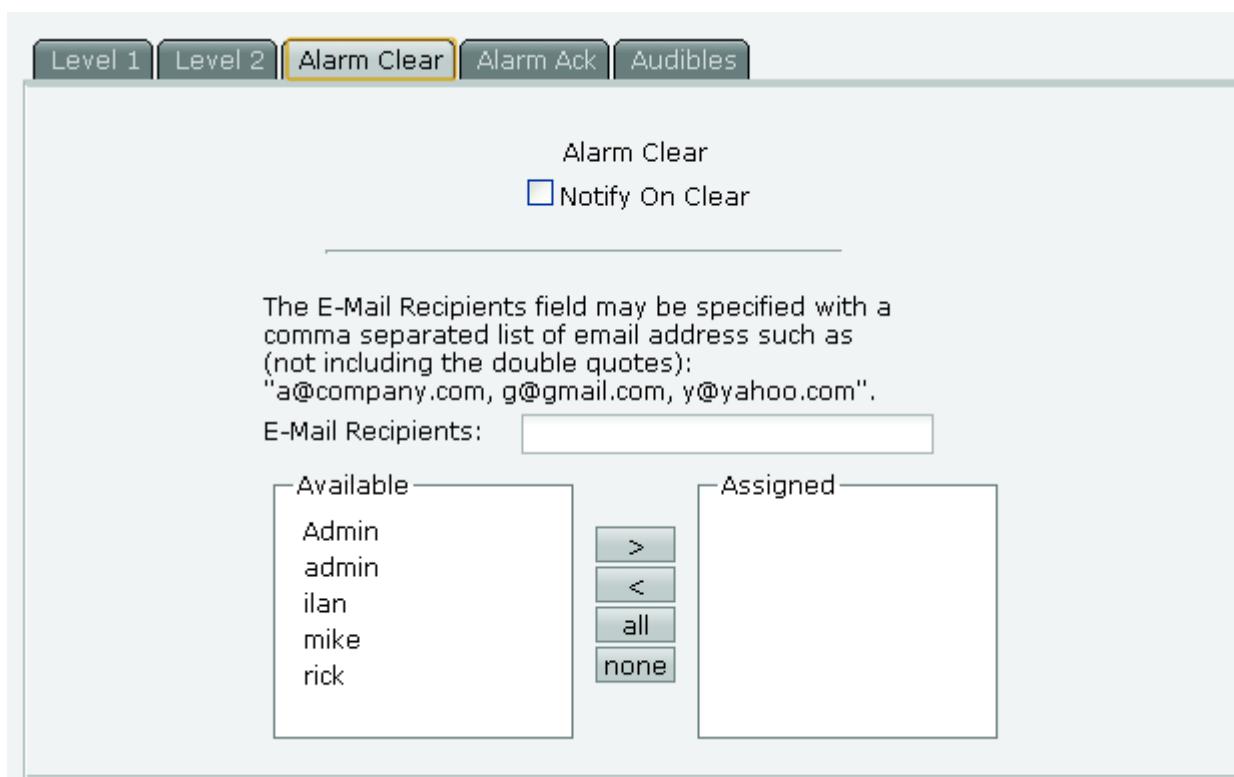


FIGURE 192. Alarm Notification Properties screen - Alarm Clear tab

- Notify On Clear - When selected email notification will be sent to listed recipients when the alarm is cleared

Alarm Ack

This tab allows the administrator to send email notifications when an alarm is acknowledged

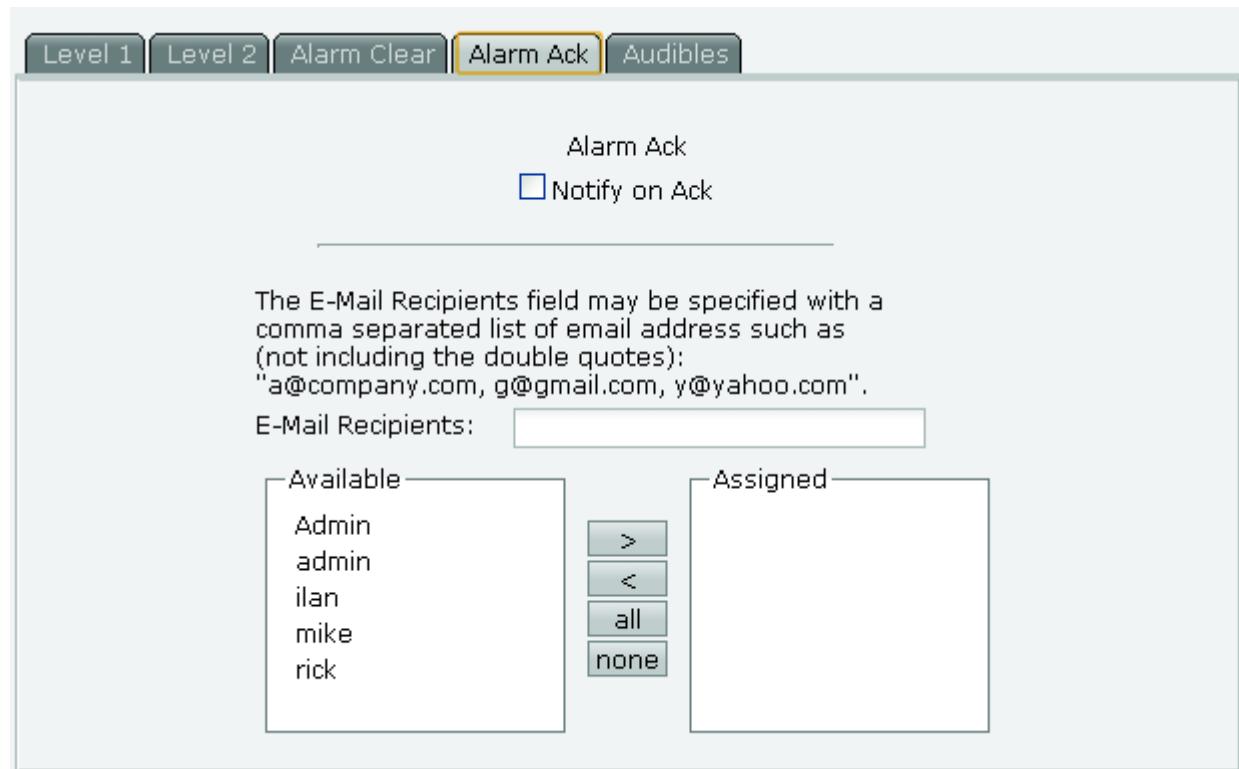


FIGURE 193. Alarm Notification Properties screen - Alarm Ack tab

- Notify On Ack - When selected email notification will be sent to listed recipients on acknowledgment of alarm

Audibles

This tab allows the configuration of alarm audibles. The administrator can set a sound to play in the GUI if an alarm is raised in an Alarm table. A different sound may be specified for each severity.

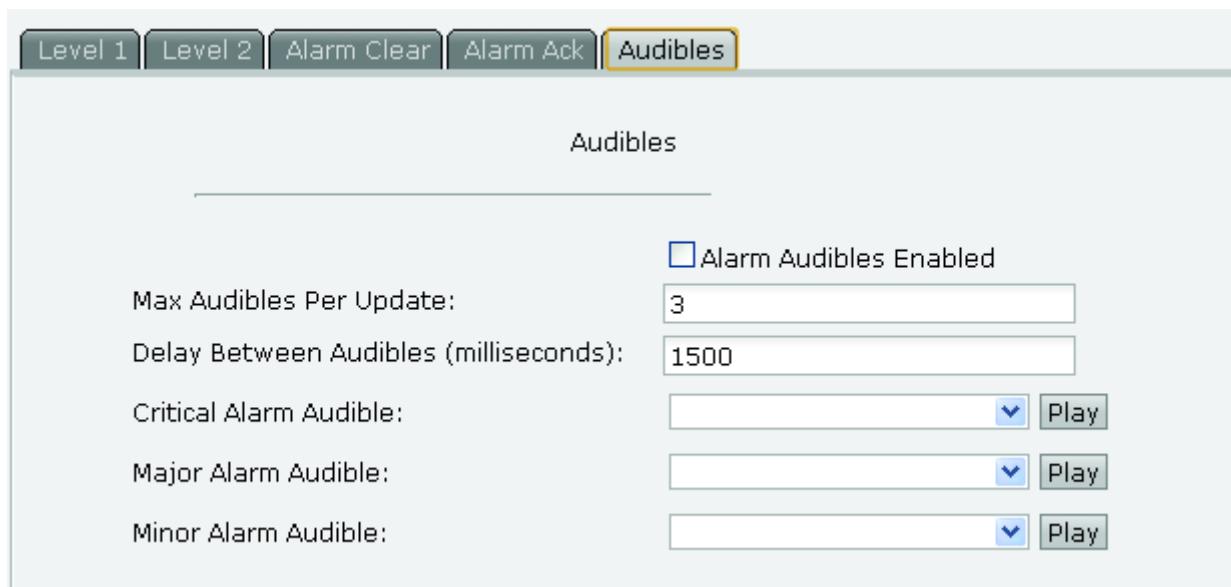


FIGURE 194. Alarm Notification Properties screen - Audibles tab

Sounds should not be played when an alarm is cleared. A setting exists to set the maximum number of audibles in an update period (five seconds), and a delay between the playing of an audible. If no delay is specified, three audibles may play at the same time, sounding like one audible.

Additional sounds can be uploaded by the following process

1. Select **Config** from Main screen toolbar
2. Select **Web Resources** from pull down menu
3. Select **Sounds** tab
4. Select **Upload** button
5. Select **Choose file** locate sound file to be uploaded

Note only MP3 audio file format is supported

Email Configuration

An administrator can configure the system to send mail notifications. Email configuration must be specified to configure mail. This configuration is available as a selection from the IntelliView toolbar > Config option.

This configuration allows the system to use SMTP to send mail using an SMTP server. Mail debugging allows non-authenticated connections to display the SMTP connection information into the server log.

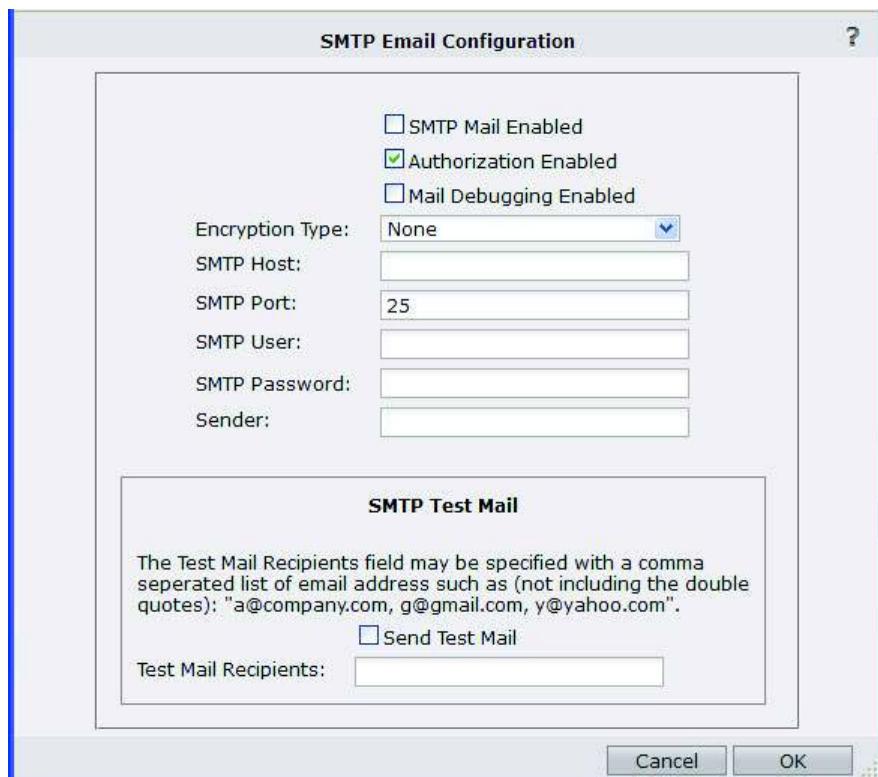


FIGURE 195. Email Configuration screen

A user may configure STARTTLS configurations which are necessary to use gmail. SSL configurations can also be used.

The email configuration allows the user to send a test mail message to verify that the connection is good. Selecting the **Send Test Mail** checkbox and submitting the form sends a test mail message to the recipients list.

Clicking **OK** displays a system message:



FIGURE 196. Email configuration confirmation

Click **OK** to close.

Device File Manager Configuration

Every device typically has a variety of user-generated files that need to be uploaded to it. Similarly, a device may have files that need to be downloaded for offline processing. The Device File Manager is an application that facilitates the transfer of arbitrary files between a device and the user, using IntelliView as the staging entity. Files can be uploaded or downloaded to or from a device. These files can also optionally reside on IntelliView and can be managed there.

Access to the File Management functions is controlled by the security system, where permissions are assigned to a user to enable various levels of operations.

There are five settings or levels:

- **None** - No File Management permissions are available to the user. The menu option used to launch the file management operations is not visible, thus the user cannot do anything.
- **View** - The user can view files that are staged on IntelliView
- **Manage** - The user may upload new files to IntelliView, these files will be stored in the staging area
- **Download** - The user can download files from the device onto the staging area on IntelliView, and further download them on the desktop
- **Upload** - The user can upload files from the staging area on IntelliView to the device. Since uploading these files can affect device operations, this is the highest privilege level.

The Device File Manager is launched from the main toolbar, **Devices > Files**.

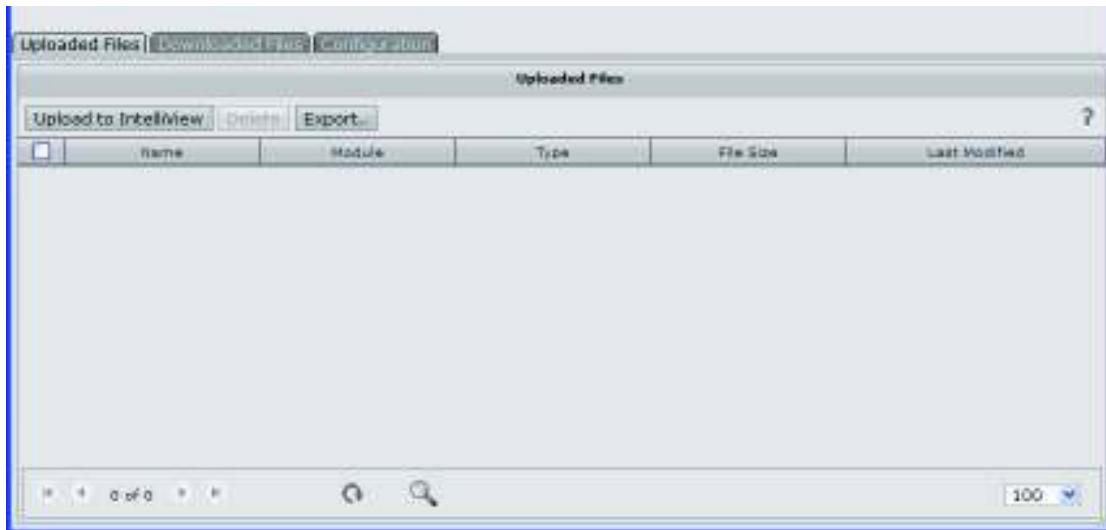


FIGURE 197. Device File Manager

Three distinct functions may be performed:

- Upload files onto the IntelliView staging area and manage them
- Download files from the staging area onto the user's desktop
- Set up the locations on IntelliView where downloaded and uploaded files are stored.

Uploading Files to IntelliView

The **Upload Files** tab page shows a list of files that have been uploaded to IntelliView. The listing is based upon the module type and the file type.

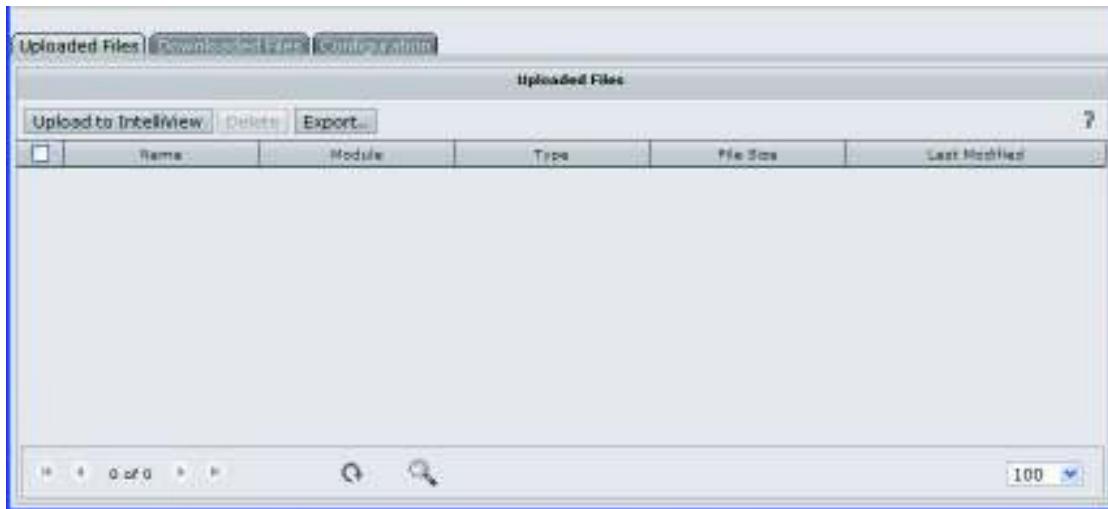


FIGURE 198. Upload Files tab page

The file listing provides the following information about the file:

- The name of the file
- The name of the module the file is associated with
- The name of the upload file type (this is dependent (upon the module)
- The size of the file
- The date-time stamp indicating when the file was last modified. This corresponds to the time when the file was uploaded to IntelliView.

To upload a new file onto the staging area:

1. Click **Upload to IntelliView**. The **File Upload** screen appears.

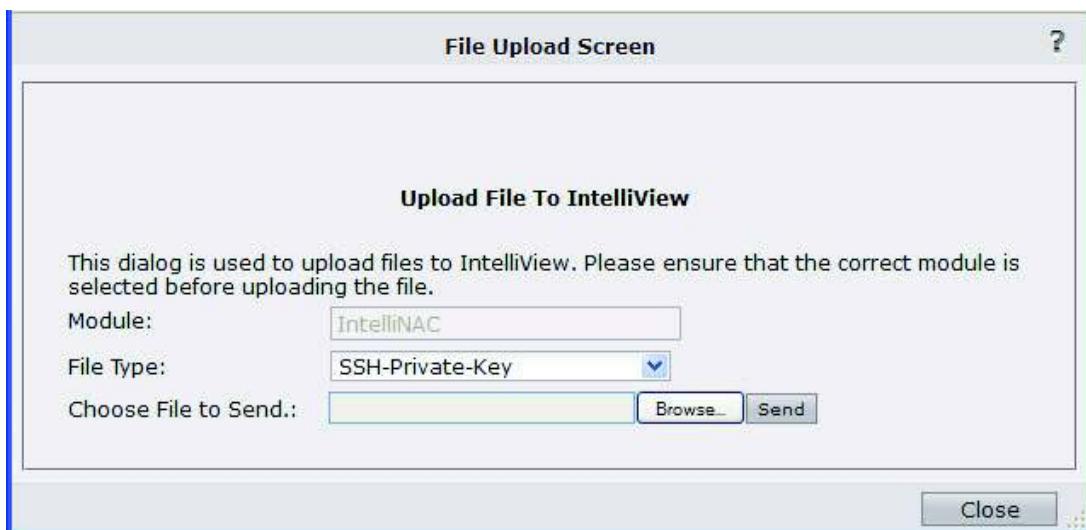


FIGURE 199. File Upload screen

2. Select the module and file type that corresponds to the file you are uploading.
3. Click **Browse** to find the location to be set for saving the file.
4. Click **Send**. This uploads the file to IntelliView and the new file appears in the list of uploaded files after a successful file transfer.

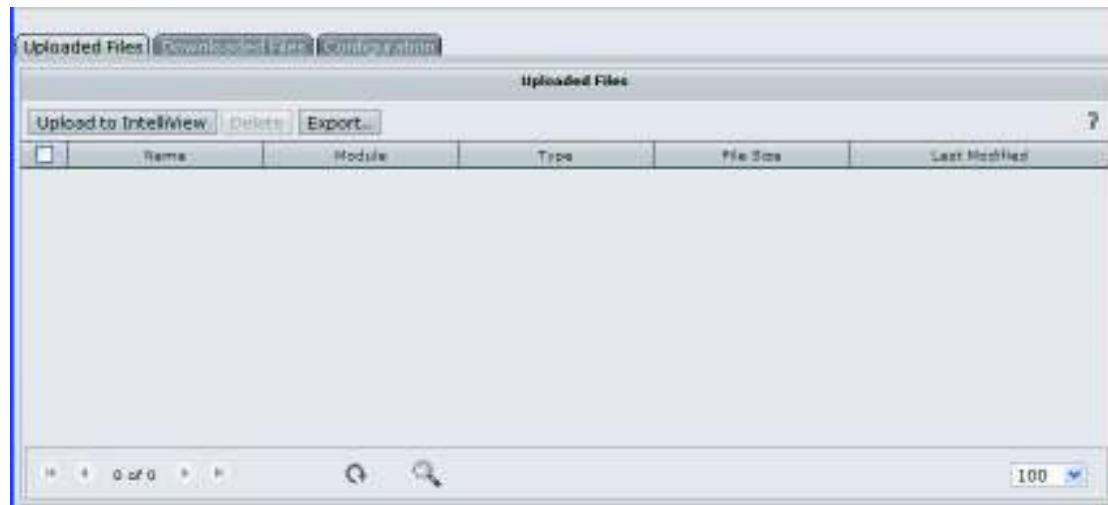


FIGURE 200. Updated list of uploaded files

Downloading Files from IntelliView

The **Downloaded Files** tab page shows a list of files that have been downloaded from one or more devices to IntelliView.

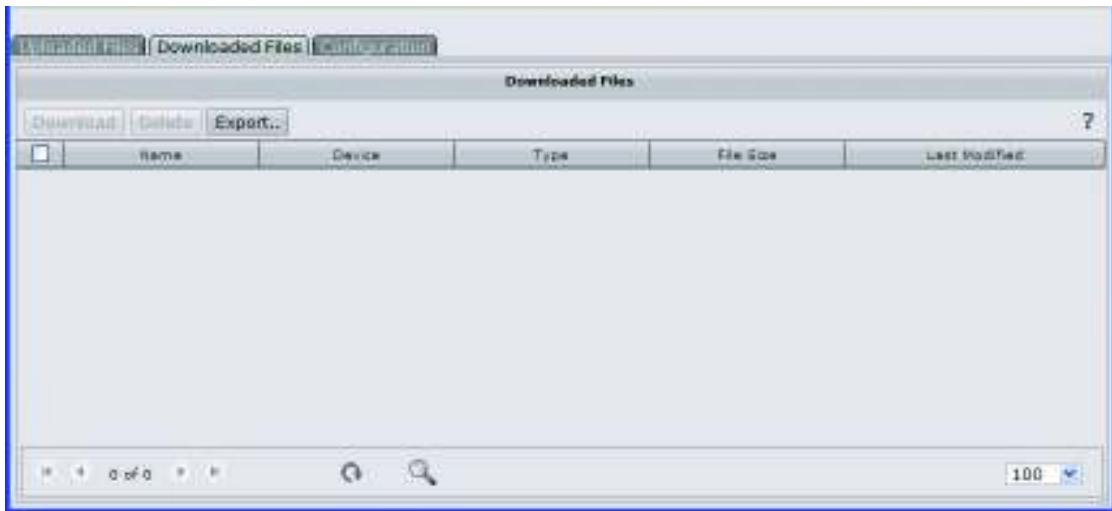


FIGURE 201. Downloaded Files tab page

The listing is based upon the device and the file type. The file listing provides the following information about the file:

- The name of the file
- The name of the device the file is associated with
- The name of the upload file type (this is dependent upon the module)
- The size of the file
- The date-time stamp indicating when the file was last modified. This usually corresponds to the time when the file was downloaded from IntelliView.

To download the file:

1. Click **Download**.
2. Click **Browse** to specify location for the file on the local file system.
3. Click **OK**. This downloads the selected file.

Staging Area

The **Configuration** tab page allows you to specify the location of the upload and download staging areas.

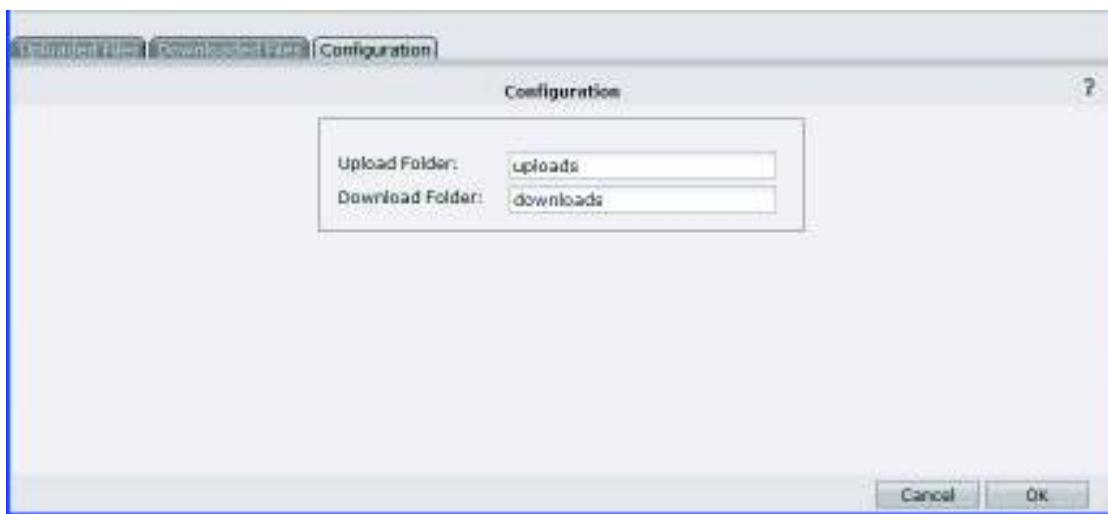


FIGURE 202. Configuration tab page

By default, these folders are called uploads and downloads and are relative to the location of where IntelliView is installed.

- The uploads location is:
 `${IView_Run}/ 3rdParty/apache-tomcat-6.0.29/webapps/ROOT/
 uploads`
- The downloads location is:

`${IView_Run}/ 3rdParty/apache-tomcat-6.0.29/webapps/ROOT/
 downloads`

These locations can be changed and all subsequent uploads and downloads will be relative to the configured locations.

Uploading a File to the Device

To upload a specific file to the device:

1. Click on the device of interest in the map or tree.
2. Select **Files > Upload** from the main toolbar or right-click and select **Files > Upload** from the displayed menu. The **Files on Device** screen appears.

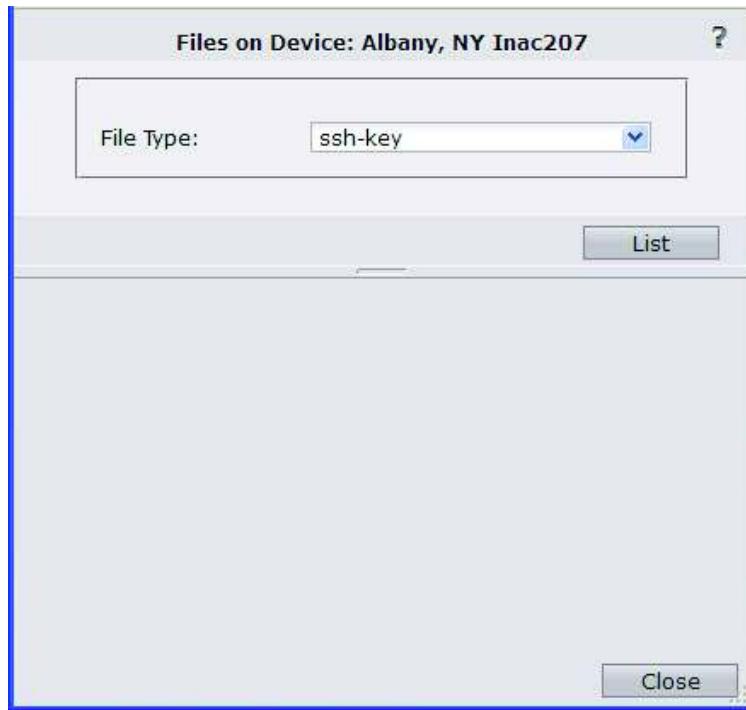


FIGURE 203. Files on Device screen

3. Select the file type from the drop-down list in the upper pane.
4. Click **List**. The files on the device which correspond to that file type are displayed.
5. Select the desired file from the Device File Listing.
6. Click **Upload**. The staging area screen appears.

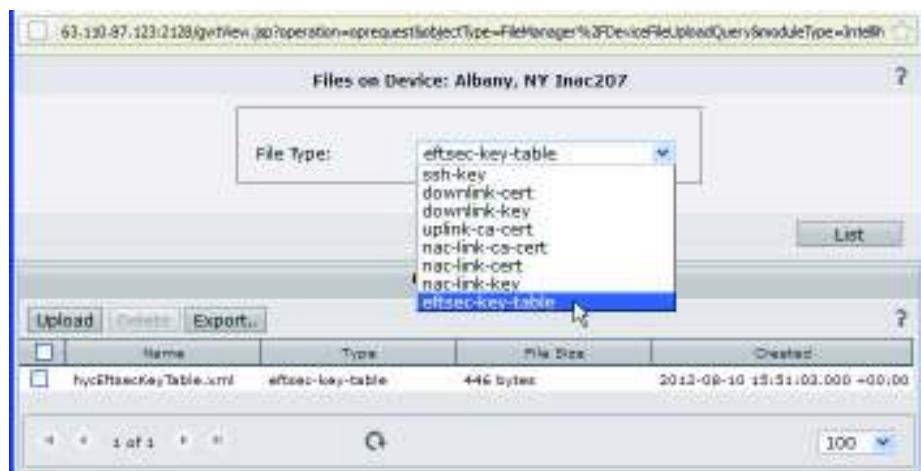


FIGURE 204. Staging area screen

7. Select the file and click **Upload to Device**. The file is transferred onto the device and the new file appears in the Device File Listing.



FIGURE 205. Updated Device File Listing

Downloading a File from the Device

To download a specific file from the device:

1. Click on the device of interest in the map or tree.
2. Select **Files > Download** from the main toolbar or right-click and select **Files > Download** from the displayed menu. The **Files on Device** screen appears
3. Select the file type from the drop-down list in the upper pane.
4. Click **List**. The files on the device which correspond to that file type are displayed.

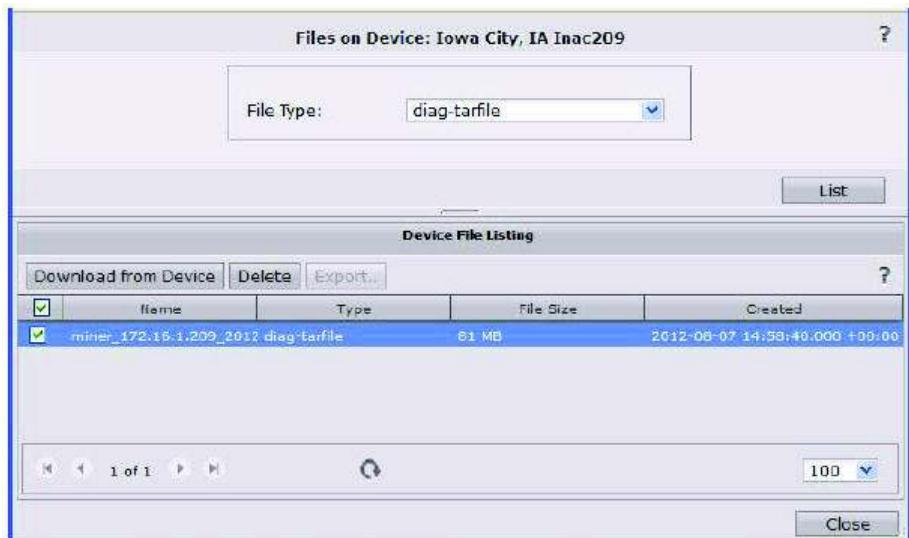


FIGURE 206. Selecting the desired file

5. Select the file and click **Download from Device**. The file is transferred from the file and a system message appears.

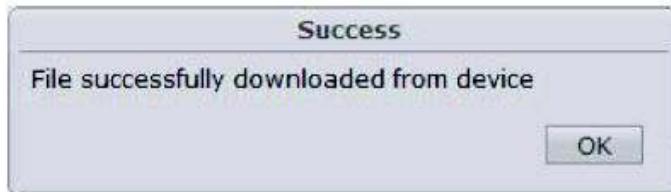


FIGURE 207. Download confirmation

Statistics Configuration

IntelliView provides a configuration application to configure scheduled statistic collection.

There are two ways to reach the Statistical collection configuration:

One:

On the Main screen select **Statistics**

From the pull down menu select **Configure**

Two:

On the Main screen **Right click** on the IntelliVIEW symbol

From the pull down menu select **Statistics**

From the extended pull down menu select **Configure**

Assignment Tab

An administrator can use the following fields to enable/disable statistics on a per device basis:

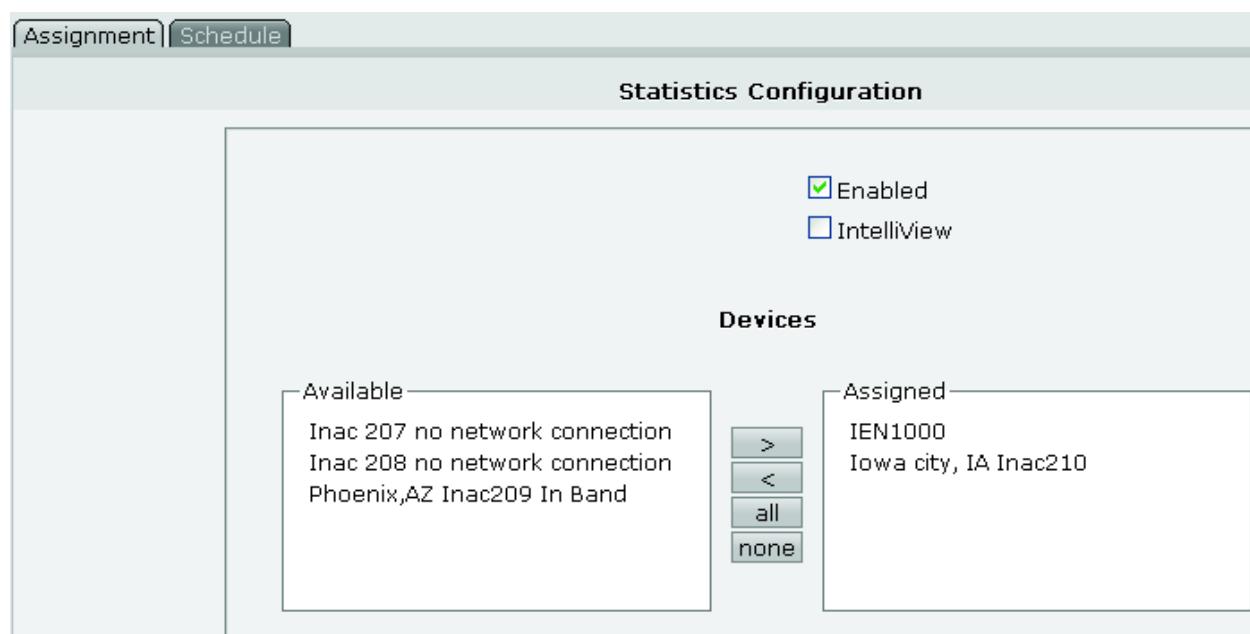


FIGURE 208. IntelliView Properties screen

- **Enabled** - This setting enables statistics for all devices.
- **IntelliView** - This setting enables/disables IntelliView statistics
- **Devices** - Choose which devices to collect statistics from

Configuration

Schedule Tab

Schedule allows an administrator to configured when to collect and reset the statistics. It also allows the configuration of where the statistic repository is located. Pre-Release 2.0 the repository can only be located on the server (VM or physical machine) that IntelliVIEW is installed.

Note: The statistics are collected from the device(s) and are stored as time stamped files for each collection time. **Reset does clear the statistics stored on the Device**

The screenshot shows a 'Collect Schedule' interface. On the left is a grid of checkboxes for selecting collection times. The columns represent hours from 00:00 to 20:00 in 15-minute increments. Rows represent minutes from 00 to 45. Some checkboxes are checked (e.g., 00:00, 01:00, 02:00, 03:00). To the right of the grid are buttons for 'Clear All', 'Collect' (radio button), and 'Collect & Reset' (radio button). Further right are dropdowns for 'File Format' (CSV) and 'Age days' (30), and text fields for 'IntelliView Repository Path' (statsCollection) and 'External Repository Path' (empty).

Collect Schedule					
<input checked="" type="checkbox"/> 00:00	<input checked="" type="checkbox"/> 04:00	<input checked="" type="checkbox"/> 08:00	<input checked="" type="checkbox"/> 12:00	<input checked="" type="checkbox"/> 16:00	<input checked="" type="checkbox"/> 20:00
<input type="checkbox"/> 00:15	<input type="checkbox"/> 04:15	<input type="checkbox"/> 08:15	<input type="checkbox"/> 12:15	<input type="checkbox"/> 16:15	<input type="checkbox"/> 20:15
<input type="checkbox"/> 00:30	<input type="checkbox"/> 04:30	<input type="checkbox"/> 08:30	<input type="checkbox"/> 12:30	<input type="checkbox"/> 16:30	<input type="checkbox"/> 20:30
<input type="checkbox"/> 00:45	<input type="checkbox"/> 04:45	<input type="checkbox"/> 08:45	<input type="checkbox"/> 12:45	<input type="checkbox"/> 16:45	<input type="checkbox"/> 20:45
<input checked="" type="checkbox"/> 01:00	<input checked="" type="checkbox"/> 05:00	<input checked="" type="checkbox"/> 09:00	<input checked="" type="checkbox"/> 13:00	<input checked="" type="checkbox"/> 17:00	<input checked="" type="checkbox"/> 21:00
<input type="checkbox"/> 01:15	<input type="checkbox"/> 05:15	<input type="checkbox"/> 09:15	<input type="checkbox"/> 13:15	<input type="checkbox"/> 17:15	<input type="checkbox"/> 21:15
<input type="checkbox"/> 01:30	<input type="checkbox"/> 05:30	<input type="checkbox"/> 09:30	<input type="checkbox"/> 13:30	<input type="checkbox"/> 17:30	<input type="checkbox"/> 21:30
<input type="checkbox"/> 01:45	<input type="checkbox"/> 05:45	<input type="checkbox"/> 09:45	<input type="checkbox"/> 13:45	<input type="checkbox"/> 17:45	<input type="checkbox"/> 21:45
<input checked="" type="checkbox"/> 02:00	<input checked="" type="checkbox"/> 06:00	<input checked="" type="checkbox"/> 10:00	<input checked="" type="checkbox"/> 14:00	<input checked="" type="checkbox"/> 18:00	<input checked="" type="checkbox"/> 22:00
<input type="checkbox"/> 02:15	<input type="checkbox"/> 06:15	<input type="checkbox"/> 10:15	<input type="checkbox"/> 14:15	<input type="checkbox"/> 18:15	<input type="checkbox"/> 22:15
<input type="checkbox"/> 02:30	<input type="checkbox"/> 06:30	<input type="checkbox"/> 10:30	<input type="checkbox"/> 14:30	<input type="checkbox"/> 18:30	<input type="checkbox"/> 22:30
<input type="checkbox"/> 02:45	<input type="checkbox"/> 06:45	<input type="checkbox"/> 10:45	<input type="checkbox"/> 14:45	<input type="checkbox"/> 18:45	<input type="checkbox"/> 22:45
<input checked="" type="checkbox"/> 03:00	<input checked="" type="checkbox"/> 07:00	<input checked="" type="checkbox"/> 11:00	<input checked="" type="checkbox"/> 15:00	<input checked="" type="checkbox"/> 19:00	<input checked="" type="checkbox"/> 23:00
<input type="checkbox"/> 03:15	<input type="checkbox"/> 07:15	<input type="checkbox"/> 11:15	<input type="checkbox"/> 15:15	<input type="checkbox"/> 19:15	<input type="checkbox"/> 23:15
<input type="checkbox"/> 03:30	<input type="checkbox"/> 07:30	<input type="checkbox"/> 11:30	<input type="checkbox"/> 15:30	<input type="checkbox"/> 19:30	<input type="checkbox"/> 23:30
<input type="checkbox"/> 03:45	<input type="checkbox"/> 07:45	<input type="checkbox"/> 11:45	<input type="checkbox"/> 15:45	<input type="checkbox"/> 19:45	<input type="checkbox"/> 23:45

Clear All

Collect Collect & Reset

File Format: CSV

Age days: 30

IntelliView Repository Path: statsCollection

External Repository Path:

FIGURE 209. Statistic Schedule screen

- Time XX:XX collection - Determines when the statistics are collect, this is a globe setting for all statistics. Statistics can be collect as often as every fifteen minutes. Time is based on a 24hr clock and referenced to the IntelliVIEW server clock. 00:00 = midnight, 12:00 = noon etc.
- Clear All - Clears all selected collect times set

Statistics Configuration

- Collect - Enables or disables the collection of the statistics
- Collect and Reset - Enables or disables the collection of the statistics and whether to zero out the statistics value after each collection
- File Format - Choose from pull down menu, currently only CSV is supported
- Age days - number of days to keep the time stamped files. After days have expired the files will be deleted. Note the disk space required to store the file are not included in the system requirements. Each collection will create a zip file with the 16 files what make up the sum of statistics the devices assigned. Each device collect from will increase directory by 8K-bytes
- IntelliVIEW Repository Path - Local server file location default (statsCollection). If empty no statistics will be collected
- External Repository Path - (Supported on 2.0 and Higher) Identify the location of an external storage repository

Device Configuration (Node)

IntelliView provides a configuration application to configure a live device or an offline configuration.

The configurable objects are organized into hierarchical categories. When a user selects a category in the navigational pane, the category screen is loaded into the content (right) pane.

Note: Only categories for which the user has permissions to see, and for which the IntelliView installation is licensed, will show in the navigation pane.



FIGURE 210. Navigational pane

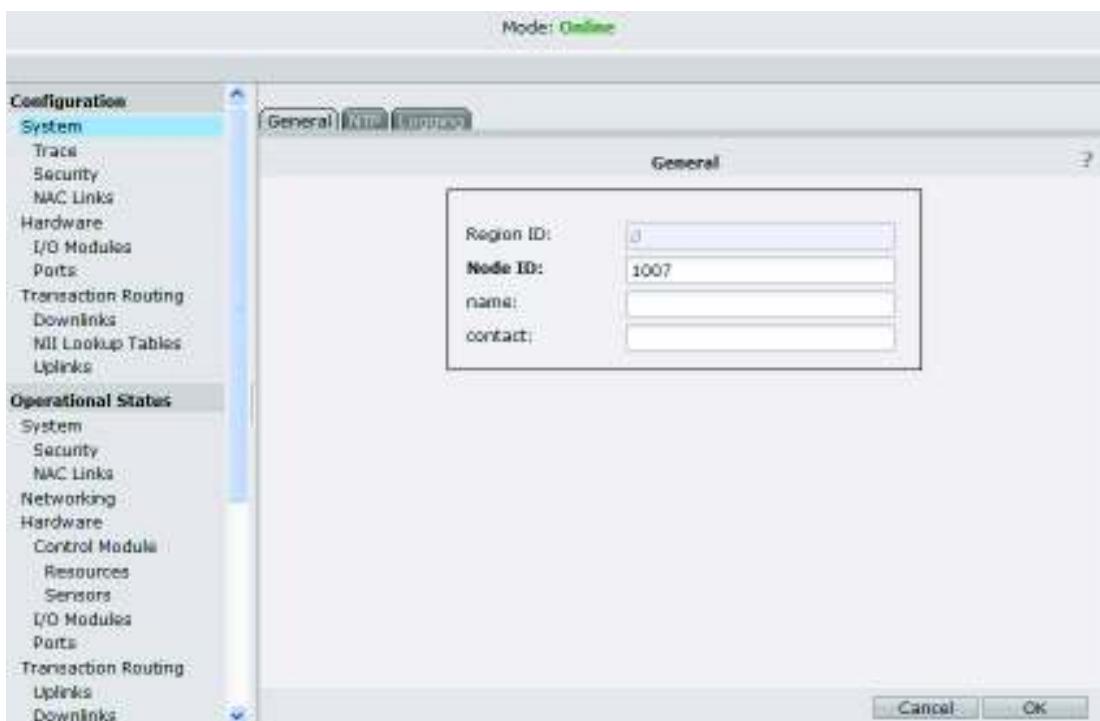
There are two types of device configurations that need to be managed, online and offline.

Online Device Configuration

This type of device configuration is currently on the IntelliNAC. This configuration is managed directly by sending configuration commands to the device. The configuration data operates on live objects. These objects have status and events (and sometimes statistics) associated with them. There will be some correlation between notifications from the device and configuration objects, based on their identity.

Configuring a Device

The configuration options are used to set up or modify an existing configuration. After selecting the device, the additional menu options appear on the toolbar. Click **Config App** and the following screen appears.

**FIGURE 211. Online Device Configuration**

The configuration options appear in the left pane and are divided into the following areas:

- System
- Hardware
- Transaction Routing

Click on the desired options to configure the device.

System

The System section contains configuration screens for trace, security and NAC links. These system-level functions involve interactions between the IntelliNAC or other-defined device and IntelliView.

Hardware

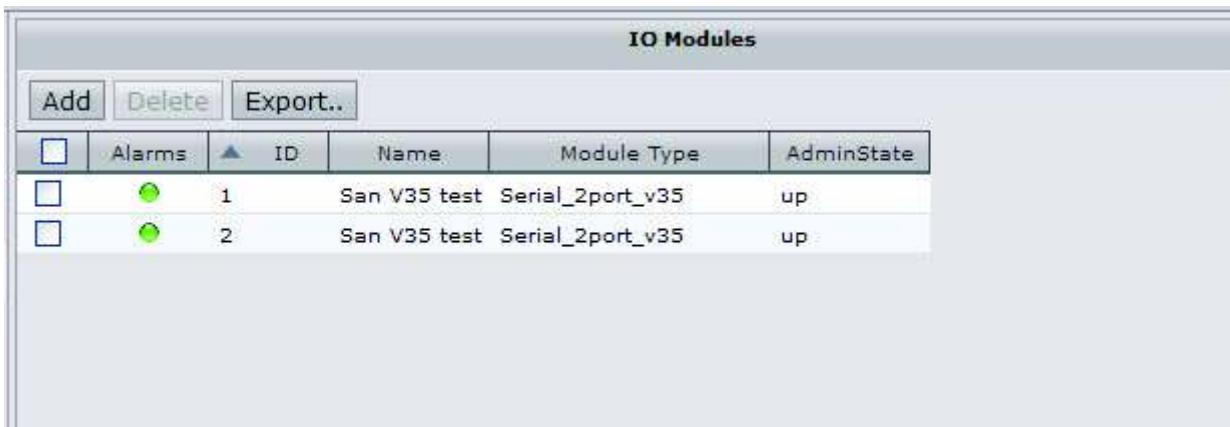
The Hardware section contains configuration screens for the I/O modules and device ports. Each must be defined and configured before they can be operational in the device.

Configuring an I/O Module

To configure an I/O module:

1. Select the device and click **Config App** on the toolbar. The System configuration screen appears.

2. In the left pane, click **I/O Modules** under Configuration > Hardware. The IO Modules screen appears.



	Alarms	ID	Name	Module Type	AdminState
<input type="checkbox"/>	●	1	San V35 test	Serial_2port_v35	up
<input type="checkbox"/>	●	2	San V35 test	Serial_2port_v35	up

FIGURE 212. IO Modules screen

3. Select a module from the listing or click **Add** to add a new module.
4. If you are adding a new module, the IO Module screen appears.



FIGURE 213. Add I/O Module

5. Enter the field information:
 - ID (select from pull-down, if not already populated)
 - Name (enter descriptive name for the module)
 - Module Type (select from the pull-down)
 - Admin State (this should be automatically populated)
6. Click **Create**.
7. If you are editing an existing module, select the module from the IO Modules listing and double-click. The IO Module screen appears.

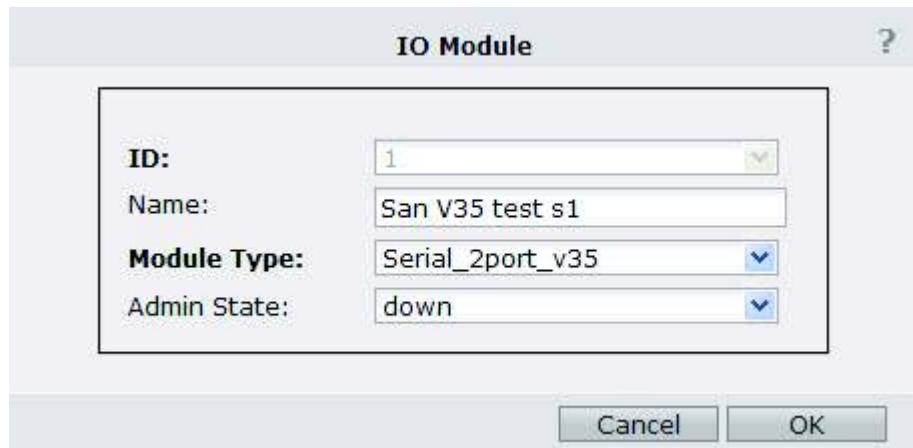


FIGURE 214. IO Module screen

8. Make your changes and click **OK**. The changes are noted in the IO Modules screen.

General Port Configuration Navigation

Note: Remember to configure a module first, before configuring a port.

To configure a device port:

1. Select the device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Ports** under Configuration > Hardware. The Ethernet Ports screen appears (default).



FIGURE 215. Ethernet Ports screen

3. Select the type of port by clicking the appropriate tab (Ethernet, ISDN PSTN, MFR2 PSTN, RBS PSTN, Analog PSTN, SNA Uplink, X25 Uplink, or X25 Downlink).

4. On the Ports screen, select the appropriate port from the listing or click **Add** to add a new port. For example, selecting the ISDN PSTN Port tab and clicking **Add**, displays the ISDN PSTN Port screen.



FIGURE 216. ISDN PSTN Port screen

5. Enter the field information:
 - Module ID
 - Port ID
 - Name (enter a descriptive port name)
 - Admin State (select an administrative state from the pull-down list)
6. Click **Create**.
7. If you selected a port from the listing, on the Port screen, make any changes and click **OK**. The changes will be noted on the Ports screen.

Ethernet Port Configuration

Note: Remember to configure a module first, before configuring a port.

To configure a Ethernet port:

1. Select the device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Ports** under Configuration > Hardware. The Ethernet Ports screen appears (default).

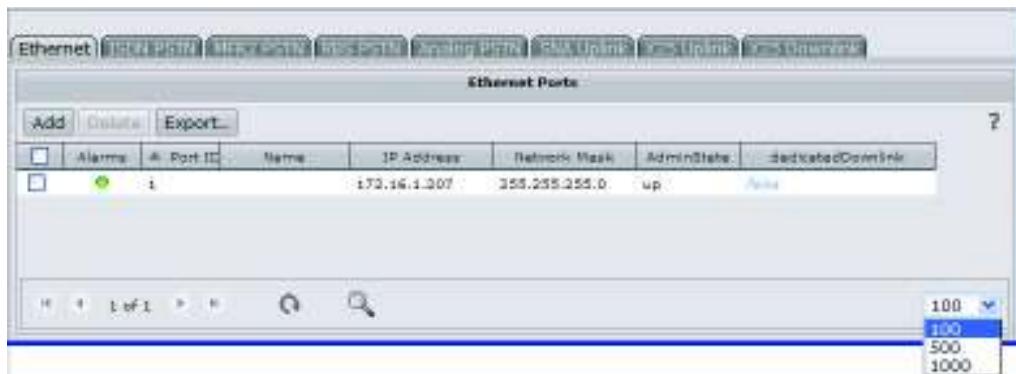


FIGURE 217. Ethernet Ports screen

3. On the Ports screen, select the appropriate port from the listing or click **Add** to add a new port.

Ethernet Port

Port ID:	<input type="text"/>
Name:	<input type="text"/>
IP Address:	<input type="text"/>
Network Mask:	<input type="text"/>
Admin State:	<input type="text" value="Default: up"/> 
Static Routes:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 150px; margin-top: 10px;"> </div>
Dedicated Downlink:	<input type="text" value="Default: false"/> 

FIGURE 218. Ethernet Ports Configuration screen

- Port ID (Enter the unique identifier for the port or select from pull-down list)
- Name (Enter descriptive name of port alphanumerics and standard special characters)
- IP Address (Enter IP address for the port xxx.xxx.xxx.xxx)
- Network Mask (Enter the IP subnet mask value - normally 255.255.255.0)
- Admin State (Set the operational state of the port once configured - default is enabled [up])
- Dedicated Downlink (Is the port going to be used as a downlink - default is uplink port)
- Static routes - click + to add a new static route or - to delete a static route

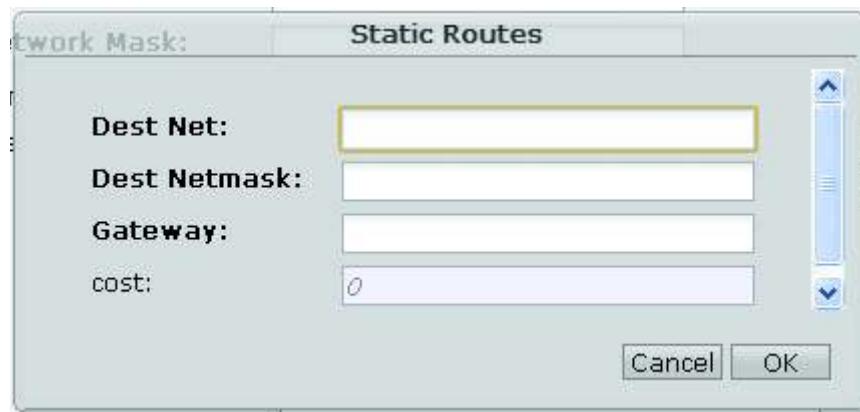


FIGURE 219. Ethernet Port Static Route configuration screen

- Dest Net (Enter a IP address on the destination network xxx.xxx.xxx.0)
 - Dest Netmask (Enter a Netmask for the destination network normally 255.255.255.0)
 - Gateway (Enter next hop IP Address xxx.xxx.xxx.xxx)
 - Cost (Enter a relative cost value from 1 through 128 where 1 equals least cost and 128 the most cost)
4. Click **OK**. The changes will be noted on the Ethernet Port screen.
 5. Click **Create**. The changes will be noted on the Ethernet Port tab.

ISDN PSTN Port Configuration

Note: Remember to configure a module first, before configuring a port.

To configure a ISDN PSTN port:

1. Select the device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Ports** under Configuration > Hardware.
3. In main screen click on ISDN PSTN tab
4. The ISDN PSTN Ports screen appears.

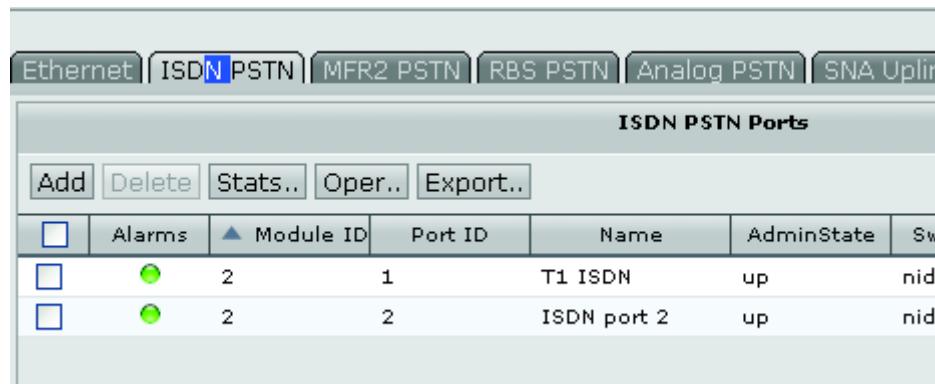


FIGURE 220. ISDN PSTN Ports screen

5. On the Ports screen, select the appropriate port from the listing or click **Add** to add a new port.

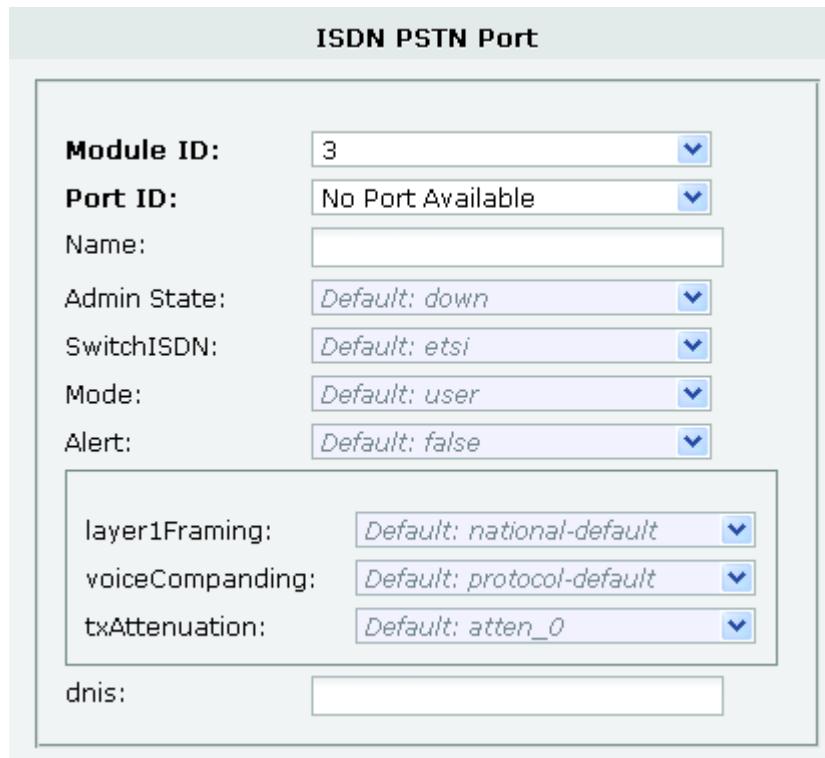


FIGURE 221. ISDN PSTN Port configuration screen

- Module ID (Select the module [card] of the port to be configured from pull down menu)
- Port ID (Select the port to be configured from pull down list)
- Name (Enter descriptive name of port alphanumerics and standard special characters)
- Admin State (Set the operational state of the port once configured - default is disabled [down])

- Switch ISDN (Select ISDN Switch type from pull down list) - see list below

Default:	etsi	4esdn
1tr6		4esds
etsi		4elds
france		4emgc
belgium		4emgi
sweden		hongkong
nidms		vn4_vn6
5ess		dss1-cn
japan		newzeal
atel		dss1-jp
italy		serbia
taiwan		
australia		

FIGURE 222. Switch types supported

- Mode (Select network mode type from pull down list) - Default: user or network
 - Alert (Select Alert enabled from pull down list) - Default: false no alert or true alert on error
 - Layer 1 Framing (Select Framing from pull down list) -
 - Default: National-default
 - national-default
 - double-framing
 - multi-framing
 - Voice Companding (Select from pull down list) -
 - Default: protocol-default (based on Switch type selected)
 - protocol-default (based on Switch type selected)
 - ALaw
 - uLaw
 - TX Attenuation (Select from pull down list) -
 - Default: atten_0db
 - atten_0db
 - atten_7.5db
 - atten_15db
 - DNIS (Enter a DNIS number for the port) Numeric only no spaces or hyphen
6. Click **OK**. The changes will be noted on the ISDN PSTN Port screen.

MFR2 PSTN Port Configuration

Note: Remember to configure a module first, before configuring a port.

To configure a MFR2 PSTN port:

1. Select the device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Ports** under Configuration > Hardware.
3. In main screen click on MFR2 PSTN tab
4. The MFR2 PSTN Ports screen appears.



FIGURE 223. MFR2 PSTN Ports screen

5. On the Ports screen, select the appropriate port from the listing or click **Add** to add a new port.

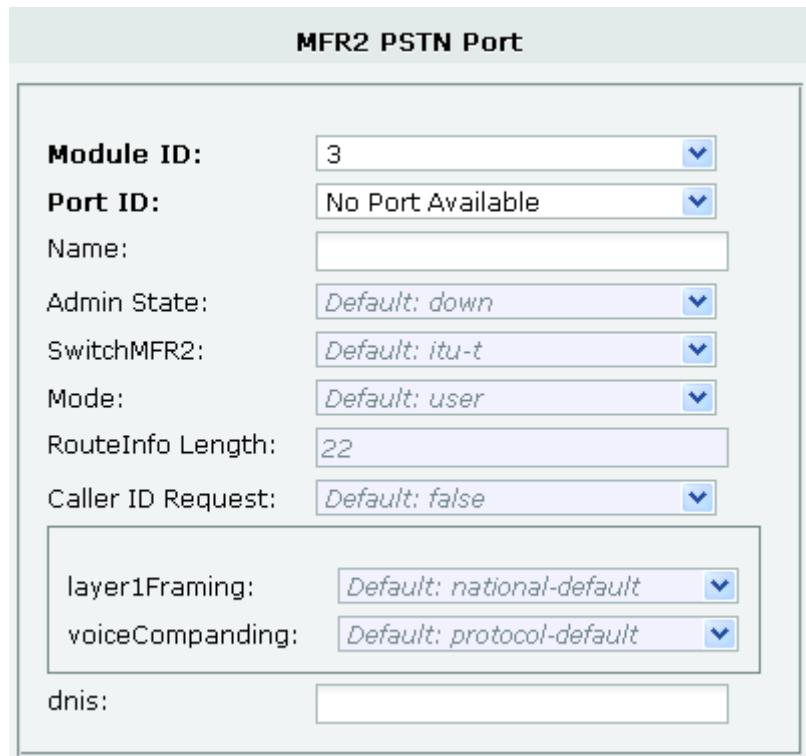


FIGURE 224. MFR2 PSTN Port configuration screen

- Module ID (Select the module [card] of the port to be configured from pull down menu)
- Port ID (Select the port to be configured from pull down list)
- Name (Enter descriptive name of port alphanumeric and standard special characters)
- Admin State (Set the operational state of the port once configured - default is disabled [down])
- Switch MFR2 (Select MFR2 Switch type from pull down list) - see list below



FIGURE 225. Switch types supported

- Mode (Select network mode type from pull down list) - Default: user (TE) or network (NT)
 - Route Info Length (Select number of routing digits from pull down list) - Default: 22 digits range 0 -22
 - Caller ID Request (Enable ANI collection) - Default: False do not collect ANI
 - Layer 1 Framing (Select Framing from pull down list) -
 - Default: National-default
 - national-default
 - double-framing
 - multi-framing
 - Voice Companding (Select from pull down list) -
 - Default: protocol-default (based on Switch type selected)
 - protocol-default (based on Switch type selected)
 - ALaw
 - uLaw
 - TX Attenuation (Select from pull down list) -
 - Default: atten_0db
 - atten_0db
 - atten_7.5db
 - atten_15db
 - DNIS (Enter a DNIS number for the port) Numeric only no spaces or hyphen
6. Click **OK**. The changes will be noted on the MFR2 PSTN Port screen.

RBS PSTN Port Configuration

Note: Remember to configure a module first, before configuring a port.

To configure a RBS PSTN port:

1. Select the device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Ports** under Configuration > Hardware.
3. In main screen click on RBS PSTN tab
4. The RBS PSTN Ports screen appears.

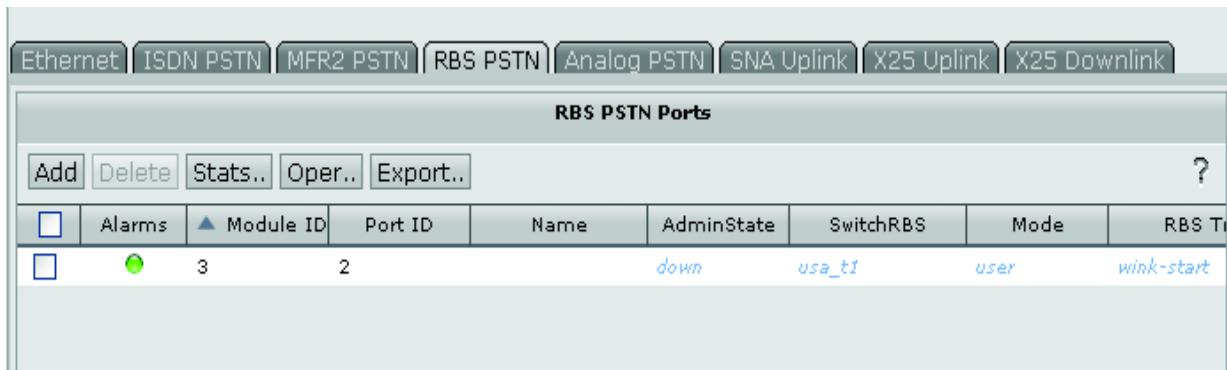


FIGURE 226. RBS PSTN Ports screen

5. On the Ports screen, select the appropriate port from the listing or click **Add** to add a new port.

A screenshot of the 'RBS PSTN Port' configuration dialog box. The title bar says 'RBS PSTN Port'. The form contains the following fields:

- Module ID:** A dropdown menu set to 3.
- Port ID:** A dropdown menu set to 2, which is highlighted with a yellow border.
- Name:** An empty text input field.
- Admin State:** A dropdown menu set to Default: down.
- switchRBS:** A dropdown menu set to Default: usa_t1.
- Mode:** A dropdown menu set to Default: user.
- RBSTrunkMode:** A dropdown menu set to Default: wink-start.
- ReceiveDigitTimeout:** A text input field containing the value 1.

layer1Framing:	Default: national-default
voiceCompanding:	Default: protocol-default
txAttenuation:	Default: atten_0

dnis: An empty text input field.

FIGURE 227. RBS PSTN Port configuration screen

- Module ID (Select the module [card] of the port to be configured from pull down menu)
- Port ID (Select the port to be configured from pull down list)

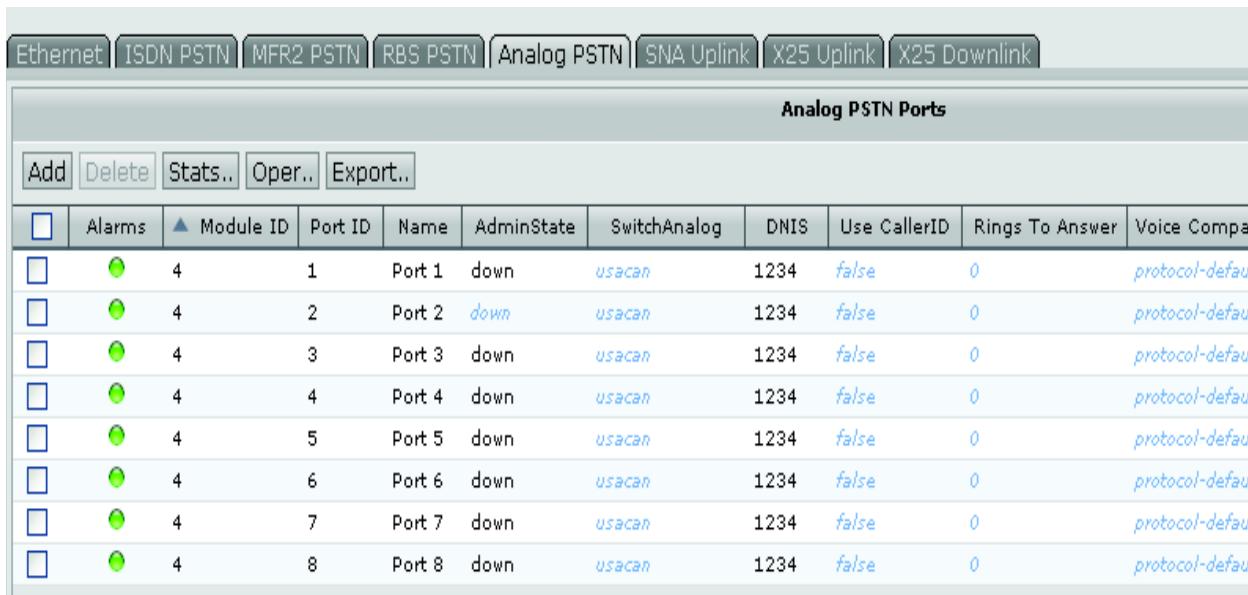
- Name (Enter descriptive name of port alphanumeric and standard special characters)
 - Admin State (Set the operational state of the port once configured - default is disabled [down])
 - Switch RBS (Only usa_t1 currently available)
 - Mode (Select network mode type from pull down list) - Default: user or network
 - RBS Trunk Mode (Select TrunkMode from pull down list) -
 - Default: wink-start
 - wink-start
 - loop-start
 - ground-start
 - Receive Digit Timeout - (DTMF digit timeout in seconds) - 1 to 60
 - Layer 1 Framing (Select Framing from pull down list) -
 - Default: National-default
 - national-default
 - double-framing
 - multi-framing
 - Voice Companding (Select from pull down list) -
 - Default: protocol-default (based on Switch type selected)
 - protocol-default (based on Switch type selected)
 - ALaw
 - uLaw
 - TX Attenuation (Select from pull down list) -
 - Default: atten_0db
 - atten_0db
 - atten_7.5db
 - atten_15db
 - DNIS (Enter a DNIS number for the port) Numeric only no spaces or hyphen
6. click **OK**. The changes will be noted on the RBS PSTN Port screen.

Analog PSTN Port Configuration

Note: Remember to configure a module first, before configuring a port.

To configure a Analog PSTN port:

1. Select the device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Ports** under Configuration > Hardware.
3. In main screen click on Analog PSTN tab
4. The Analog PSTN Ports screen appears.



The screenshot shows the 'Analog PSTN Ports' screen. At the top, there is a navigation bar with tabs: Ethernet, ISDN PSTN, MFR2 PSTN, RBS PSTN, Analog PSTN (which is selected and highlighted in blue), SNA Uplink, X25 Uplink, and X25 Downlink. Below the navigation bar is a toolbar with buttons: Add, Delete, Stats.., Oper.., and Export..

The main area is a table titled 'Analog PSTN Ports' with 8 rows. The columns are: Alarms, Module ID, Port ID, Name, AdminState, SwitchAnalog, DNIS, Use CallerID, Rings To Answer, and Voice Compa. Each row represents a port, and all ports are currently set to 'down'. The 'Name' column lists 'Port 1' through 'Port 8'. The 'AdminState' column shows 'down' for all ports. The 'SwitchAnalog' column shows 'usacan' for all ports. The 'DNIS' column shows '1234' for all ports. The 'Use CallerID' column shows 'false' for all ports. The 'Rings To Answer' column shows '0' for all ports. The 'Voice Compa' column shows 'protocol-defau.' for all ports.

Alarms	Module ID	Port ID	Name	AdminState	SwitchAnalog	DNIS	Use CallerID	Rings To Answer	Voice Compa
	4	1	Port 1	down	usacan	1234	false	0	protocol-defau.
	4	2	Port 2	<i>down</i>	usacan	1234	false	0	protocol-defau.
	4	3	Port 3	down	usacan	1234	false	0	protocol-defau.
	4	4	Port 4	down	usacan	1234	false	0	protocol-defau.
	4	5	Port 5	down	usacan	1234	false	0	protocol-defau.
	4	6	Port 6	down	usacan	1234	false	0	protocol-defau.
	4	7	Port 7	down	usacan	1234	false	0	protocol-defau.
	4	8	Port 8	down	usacan	1234	false	0	protocol-defau.

FIGURE 228. Analog PSTN Port Screen

5. On the Ports screen, select the appropriate port from the listing or click **Add** to add a new port.

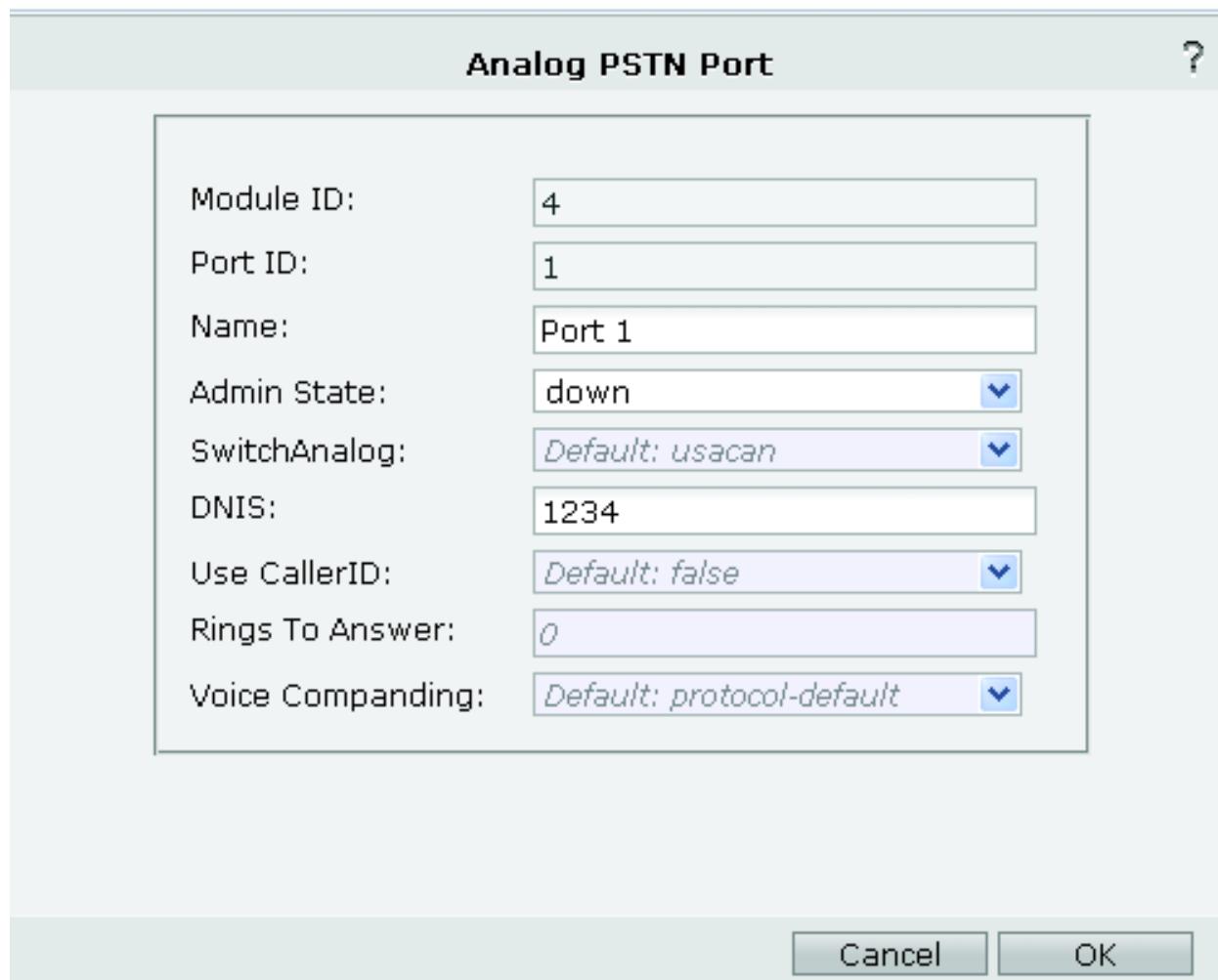


FIGURE 229. Analog PSTN Port configuration screen

- Module ID (Select the module [card] of the port to be configured from pull down menu)
- Port ID (Select the port to be configured from pull down list)
- Name (Enter descriptive name of port alphanumeric and standard special characters)
- Admin State (Set the operational state of the port once configured - default is disabled [down])

- Switch Analog - Telco Country Switch (Select PSTN Switch type from pull down list) - see list below

Default: usacan	taiwan
tbr21	safrica
usacan	bulgaria
denmark	croatia
sweden	czech
uae	estonia
netherlands	hungary
australia	latvia
japan	lithuania
unitedkingdom	poland
skorea	romania
china	slovakia
india	slovenia
malaysia	russia
singapore	thailand

- DNIS (Enter a DNIS number for the port) Numeric only no spaces or hyphen
- Use Caller ID (Select from pull down list) - Default false - Don't use caller ID
 - True use caller ID
- Rings To Answer (Enter the number of rings before answering) 0 through 1024
- Voice Companding (Select from pull down list) -
 - Default: protocol-default (based on Switch type selected)
 - protocol-default (based on Switch type selected)
 - ALaw
 - uLaw

Click **OK**. The changes will be noted on the Analog PSTN Port screen.

SNA Uplink Port Configuration

Note: Remember to configure a module first, before configuring a port.

To configure a SNA Uplink port:

1. Select the device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Ports** under Configuration > Hardware.
3. In main screen click on SNA Uplink tab
4. The SNA Uplink Ports screen appears.

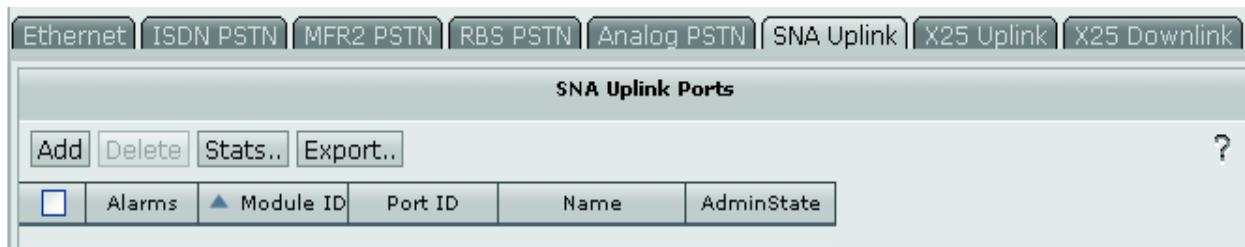


FIGURE 230. SNA Uplink Ports screen

5. On the Ports screen, select the appropriate port from the listing or click **Add** to add a new port.

SNA Uplink Port

Module ID:	4
Port ID:	1
Name:	SNA M4P1 7F
Admin State:	down

SNA Serial Line SDLC

sna3270Header:	Default: false
snaIncludePosTpdu:	false
snaInitSelf:	true
snaDluName:	LU0 M/T
snaUserData:	SNA M4P1
snaInsertPos1Hdr:	Default: false
snaLu0Multithread:	Default: false
snaLu0Pairing:	Default: false
snaLu2Bracket:	Default: false
snaHostFormat:	Default: SNA_ASCII
snaTermFormat:	Default: TERM_ASCII
snaStartingLu:	2
snaThOutSegmentSize:	256

FIGURE 231. SNA Uplink Port configuration screen

- Module ID (Select the module [card] of the port to be configured from pull down menu)
- Port ID (Select the port to be configured from pull down list)
- Name (Enter descriptive name of port alphanumeric and standard special characters)
- Admin State (Set the operational state of the port once configured - default is disabled [down])



FIGURE 232. SNA Protocol configuration Tab

- SNA 3270 Header (Insert 3270 header in the SAN Message) From Pull down to select
 - Default: False no header insertion
 - True insert 3270 header
- SNA Include POS TPDU (Insert 5 byte POS TPDU in the SANA message) From Pull down to select
 - Default: False no TPDU insertion

- True insert TPDU header

Note - Must be set True if LU0 multi-threaded is selected

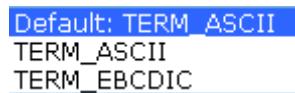
- SNA Init Self (Send INIT-SELF every 3 minutes to the host after ACTLU till SNA bind received) From Pull down to select
 - Default: False INIT-SELF to host
 - True send INIT-SELF to Host
- SNA DLU Name - Enter up to 8 characters (0-9, a-z, A-Z, Space)
- SNA User Data - Enter up to 8 characters (0-9, a-z, A-Z, Space)
- SNA Insert POS1 Header (prefix POS1 to outbound SNA message) From Pull down select
 - Default: False No POS1
 - True send POS1
- SNA LU0 Multi-threading (LU0 multi-threading and TPDU insertion)
 - Default: False (multi-threading not enabled)
 - True (multi-threading enabled)
- SNA LU0 Pairing (LU0 pairing)
 - Default: False (No LU0 pairing)
 - True (LU0 pairing enabled)

Note - Starting LU is configured separately

- SNA LU2 Bracket (LU2 Bracket mode control)
 - Default: False (LU2 Bracket mode disabled)
 - True (LU2 Bracket mode enabled)
- SNA Host Format (SNA host data format) select format from pull down menu



- SNA Terminal Format (Terminal data format) select format from pull down menu



- SNA Starting LU (Starting LU number - default value is 2) max value 65535
- SNA TX out segment (Maximum size of outbound header - default is 256 bytes) max value

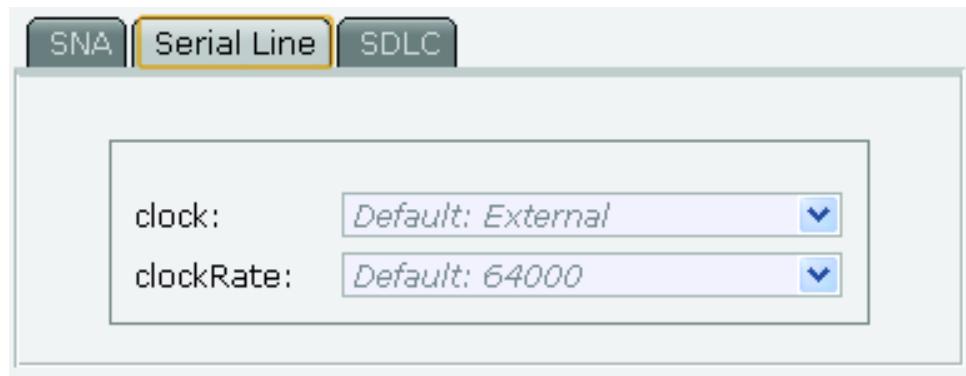
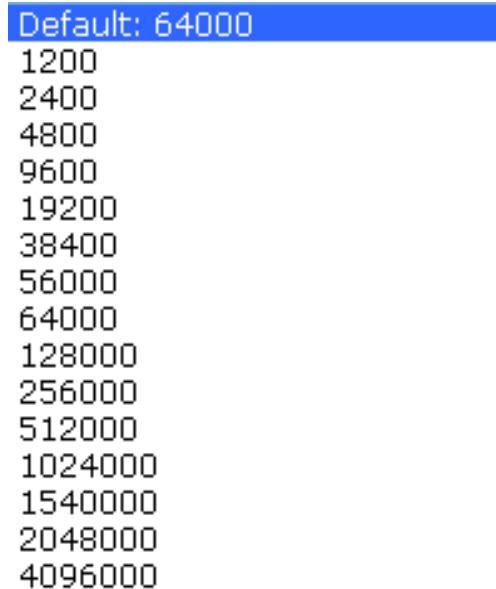


FIGURE 233. SNA Serial configuration Tab

- Clock (Serial Clock source) - Default External clock reference (DCE)
 - Internal provided clock source (DTE)
- Clock Rate (Internal Serial clock baud rate) -Select from pull down menu
 - Default 64000Kbs



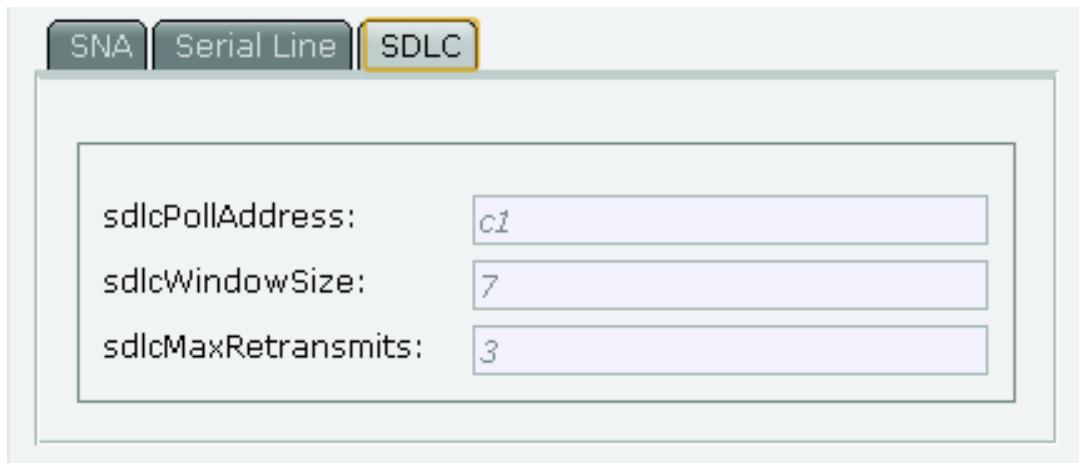


FIGURE 234. SNA SDLC configuration Tab

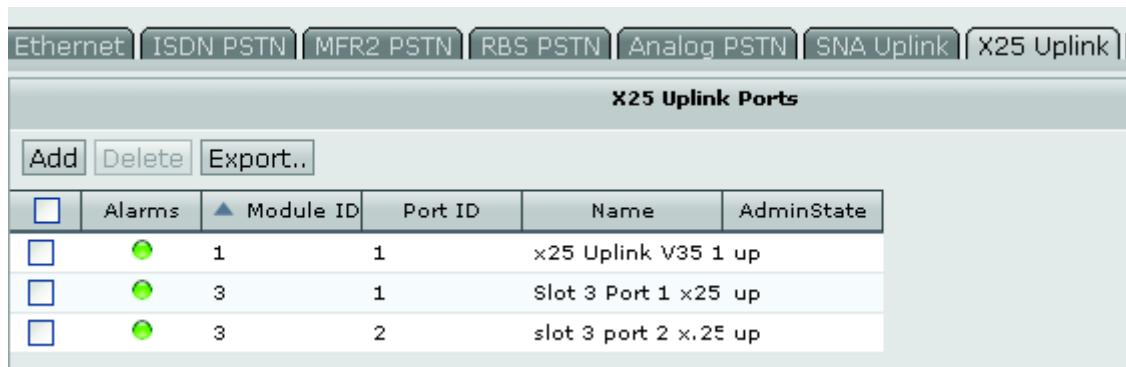
- SDLC Poll Address (SDLC station address) Must be a hexadecimal value - Default is 0XC1
 - SDLC window size (Number of SDLC frames chained) Default is 7
 - SDLC Max Retransmits (Maximum number of retransmissions) Default is 3
6. Click **OK**. The changes will be noted on the SNA Uplink Port screen.

X.25 Uplink Port Configuration

Note: Remember to configure a module first, before configuring a port.

To configure a X.25 Uplink port:

1. Select the device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Ports** under Configuration > Hardware.
3. In main screen click on X.25 Uplink tab
4. The X.25 Uplink Ports screen appears.



The screenshot shows a software interface for managing X.25 Uplink ports. At the top, there is a horizontal menu bar with several tabs: Ethernet, ISDN PSTN, MFR2 PSTN, RBS PSTN, Analog PSTN, SNA Uplink, and X25 Uplink. The X25 Uplink tab is currently selected. Below the menu is a sub-menu titled "X25 Uplink Ports". Underneath this, there is a toolbar with three buttons: "Add", "Delete", and "Export..". The main area is a table listing three X.25 uplink ports. The columns are labeled: Alarms, Module ID, Port ID, Name, and AdminState. The data in the table is as follows:

Alarms	Module ID	Port ID	Name	AdminState
	1	1	x25 Uplink V35 1 up	
	3	1	Slot 3 Port 1 x25 up	
	3	2	slot 3 port 2 x.25 up	

FIGURE 235. X.25 Uplink Ports screen

5. On the Ports screen, select the appropriate port from the listing or click **Add** to add a new port.



FIGURE 236. X.25 Uplink Port configuration screen

- Module ID (Select the module [card] of the port to be configured from pull down menu)
- Port ID (Select the port to be configured from pull down list)
- Name (Enter descriptive name of port alphanumeric and standard special characters)
- Admin State (Set the operational state of the port once configured - default is disabled [down])

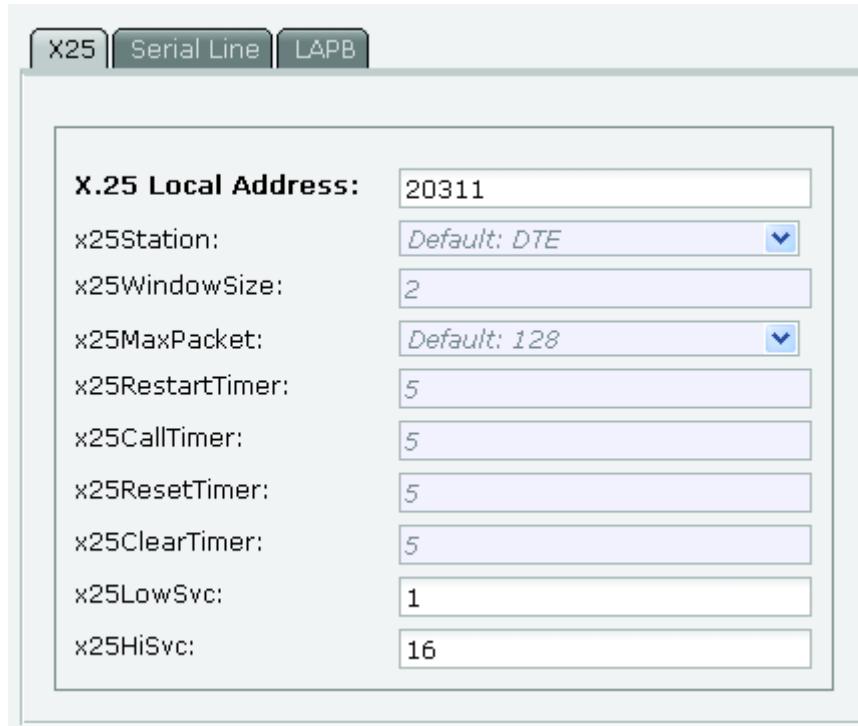


FIGURE 237. X.25 Protocol configuration Tab

- X.25 Local Address (X.121 IDN Format - up to 14 digits) Numeric only 0 - 9
- X25 Station (Logical station type) From Pull down to select
 - Default DTE (Data terminal equipment)
 - DCE (Data communications Equipment)
- X25 window size (Transmit and receive widow size ala number of chained frames) Default is 2, maximum is 7
- X25 Max Packet - (Maximum number of bytes in a receive or transmit packet) Default is 128 bytes to a maximum of 65535 bytes
- X25 Restart Timer - (X25 T10 timer in seconds) Default is 5 seconds
- X25 Call timer - (X25 T11 timer in seconds) Default is 5 seconds
- X25 Reset timer - (X25 T12 timer in seconds) Default is 5 seconds
- X25 Clear timer - (X25 T13 timer in seconds) Default is 5 seconds
- X25 Low Service (Lowest number of switched virtual circuit) Default is 1 circuit

Configuration

- X25 Highest Service (Highest number of switched virtual circuit) Default is 16 circuits must be greater than Low Service circuit value

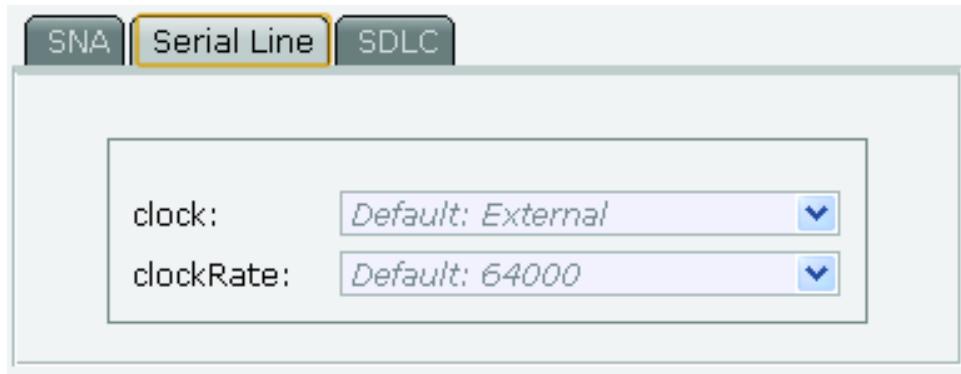


FIGURE 238. X.25 Serial configuration Tab

- Clock (Serial Clock source) - Default External clock reference (DCE)
 - Internal provided clock source (DTE)
- Clock Rate (Internal Serial clock baud rate) -Select from pull down menu
 - Default 64000Kbs

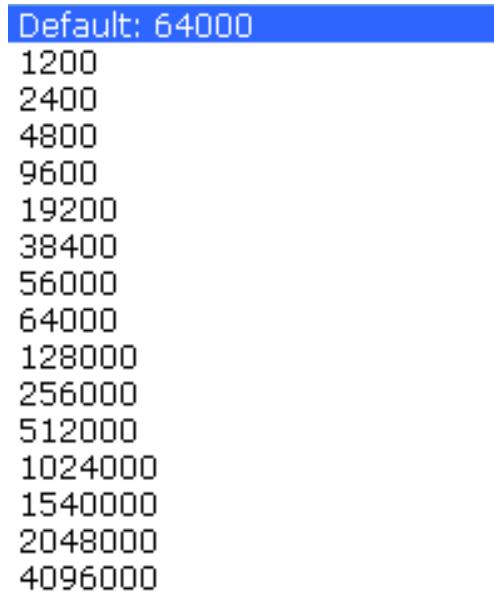


FIGURE 239. X.25 LAPB configuration Tab

- LAPB Station mode (Logical station mode) From Pull down to select

- Default DTE (Data terminal equipment)
- DCE (Data communications Equipment)
- LAPB window size (Number of SDLC frames chained) Default is 7
- LAPB Retransmit Timer (LAPB T1 timer in seconds) Default is 5 seconds
- LAPB Max Retransmits (Maximum number of retransmissions) Default is 3
- LAPB Idle RR Timer (LAPB T4 timer in seconds) Default is 15 seconds

Click **OK**. The changes will be noted on the X.25 Uplink Port screen.

X.25 Down Link Port Configuration

Note: Remember to configure a module first, before configuring a port.

To configure a X.25 Down link port:

1. Select the device and click **Config App** on the toolbar. The System configuration screen appears.
2. In the left pane, click **Ports** under Configuration > Hardware.
3. In main screen click on X.25 Down link tab
4. The X.25 Down link Ports screen appears.

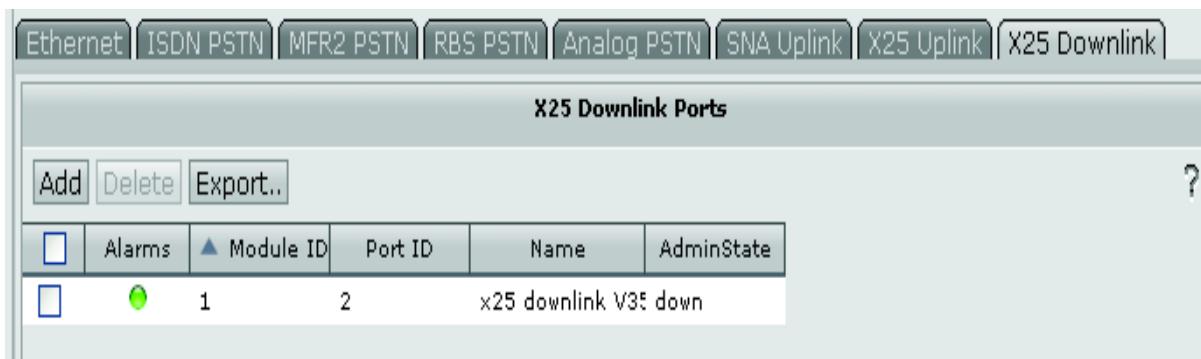


FIGURE 240. X.25 Down link Ports screen

5. On the Ports screen, select the appropriate port from the listing or click **Add** to add a new port.

TCP/IP Downlink

Address:	172.16.1.210
Port:	1221
Name:	172..210:1221
Enable:	true
SSL:	<i>Default: false</i>
Length Field Format:	hex
Include Length Field in Length:	<i>Default: false</i>
Certificate:	
Private Key:	
Password:	
Mutual Authentication:	<i>Default: false</i>

FIGURE 241. X.25 Down Link Port configuration screen

- Module ID (Select the module [card] of the port to be configured from pull down menu)
- Port ID (Select the port to be configured from pull down list)
- Name (Enter descriptive name of port alphanumeric and standard special characters)
- Admin State (Set the operational state of the port once configured - default is disabled [down])

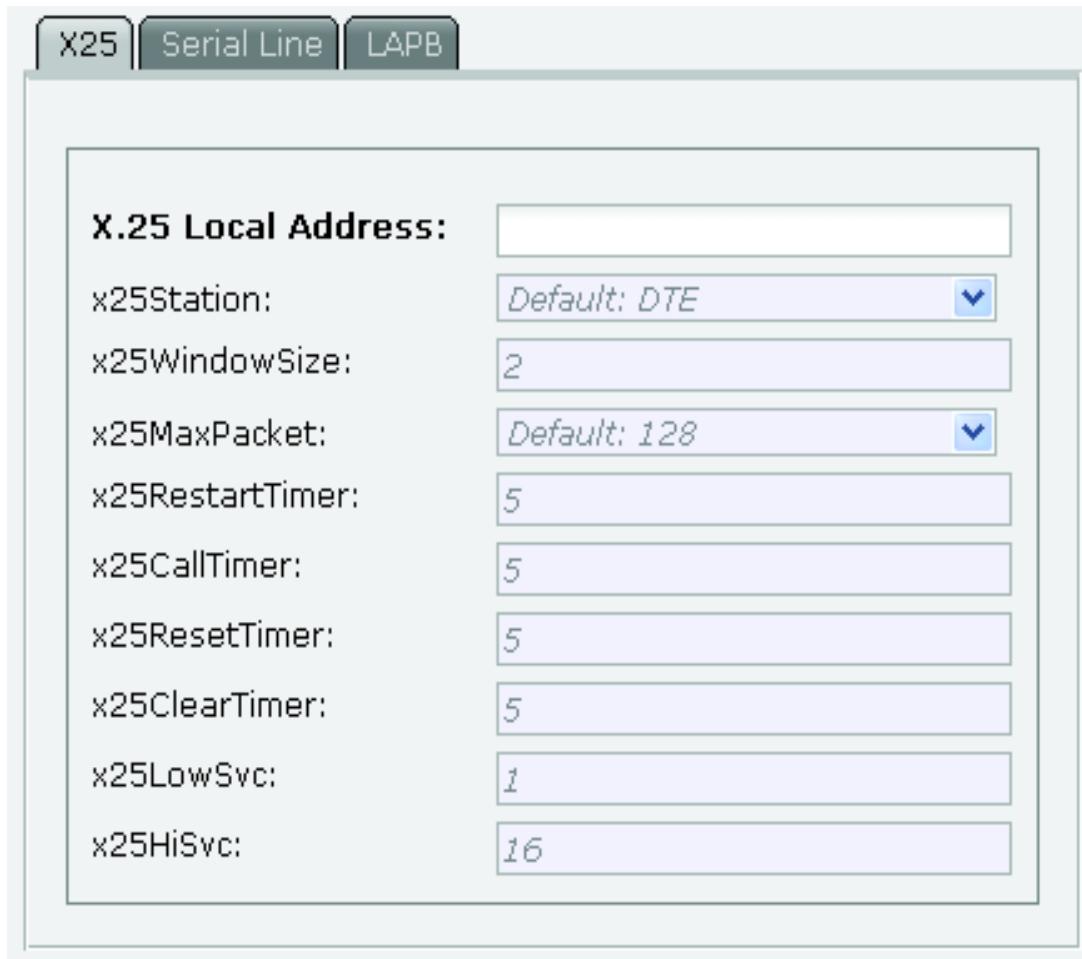


FIGURE 242. X.25 Protocol configuration Tab

- X.25 Local Address (X.121 IDN Format - up to 14 digits) Numeric only 0 - 9
- X25 Station (Logical station type) From Pull down to select
 - Default DTE (Data terminal equipment)
 - DCE (Data communications Equipment)
- X25 window size (Transmit and receive widow size ala number of chained frames) Default is 2, maximum is 7
- X25 Max Packet - (Maximum number of bytes in a receive or transmit packet) Default is 128 bytes to a maximum of 65535 bytes

- X25 Restart Timer - (X25 T10 timer in seconds) Default is 5 seconds
- X25 Call timer - (X25 T11 timer in seconds) Default is 5 seconds
- X25 Reset timer - (X25 T12 timer in seconds) Default is 5 seconds
- X25 Clear timer - (X25 T13 timer in seconds) Default is 5 seconds
- X25 Low Service (Lowest number of switched virtual circuit) Default is 1 circuit
- X25 Highest Service (Highest number of switched virtual circuit) Default is 16 circuits must be greater than Low Service circuit value

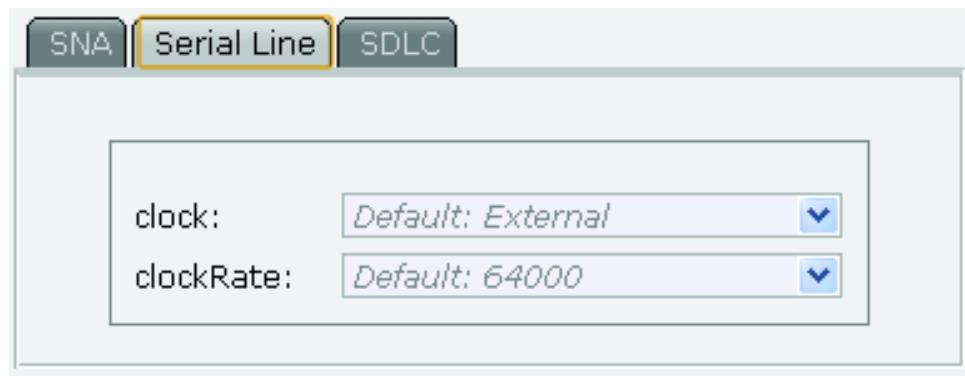
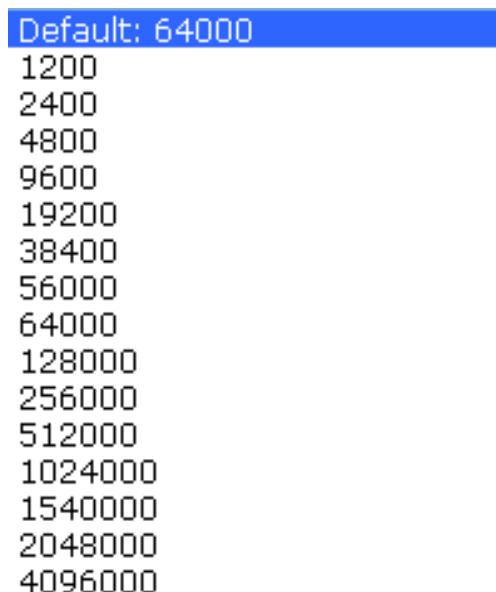


FIGURE 243. X.25 Serial configuration Tab

- Clock (Serial Clock source) - Default External clock reference (DCE)
 - Internal provided clock source (DTE)
- Clock Rate (Internal Serial clock baud rate) -Select from pull down menu
 - Default 64000Kbs



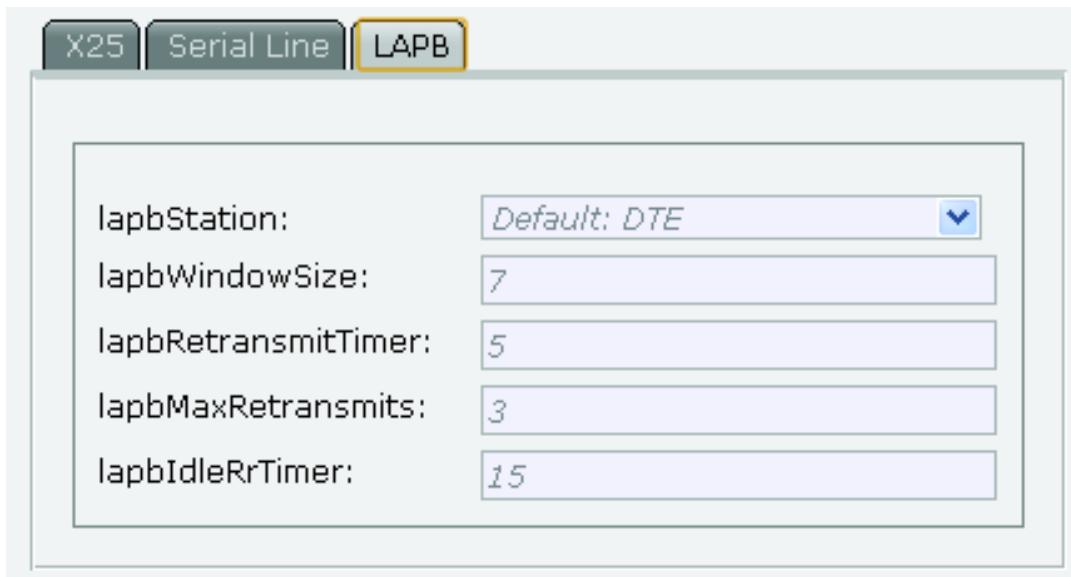


FIGURE 244. X.25 LAPB configuration Tab

- LAPB Station mode (Logical station mode) From Pull down to select
 - Default DTE (Data terminal equipment)
 - DCE (Data communications Equipment)
- LAPB window size (Number of SDLC frames chained) Default is 7
- LAPB Retransmit Timer (LAPB T1 timer in seconds) Default is 5 seconds
- LAPB Max Retransmits (Maximum number of retransmissions) Default is 3
- LAPB Idle RR Timer (LAPB T4 timer in seconds) Default is 15 seconds

Click **OK**. The changes will be noted on the X.25 Down link Port screen.

Transaction Routings

The device uplinks, downlinks, and NII lookup tables are defined in these screens. These are important in defining the transaction routes.

TCP/IP Downlinks Configuration

To configure a TCP/IP downlink:

1. On the Config App screen, under Transaction Routing (in the left pane), click **Downlinks**. The TCP/IP Downlinks screen appears (default).



FIGURE 245. Downlinks Configuration screen

2. Click on the TCP/IP TAB.
3. Select a downlink on the listing or click **Add**. The TCP/IP Downlink screen appears.

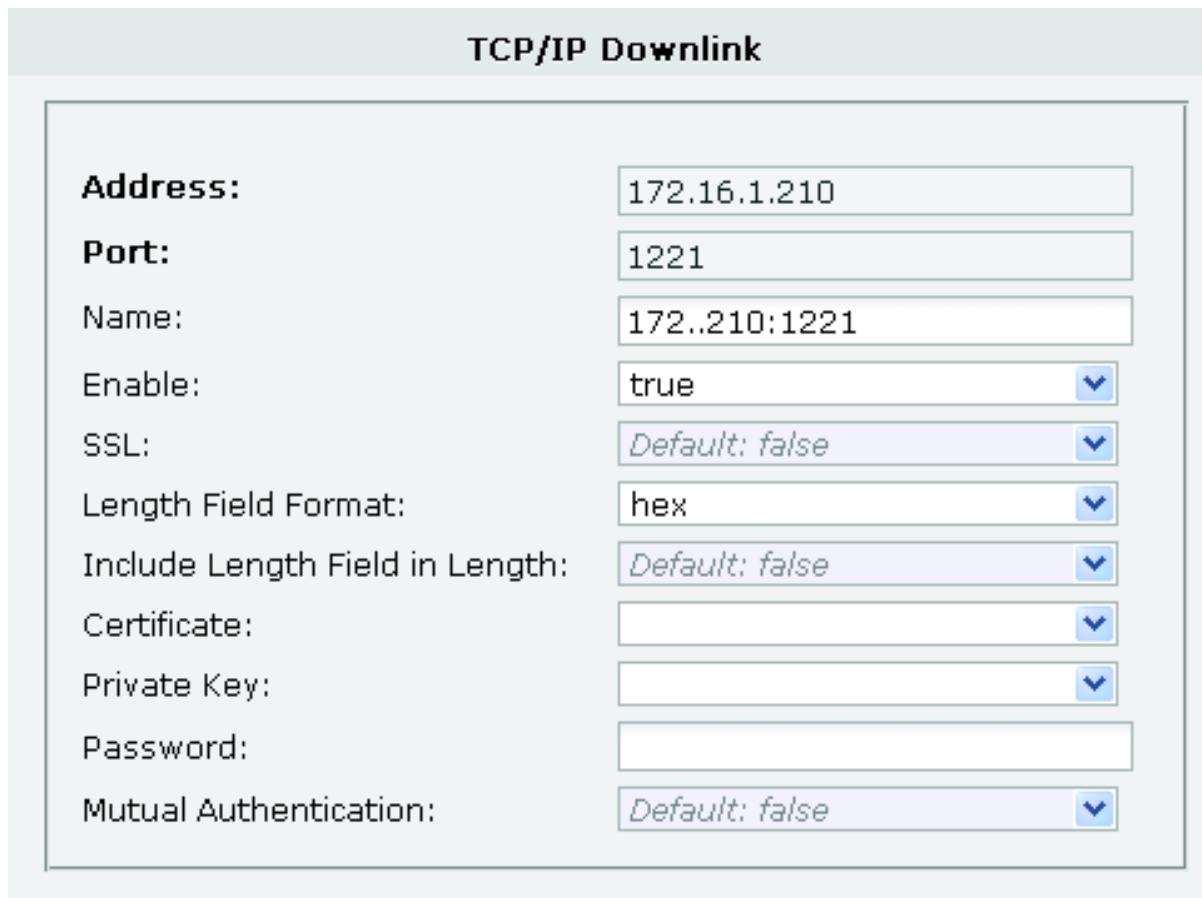
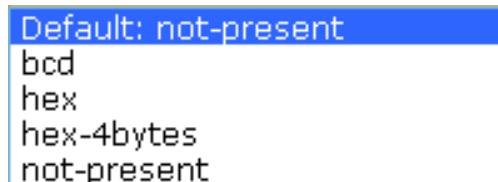


FIGURE 246. TCP/IP Downlink screen

4. Enter the field information:

- Address (enter new IP address if different) Format is 123.123.123.123
- Port (enter port id)
- Name (enter descriptive name of port downlink) up to 128 characters
- Enable (select whether calls will be accepted for this downlink from pull-down list) Default is enabled
- SSL (identify whether SSL security is used for the interface from the pull-down list) Default is disabled
- Length Field Format (specify whether a 2- or 4-byte length and its format is present) Select from pull down menu - Default is not present



- Include Length Field Format (select true or false from pull-down, identifying whether length field is included in the length calculation)
 - Certificate (select the applicable security certificate from the pull-down list)
 - Private Key (select the related security key from the pull-down list)
 - Password (enter the related pass-phrase associated with certificate key selected)
 - Mutual Authentication (enable the uses of mutual authentication on the interface) Default is disabled
5. Click **OK** to create entry.

PSTN Downlinks Configuration

To configure a PSTN downlink:

1. On the Config App screen, under Transaction Routing (in the left pane), click **Downlinks**. The TCP/IP Downlinks screen appears (default).



FIGURE 247. Downlinks Configuration screen

2. Click on the PSTN TAB.

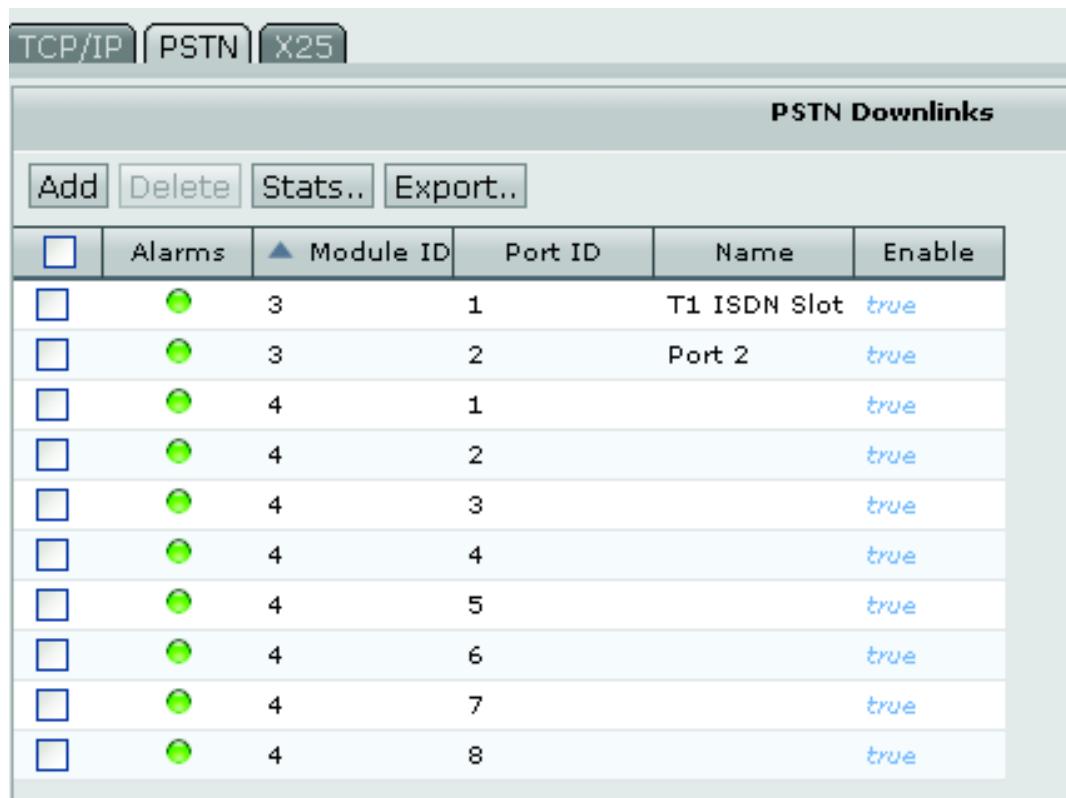


FIGURE 248. PSTN Downlink screen

3. Select a downlink on the listing or click **Add**. The PSTN Downlink screen appears.

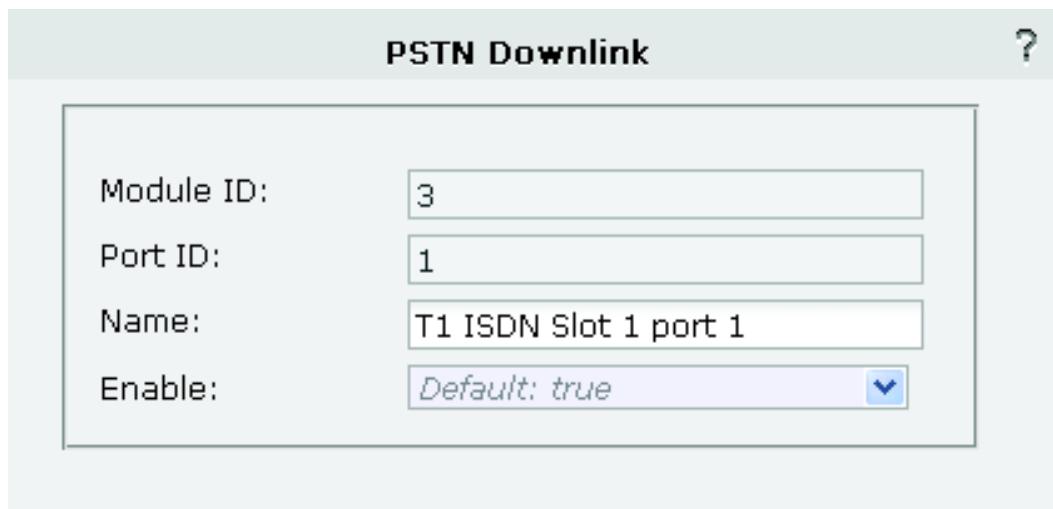


FIGURE 249. PSTN Downlink configuration screen

4. Enter the field information:

- Module ID (If adding select from pull down menu of available Modes)
- Port (If adding select from pull down menu of available Ports)
- Name (enter descriptive name of port downlink) up to 128 characters
- Enable (select whether calls will be accepted for this downlink from pull-down list) Default is enabled

X.25 Downlinks Configuration

To configure a X.25 downlink:

1. On the Config App screen, under Transaction Routing (in the left pane), click **Downlinks**. The TCP/IP Downlinks screen appears (default).



FIGURE 250. Downlinks Configuration screen

2. Click on the X.25 TAB.

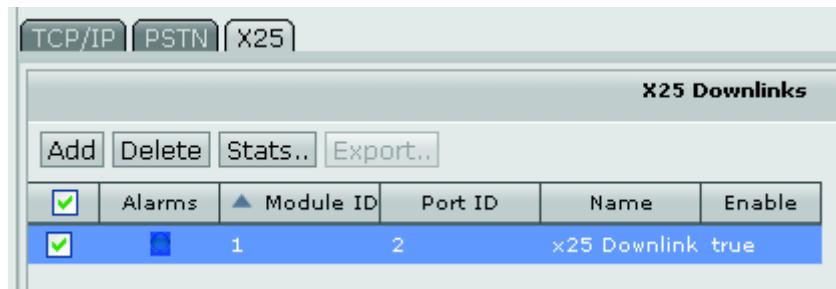


FIGURE 251. X.25 Downlink screen

3. Select a downlink on the listing or click **Add**. The X.25 Downlink screen appears.

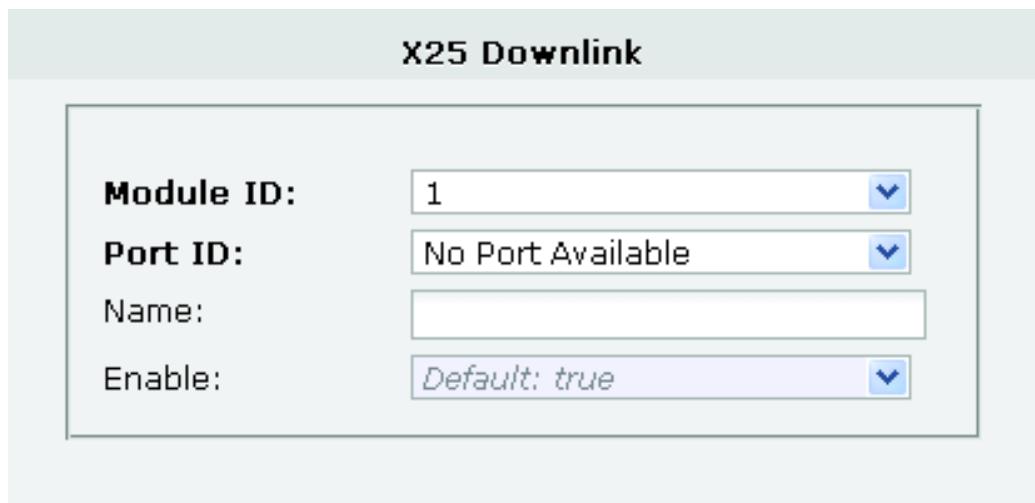


FIGURE 252. X.25 Downlink configuration screen

4. Enter the field information:

- Module ID (If adding select from pull down menu of available Modes)
- Port (If adding select from pull down menu of available Ports)
- Name (enter descriptive name of port downlink) up to 128 characters

Enable (select whether calls will be accepted for this downlink from pull-down list) Default is enabled

NII Lookup Tables Configuration

TCP/IP NII Table Configuration

To configure an NII lookup table:

1. On the Config App screen, under Transaction Routing (in the left pane), click on NII Lookup Tables. The TCP/IP screen appears (default).

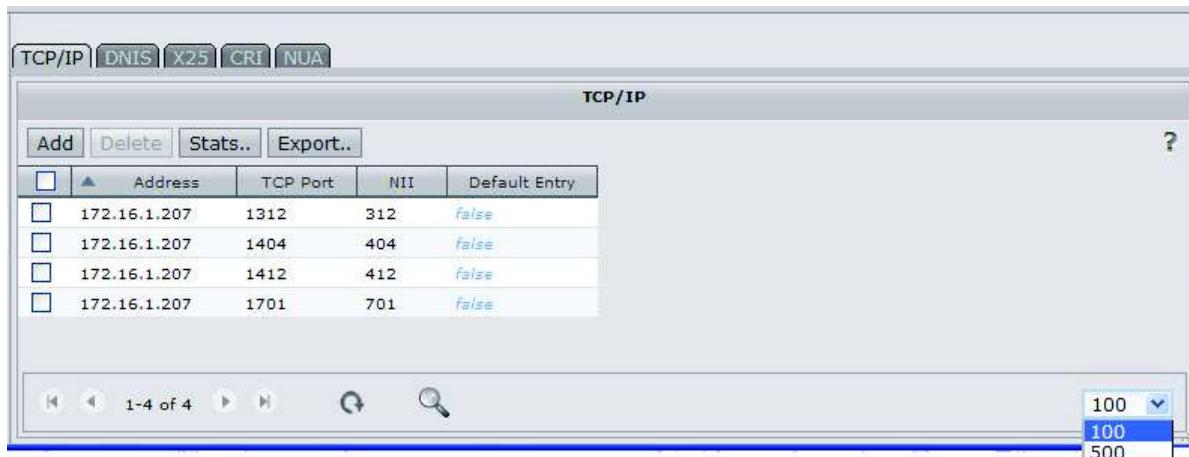
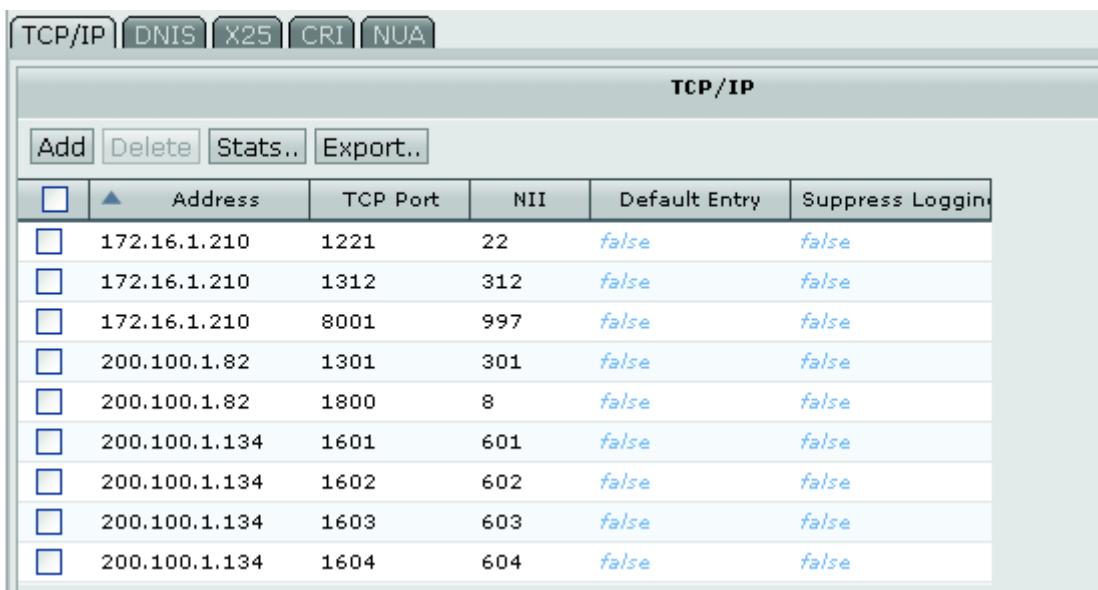


FIGURE 253. TCP/IP NII screen

2. Click on the TCP/IP TAB.
3. Select a downlink on the listing or click **Add**. The TCP/IP Downlink screen appears.



Transaction Routings

FIGURE 254. TCP/IP NII Configuration screen

4. Select a lookup table from the listing or click **Add**. The TCP/IP NII screen appears.

TCP/IP

Main	Options
Address: 172.16.1.210 TCP Port: NII: Default Entry: Default: false <input type="checkbox"/> Override Default entry Suppress Logging: Default: false	Routing Options EFTSec routingType: Default: this-nii overwriteNii: Default: false lastResortNii: 0

Protocol Options

Visa	Send DNIS Alarm	Term Master
Maximum Request Size: 2048 Inactivity Timer: 180000 Host Response Timer: 60000 Maximum Retransmissions: 3 Retransmission Timer: 3000 POS Protocol: Default: auto-pos Transaction Portal Protocol: Default: false Apply CINP Action: Default: false ANI Tagging: Default: disable Permanent Connection: Default: false	mode: Default: spoofed Transaction Reversal: Default: false interChunkTimer: 500 stripControlChars: Default: all stripParity: true maximumSpoofedEnqs: 5 initialEnqDelay: 800 secondEnqDelay: 3000 subsequentEnqDelay: 3000 expectHostEnq: Default: true delayToEot: 200 forceVisaMultiTrans: Default: false vericentreMode: Default: false hostDownOptions: Default: eot	

FIGURE 255. TCP/IP NII Lookup Table screen

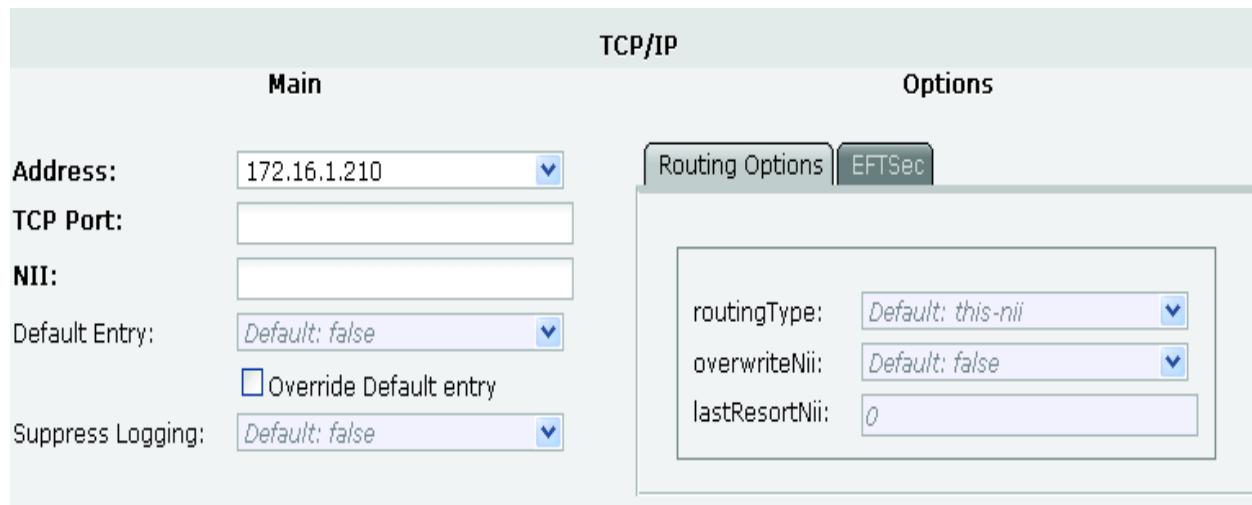
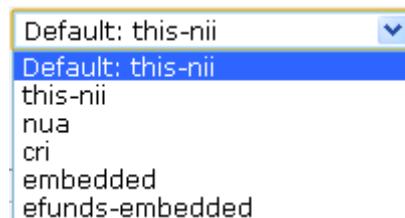


FIGURE 256. Upper part of TCP/IP NII Lookup Table screen

- Address (Select ports IP address to configured from pull down menu)
 - TCP Port (Enter TCP port to be used)
 - NII (enter routing NII for this entry)
 - Default Entry (you can choose to use the default information or enter a value from the pull-down list and select the Override Default entry option) Default is false
 - Suppress Logging (Enable NII logging records for this table) Default is disabled
- Routing Options:
- Routing Type (select the routing type from the pull-down list) Default is “this-nii”



- Overwrite Nii (select whether to overwrite the NII) Default is disabled (false)
 - Last Resort Nii (enter alternate NII table to use if current NII table or backup NII table are not available)
- EFTSec
- Enable (Enable EFTSec for this NII table configuration) Default is disabled (false)
 - Non-Encrypted Transaction Action (If EFTSec is enabled and a non-encrypted transaction is received what action should be preformed) Default is unset

```

unset
unset
enable-with-alarm
enable-without-alarm
disable-with-alarm
disable-without-alarm

```

Protocol Options (most of these fields are pre-filled with default values)

The screenshot shows a configuration interface titled "Protocol Options". On the left, there is a list of protocol options with their current values or default settings:

- Maximum Request Size: 2048
- Inactivity Timer: 10000
- Host Response Timer: 30000
- Maximum Retransmissions: 3
- Retransmission Timer: 3000
- POS Protocol: iso8583
- Transaction Portal Protocol: Default: false
- Apply CINP Action: Default: false
- ANI Tagging: Default: disable
- Permanent Connection: Default: false

On the right side, there is a vertical sidebar with several items listed:

- VISA
- mode
- Trans
- interC
- stripC
- stripF
- maxir
- initial
- secor
- subset
- expect
- ...

FIGURE 257. Protocol Options of TCP/IP NII Lookup Table screen

- Maximum Request Size (TCP Request Size in bytes) Default is 2048 Maximum value is 65535

Note: For CRI routed as a VISA transaction the value must set to 900

- Inactivity Timer (The timer determines the disconnect time with the protocol does not provide a disconnect) Value is in seconds Default is 180000 seconds
 - VISA Transparent and Fully transparent connection with no determined protocol
 - CRI Interleaved authorizations

- Multi-threaded transactions

Note: The timer is reset on either transmit or receive messages

- Host Response Timer (Timer use when Host response is expected) Value is in seconds - Default is 6000 seconds

Note: Under certain conditions a host response is expect: like a transaction which a non-trailer block is sent

- Max Retransmits (Maximum number of retransmissions) Default is 3

Note: Only used with Non-transparent transactions

- Retransmission Timer (The timer starts after the transmission of the response and stopped at the start of the acknowledgment reception) Value is in seconds Default is 3000 seconds
- POS Protocol (The protocol can be auto detected or set for a specific POS protocol) Select from the pull down menu - Default is "auto-pos"

Default: auto-pos
auto-pos
apacs
modified-async-gsm
term-master
visa
iso8583
none

- Transaction Portal Protocol (Enables Risk Management) Default is False (Disabled)
- Apply CINP Action (ISO8473 Connectionless protocol) Default is False (Disabled)

Note: Only used with X.25 and TCP/IP

- ANI Tagging (Enable prefixing ANI and DNIS information on the transaction request) Select from pull down menu - Default is false (disabled)

Default: disable
disable
enable
enable-with-lri-header

Note: Only used with PSTN

- Permanent Connection (Down link connection to the terminal that is not disconnected) Default is false (disabled)

Note: A variety of multi-threaded transaction, each with a unique transaction ID can exist within a single permanent connection. Each unique transaction will have it's own inactivity timer and can generate a unique down link statistic.

**FIGURE 258. TCP/IP NII Visa protocol tab**

- Mode (VISA protocol mode) Select from pull down menu - Default is spoofed

Default: spoofed

spoofed
transparent
fully-transparent

- Transaction Reversal (Enable transaction reversal message protocol) - Default is false (Disabled)

Note: Only applies in VISA spoofed mode

- Inter-Chunk Timer (Two modes of operation: fully transparent mode it is the data forwarding timer, in all other modes specifies time out of assemble syntactically correct message) Value in seconds - Default is 500 seconds
- Strip Control Characters (Strip VISA control characters from the transaction message) Select from pull down menu - Default is "all"

Default: all
none
lrc
all

Note: Only enabled in spoof mode

- Strip Parity (Strip parity from transaction message) Default is false (Disabled)

Note: Actually controlled by the setting of VISA Mode

- Maximum spoofed ENQs (Sets the maximum number of ENQ messages to sent) Default is 5
- Initial ENQ delay (Delay in sending ENQ initial ENQ message to POS terminal) Value in seconds - Default is 800 seconds
- Second ENQ delay (Delay in sending ENQ second ENQ message to POS terminal) Value in seconds - Default is 3000 seconds
- Subsequent ENQ delay (Delay in sending ENQ subsequent ENQ messages to POS terminal) Value in seconds - Default is 3000 seconds
- Expect Host ENQ (Is the host expected to send ENQs) Default is True

Note set to false (host not expected to send ENQs) if in transparent mode

- Delay to EOT (Set the delay before sending EOT to POS terminal follow the maximum number of ENQs) Value in seconds - Default is 200 seconds
- Force VISA Multi-Transaction (Force multiple VISA transactions which are routed to a fixed NII destination) Default is False (Disabled)

Note: Only for Spoofed VISA protocol mode

- VeriCenter Mode (Enable VeriCenter mode - The message may contain a second LRC character which is not validated) Default is False (Disabled)

Note: VISA transparent mode only

- Host Down Option (Not applicable in TCP/IP always EOT)

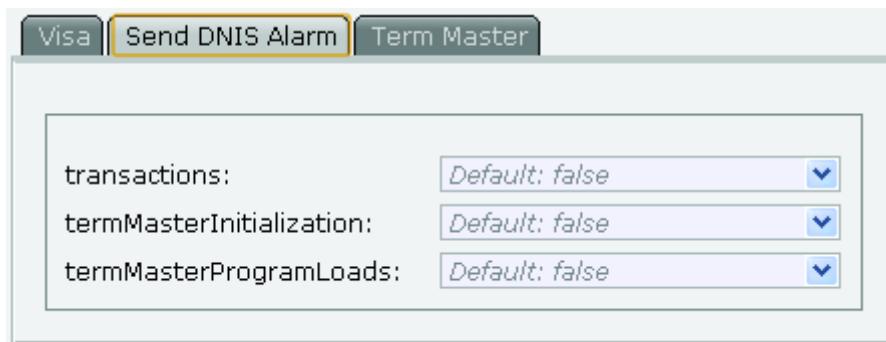


FIGURE 259. TCP/IP DNIS Alarm tab

- Transactions (Send DNIS alarm for transaction) - Default is False (Disabled)

- TermMaster Initialization (Send DNIS alarm for initialization of TermMaster) - Default is False (Disabled)
- TermMaster Program Loads (Send DNIS alarm for terminal program loads from TermMaster)
 - Default is False (Disabled)

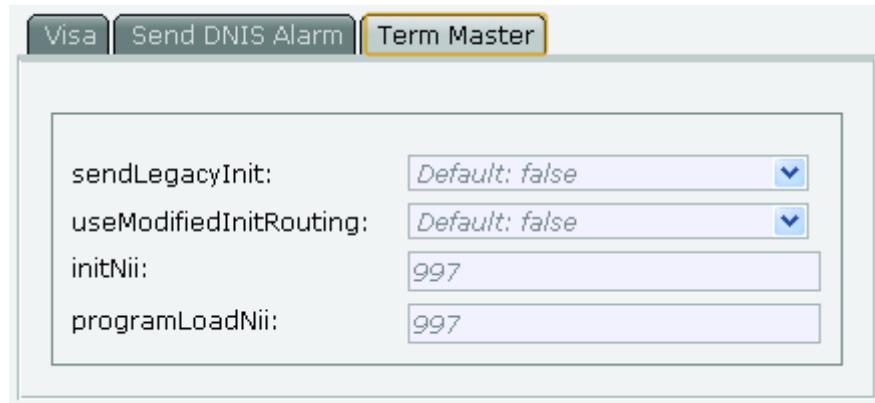


FIGURE 260. TermMaster tab

- Send Legacy Initialization (Send Legacy initialization to application host) Default is False (disabled)
- Use Modified Initialization Routing (Use modified routing of TermMaster initializations) Default is False (Disabled)

Note: If enabled legacy initialization messages with process ID's of 92 or 94 are considered application transactions

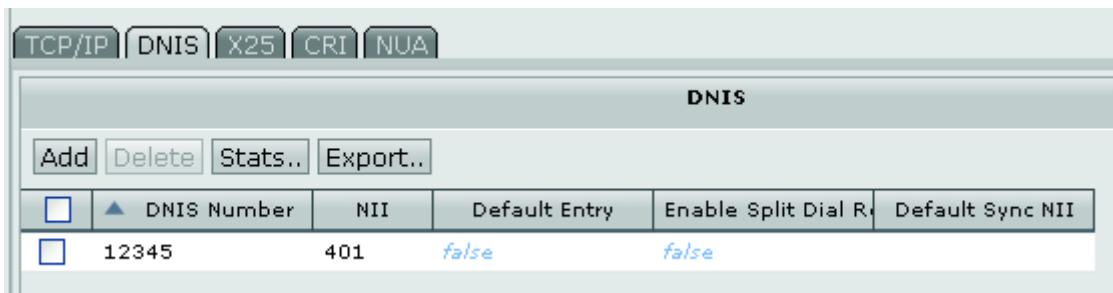
- Initial NII (Initial NII destination) Default is 997
- Program Load NII (Program load NII destination) Default is 997

5. Click **OK**. The changes will be noted on the TCP/IP NII table screen.

DNIS NII Table Configuration

To configure an NII lookup table:

1. On the Config App screen, under Transaction Routing (in the left pane), click on NII Lookup Tables. Click on the “DNIS Tab”, the DNIS screen appears.



DNIS					
		Add	Delete	Stats..	Export..
	DNIS Number	NII	Default Entry	Enable Split Dial R	Default Sync NII
<input type="checkbox"/>	12345	401	false	false	

FIGURE 261. DNIS NII screen

2. On the DNIS TAB.
3. Select a downlink on the listing or click **Add**. The DNIS Downlink screen appears.

Transaction Routings

DNIS

Main	Options
DNIS Number: <input type="text"/>	Routing Options <input checked="" type="radio"/> Call Setup <input type="radio"/> EFTSec
NII: <input type="text"/>	Routing Type: <input type="text"/> Default: this-nii
Default Entry: <input type="text"/> Default: false	NII Overwrite: <input type="text"/> Default: false
<input type="checkbox"/> Override Default entry	NII of Last Resort: <input type="text"/> 0
Enable Split Dial Routing: <input type="text"/> Default: false	
Default Sync NII: <input type="text"/>	

Protocol Options

Visa	Send DNIS Alarm	Term Master
Maximum Request Size: <input type="text"/> 2048	Mode: <input type="text"/> Default: spoofed	
Inactivity Timer: <input type="text"/> 180000	Inter-Chunk Timer: <input type="text"/> 500	
Host Response Timer: <input type="text"/> 60000	Visa Strip Control Chars: <input type="text"/> Default: all	
Maximum Retransmissions: <input type="text"/> 3	Strip Parity: <input type="text"/> true	
Retransmission Timer: <input type="text"/> 3000	Maximum Spoofed ENQs: <input type="text"/> 5	
POS Protocol: <input type="text"/> Default: auto-pos	Initial ENQ Delay: <input type="text"/> 800	
Transaction Portal Protocol: <input type="text"/> Default: false	Second ENQ Delay: <input type="text"/> 3000	
Apply CINP Action: <input type="text"/> Default: false	Subsequent ENQ Delay: <input type="text"/> 3000	
ANI Tagging: <input type="text"/> Default: disable	Expect Host ENQ: <input type="text"/> Default: true	
Permanent Connection: <input type="text"/> Default: false	Delay To EOT: <input type="text"/> 200	

FIGURE 262. DNIS NII Configuration screen

The screenshot shows the 'DNIS' configuration screen. At the top, there's a header bar with the title 'DNIS'. Below it, there are two tabs: 'Main' on the left and 'Options' on the right. Under the 'Main' tab, there are several input fields and dropdown menus:

- DNIS Number:** A text input field.
- NII:** A text input field.
- Default Entry:** A dropdown menu set to 'Default: false' with a checked checkbox below it labeled 'Override Default entry'.
- Enable Split Dial Routing:** A dropdown menu set to 'Default: false'.
- Default Sync NII:** A text input field.

Under the 'Options' tab, there are three more dropdown menus:

- Routing Type:** Set to 'Default: this-nii'.
- NII Overwrite:** Set to 'Default: false'.
- NII of Last Resort:** A text input field containing '0'.

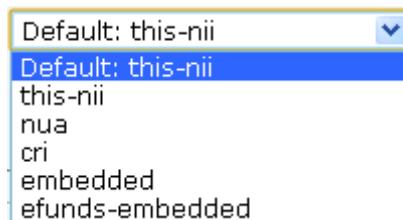
FIGURE 263. Upper part of DNIS Lookup Table screen

- DNIS (Enter DNIS number to configured or VIEW DNIS to be modified)
- NII (enter routing NII for this entry)
- Default Entry (Select this NII Route when a look up fails) Default is false
- Check BOX Override Default entry (If checked the will override any other DNIS NII table configuration) Note IF another DNIS NII table has "default entry" true it will change that "default entry" to false
- Enable Split Dial Routing (Enable NII routing to be split between Async and sync transactions for this NII entry) Default is disabled (false)
- Default Sync NII (The NII route of the sync transaction if split dial routing is enabled)

Note you must configure an DNIS NII table for the SYNC transaction

Routing Options:

- Routing Type (select the routing type from the pull-down list) Default is "this-nii"



- Overwrite NII (select whether to overwrite the NII) Default is legacy-auto-detect
- Last Resort NII (enter alternate NII table to use if current NII table or backup NII table are not available)

Call Setup

- Modem Protocol (Choose a modem protocol for this DNIS route) Select from the pull down menu - Default is disabled (false)

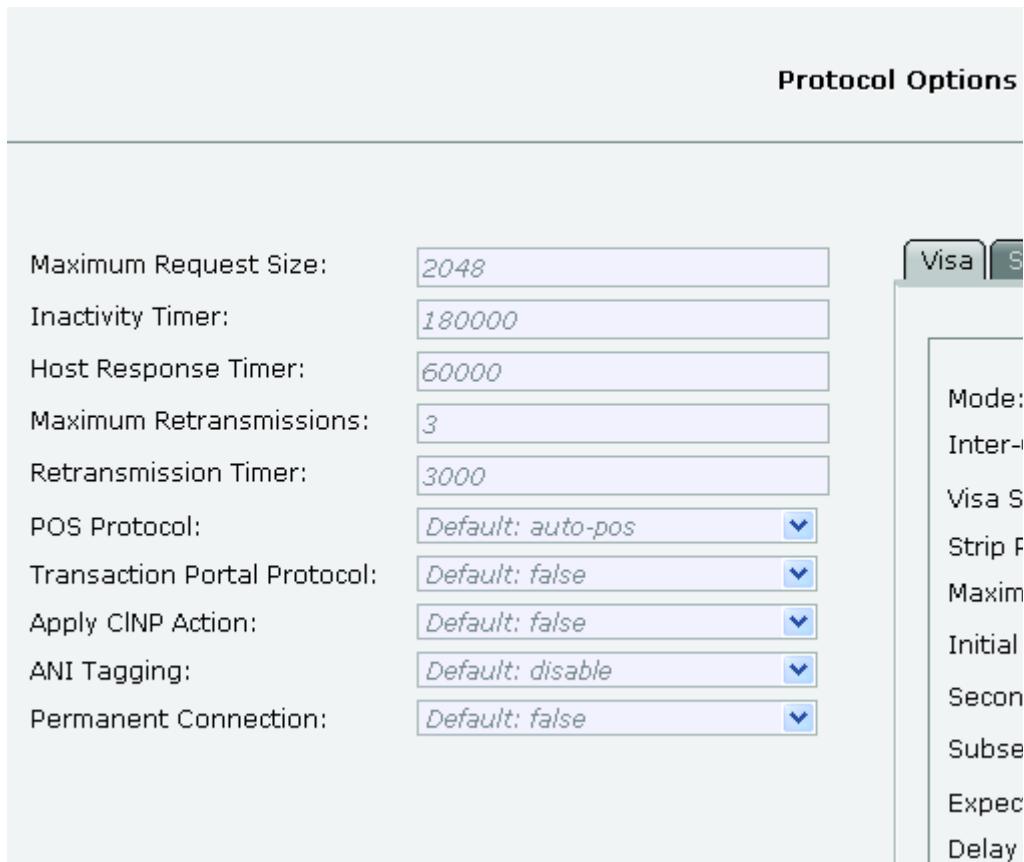
Default: legacy-auto-detect
legacy-auto-detect
itu-v90
itu-v34
v110
64kb-bchan

EFTSec

- Enable (Enable EFTSec for this NII table configuration) Default is disabled (false)
- Non-Encrypted Transaction Action (If EFTSec is enabled and a non-encrypted transaction is received what action should be preformed) Default is unset

unset
unset
enable-with-alarm
enable-without-alarm
disable-with-alarm
disable-without-alarm

Protocol Options (most of these fields are pre-filled with default values)

**FIGURE 264. Protocol Options of DNIS Lookup Table screen**

- Maximum Request Size (TCP Request Size in bytes) Default is 2048 Maximum value is 65535

Note: For CRI routed as a VISA transaction the value must set to 900

- Inactivity Timer (The timer determines the disconnect time with the protocol does not provide a disconnect) Value is in seconds Default is 180000 seconds
 - VISA Transparent and Fully transparent connection with no determined protocol
 - CRI Interleaved authorizations
 - Multi-threaded transactions

Note: The timer is reset on either transmit or receive messages

- Host Response Timer (Timer use when Host response is expected) Value is in seconds - Default is 60000 seconds

Note: Under certain conditions a host response is expect: like a transaction which a non-trailer block is sent

- Max Retransmits (Maximum number of retransmissions) Default is 3

Note: Only used with Non-transparent transactions

- Retransmission Timer (The timer starts after the transmission of the response and stopped at the start of the acknowledgment reception) Value is in seconds Default is 3000 seconds
- POS Protocol (The protocol can be auto detected or set for a specific POS protocol) Select from the pull down menu - Default is “auto-pos”

Default: auto-pos

auto-pos
apacs
modified-async-gsm
term-master
visa
iso8583
none

- Transaction Portal Protocol (Enables Risk Management) Default is False (Disabled)
- Apply CINP Action (ISO8473 Connectionless protocol) Default is False (Disabled)

Note: Only used with X.25 and TCP/IP

- ANI Tagging (Enable prefixing ANI and DNIS information on the transaction request) Select from pull down menu - Default is false (disabled)

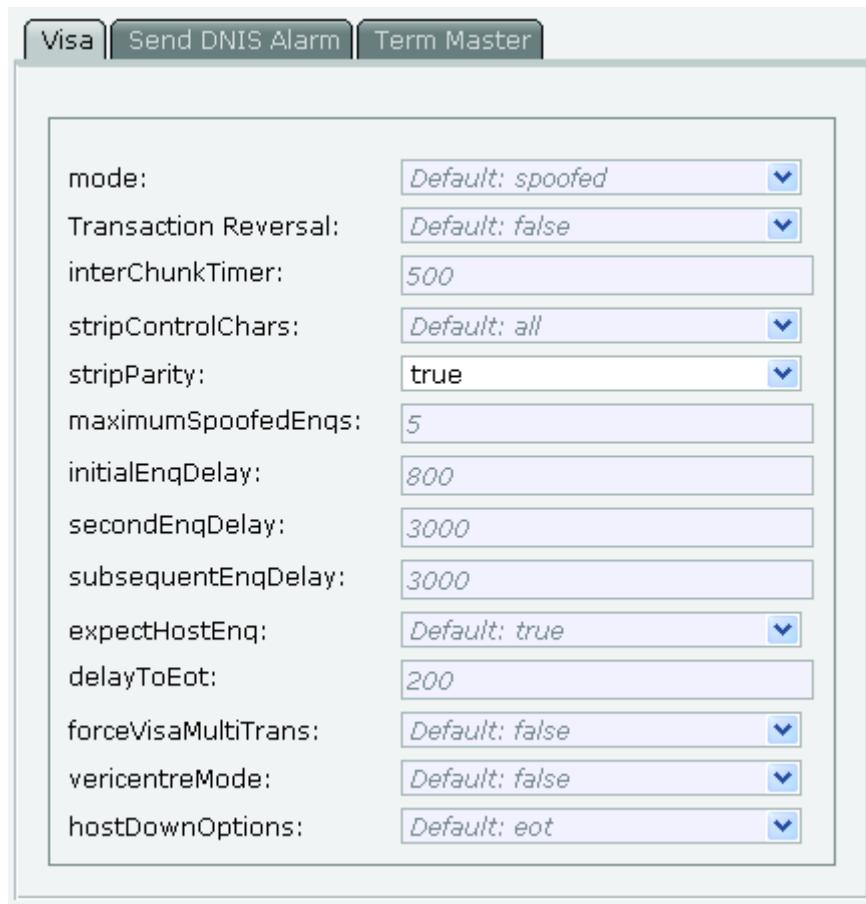
Default: disable

disable
enable
enable-with-lri-header

Note: Only used with PSTN

- Permanent Connection (Down link connection to the terminal that is not disconnected) Default is false (disabled)

Note: A variety of multi-threaded transaction, each with a unique transaction ID can exist within a single permanent connection. Each unique transaction will have its own inactivity timer and can generate a unique down link statistic.

**FIGURE 265. DNIS Visa protocol tab**

- Mode (VISA protocol mode) Select from pull down menu - Default is spoofed

Default: spoofed

spoofed
transparent
fully-transparent

- Transaction Reversal (Enable transaction reversal message protocol) - Default is false (Disabled)

Note: Only applies in VISA spoofed mode

- Inter-Chunk Timer (Two modes of operation: fully transparent mode it is the data forwarding timer, in all other modes specifies time out of assemble syntactically correct message) Value in seconds - Default is 500 seconds
- Strip Control Characters (Strip VISA control characters from the transaction message) Select from pull down menu - Default is "all"

Default: all

none
lrc
all

Note: Only enabled in spoof mode

- Strip Parity (Strip parity from transaction message) Default is false (Disabled)

Note: Actually controlled by the setting of VISA Mode

- Maximum spoofed ENQs (Sets the maximum number of ENQ messages to sent) Default is 5
- Initial ENQ delay (Delay in sending ENQ initial ENQ message to POS terminal) Value in seconds - Default is 800 seconds
- Second ENQ delay (Delay in sending ENQ second ENQ message to POS terminal) Value in seconds - Default is 3000 seconds
- Subsequent ENQ delay (Delay in sending ENQ subsequent ENQ messages to POS terminal) Value in seconds - Default is 3000 seconds
- Expect Host ENQ (Is the host expected to send ENQs) Default is True

Note set to false (host not expected to send ENQs) if in transparent mode

- Delay to EOT (Set the delay before sending EOT to POS terminal follow the maximum number of ENQs) Value in seconds - Default is 200 seconds
- Force VISA Multi-Transaction (Force multiple VISA transactions which are routed to a fixed NII destination) Default is False (Disabled)

Note: Only for Spoofed VISA protocol mode

- VeriCenter Mode (Enable VeriCenter mode - The message may contain a second LRC character which is not validated) Default is False (Disabled)

Note: VISA transparent mode only

- Host Down Option (Send EOT or canned message) Default is EOT

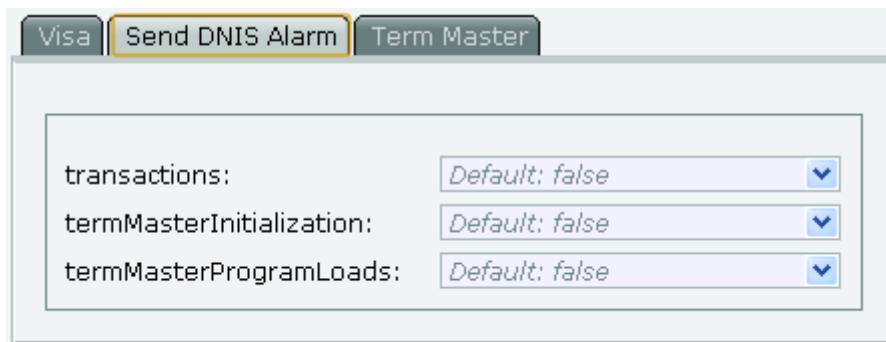


FIGURE 266. TCP/IP DNIS Alarm tab

- Transactions (Send DNIS alarm for transaction) - Default is False (Disabled)

Configuration

- TermMaster Initialization (Send DNIS alarm for initialization of TermMaster) - Default is False (Disabled)
- TermMaster Program Loads (Send DNIS alarm for terminal program loads from TermMaster)
 - Default is False (Disabled)

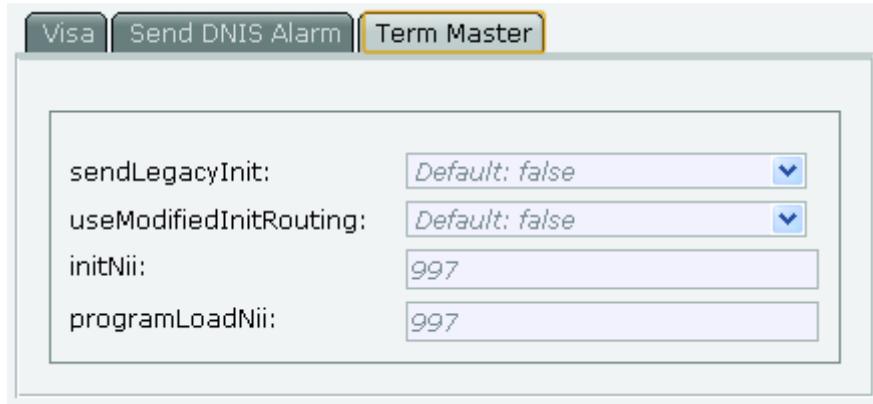


FIGURE 267. TermMaster tab

- Send Legacy Initialization (Send Legacy initialization to application host) Default is False (disabled)
- Use Modified Initialization Routing (Use modified routing of TermMaster initializations) Default is False (Disabled)

Note: If enabled legacy initialization messages with process ID's of 92 or 94 are considered application transactions

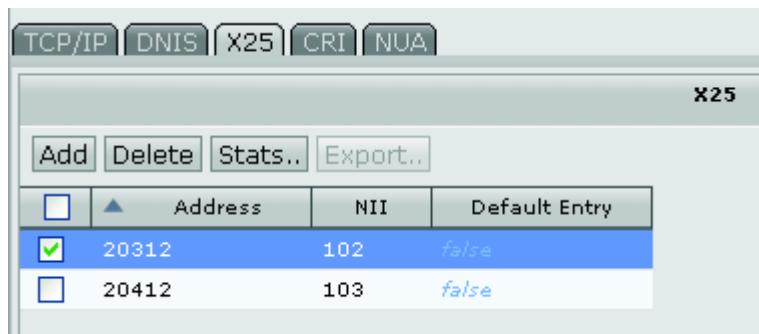
- Initial NII (Initial NII destination) Default is 997
- Program Load NII (Program load NII destination) Default is 997

4. Click **OK**. The changes will be noted on the DNIS NII table screen.

X.25 NII Table Configuration

To configure an NII lookup table:

1. On the Config App screen, under Transaction Routing (in the left pane), click on NII Lookup Tables. Click on the “X.25 Tab”, the X.25 screen appears .



	Address	NII	Default Entry
<input checked="" type="checkbox"/>	20312	102	false
<input type="checkbox"/>	20412	103	false

FIGURE 268. X.25 NII screen

2. On the X.25 TAB.
3. Select a downlink on the listing or click **Add**. The X.25 Downlink screen appears.

Configuration

X25

Main	Options
Address: 20312	
NII: 102	
Default Entry: Default: false	<input type="checkbox"/> Override Default entry
	Routing Options EFTSec
	routingType: Default: this-nii
	overwriteNii: Default: false
	lastResortNii: 0

Protocol Options

Visa	Send DNIS Alarm	Term Master
Maximum Request Size: 2048		
Inactivity Timer: 180000		
Host Response Timer: 60000		
Maximum Retransmissions: 3		
Retransmission Timer: 3000		
POS Protocol: Default: auto-pos		
Transaction Portal Protocol: Default: false		
Apply CINP Action: Default: false		
ANI Tagging: Default: disable		
Permanent Connection: Default: false		
	mode: Default: spoofed	
	Transaction Reversal: Default: false	
	interChunkTimer: 500	
	stripControlChars: Default: all	
	stripParity: true	
	maximumSpoofedEnqs: 5	
	initialEnqDelay: 800	
	secondEnqDelay: 3000	
	subsequentEnqDelay: 3000	
	expectHostEnq: Default: true	
	delayToEot: 200	
	forceVisaMultiTrans: Default: false	
	vericentreMode: Default: false	
	hostDownOptions: Default: eot	

FIGURE 269. X.25 NII Configuration screen

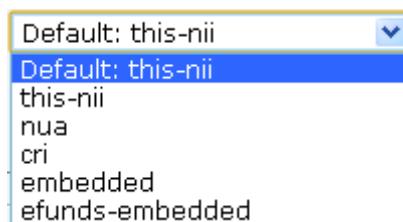


FIGURE 270. Upper part of X.25 Lookup Table screen

- DNIS (Enter DNIS number to configured or VIEW DNIS to be modified)
- NII (enter routing NII for this entry)
- Default Entry (Select this NII Route when a look up fails) Default is false
- Check BOX Override Default entry (If checked the will override any other DNIS NII table configuration) Note IF another DNIS NII table has “default entry” true it will change that “default entry” to false

Routing Options:

- Routing Type (select the routing type from the pull-down list) Default is “this-nii”



- Overwrite NII (select whether to overwrite the NII) Default is legacy-auto-detect
- Last Resort NII (enter alternate NII table to use if current NII table or backup NII table are not available)

EFTSec

- Enable (Enable EFTSec for this NII table configuration) Default is disabled (false)

Configuration

- Non-Encrypted Transaction Action (If EFTSec is enabled and a non-encrypted transaction is received what action should be preformed) Default is unset

unset
unset
enable-with-alarm
enable-without-alarm
disable-with-alarm
disable-without-alarm

Protocol Options (most of these fields are pre-filled with default values)

Protocol Options

Maximum Request Size:	<input type="text" value="2048"/>	Visa S
Inactivity Timer:	<input type="text" value="180000"/>	Mode: Inter-
Host Response Timer:	<input type="text" value="60000"/>	Visa S
Maximum Retransmissions:	<input type="text" value="3"/>	Strip F
Retransmission Timer:	<input type="text" value="3000"/>	Maxim
POS Protocol:	<input type="text" value="Default: auto-pos"/>	Initial
Transaction Portal Protocol:	<input type="text" value="Default: false"/>	Secon
Apply CINP Action:	<input type="text" value="Default: false"/>	Subse
ANI Tagging:	<input type="text" value="Default: disable"/>	Expec
Permanent Connection:	<input type="text" value="Default: false"/>	Delay

FIGURE 271. Protocol Options of X.25 Lookup Table screen

- Maximum Request Size (TCP Request Size in bytes) Default is 2048 Maximum value is 65535

Note: For CRI routed as a VISA transaction the value must set to 900

- Inactivity Timer (The timer determines the disconnect time with the protocol does not provide a disconnect) Value is in seconds Default is 180000 seconds

- VISA Transparent and Fully transparent connection with no determined protocol
- CRI Interleaved authorizations
- Multi-threaded transactions

Note: The timer is reset on either transmit or receive messages

- Host Response Timer (Timer use when Host response is expected) Value is in seconds - Default is 60000 seconds

Note: Under certain conditions a host response is expect: like a transaction which a non-trailer block is sent

- Max Retransmits (Maximum number of retransmissions) Default is 3

Note: Only used with Non-transparent transactions

- Retransmission Timer (The timer starts after the transmission of the response and stopped at the start of the acknowledgment reception) Value is in seconds Default is 3000 seconds
- POS Protocol (The protocol can be auto detected or set for a specific POS protocol) Select from the pull down menu - Default is "auto-pos"

Default: auto-pos
auto-pos
apacs
modified-async-gsm
term-master
visa
iso8583
none

- Transaction Portal Protocol (Enables Risk Management) Default is False (Disabled)
- Apply CINP Action (ISO8473 Connectionless protocol) Default is False (Disabled)

Note: Only used with X.25 and TCP/IP

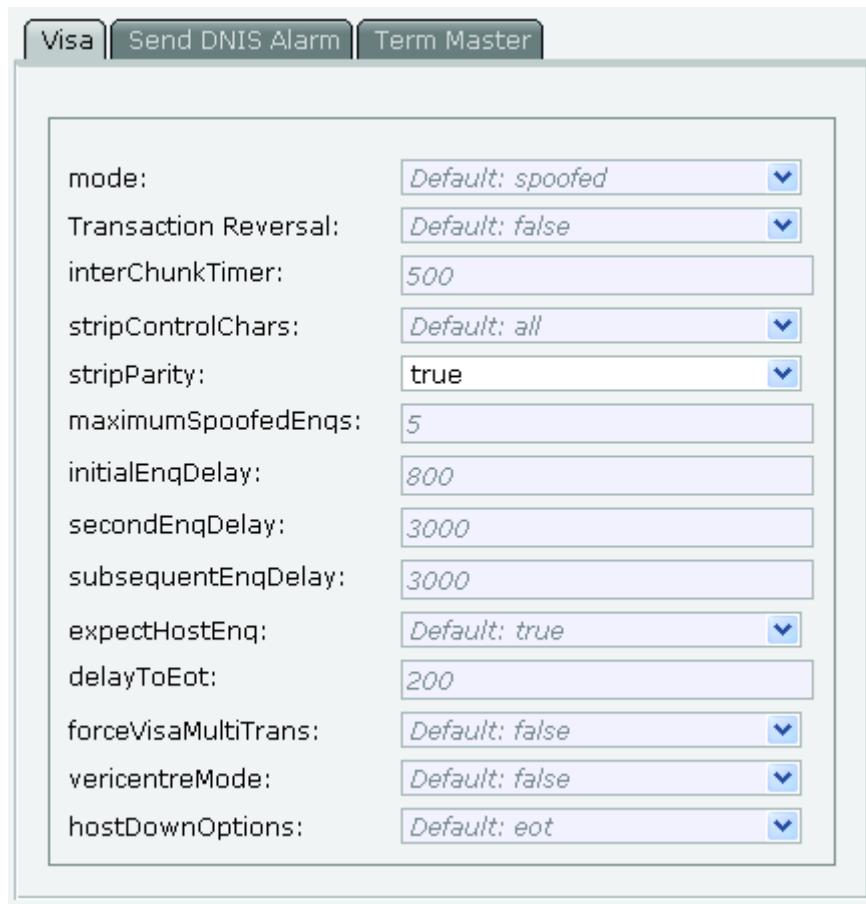
- ANI Tagging (Enable prefixing ANI and DNIS information on the transaction request) Select from pull down menu - Default is false (disabled)

Default: disable
disable
enable
enable-with-lri-header

Note: Only used with PSTN

- Permanent Connection (Down link connection to the terminal that is not disconnected) Default is false (disabled)

Note: A variety of multi-threaded transaction, each with a unique transaction ID can exist within a single permanent connection. Each unique transaction will have it's own inactivity timer and can generate a unique down link statistic.

**FIGURE 272. X.25 Visa protocol tab**

- Mode (VISA protocol mode) Select from pull down menu - Default is spoofed

Default: spoofed

spoofed
transparent
fully-transparent

- Transaction Reversal (Enable transaction reversal message protocol) - Default is false (Disabled)

Note: Only applies in VISA spoofed mode

- Inter-Chunk Timer (Two modes of operation: fully transparent mode it is the data forwarding timer, in all other modes specifies time out of assemble syntactically correct message) Value in seconds - Default is 500 seconds
- Strip Control Characters (Strip VISA control characters from the transaction message) Select from pull down menu - Default is "all"

–
Default: all
none
lrc
all

Note: Only enabled in spoof mode

- Strip Parity (Strip parity from transaction message) Default is false (Disabled)

Note: Actually controlled by the setting of VISA Mode

- Maximum spoofed ENQs (Sets the maximum number of ENQ messages to sent) Default is 5
- Initial ENQ delay (Delay in sending ENQ initial ENQ message to POS terminal) Value in seconds - Default is 800 seconds
- Second ENQ delay (Delay in sending ENQ second ENQ message to POS terminal) Value in seconds - Default is 3000 seconds
- Subsequent ENQ delay (Delay in sending ENQ subsequent ENQ messages to POS terminal) Value in seconds - Default is 3000 seconds
- Expect Host ENQ (Is the host expected to send ENQs) Default is True

Note set to false (host not expected to send ENQs) if in transparent mode

- Delay to EOT (Set the delay before sending EOT to POS terminal follow the maximum number of ENQs) Value in seconds - Default is 200 seconds
- Force VISA Multi-Transaction (Force multiple VISA transactions which are routed to a fixed NII destination) Default is False (Disabled)

Note: Only for Spoofed VISA protocol mode

- VeriCenter Mode (Enable VeriCenter mode - The message may contain a second LRC character which is not validated) Default is False (Disabled)

Note: VISA transparent mode only

- Host Down Option (Send EOT or canned message) Default is EOT

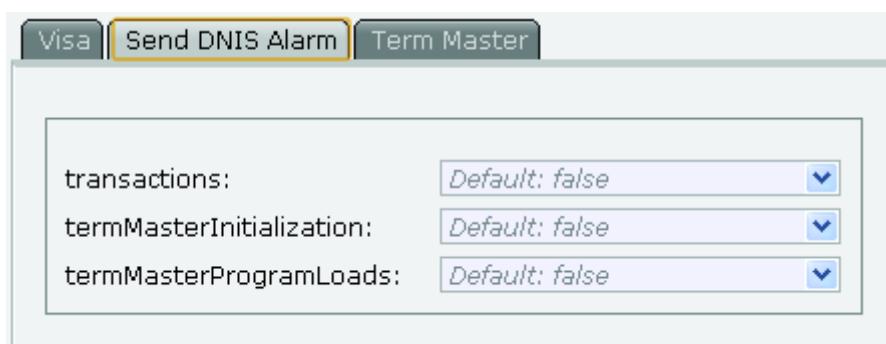


FIGURE 273. X.25 DNIS Alarm tab

- Transactions (Send DNIS alarm for transaction) - Default is False (Disabled)

Configuration

- TermMaster Initialization (Send DNIS alarm for initialization of TermMaster) - Default is False (Disabled)
- TermMaster Program Loads (Send DNIS alarm for terminal program loads from TermMaster)
 - Default is False (Disabled)

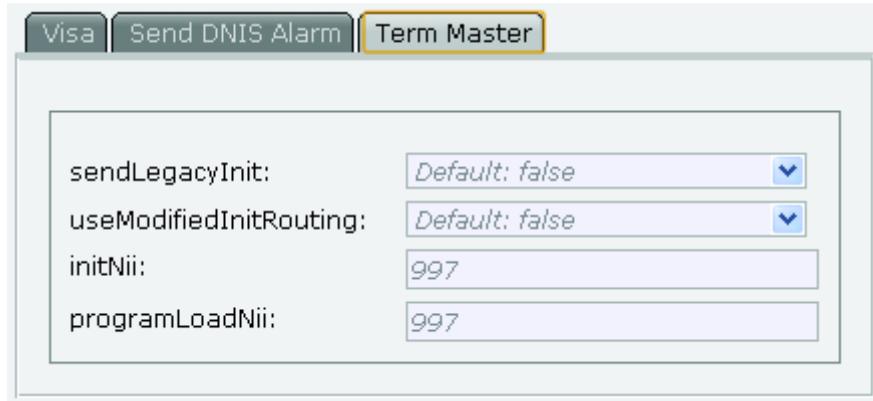


FIGURE 274. TermMaster tab

- Send Legacy Initialization (Send Legacy initialization to application host) Default is False (disabled)
- Use Modified Initialization Routing (Use modified routing of TermMaster initializations) Default is False (Disabled)

Note: If enabled legacy initialization messages with process ID's of 92 or 94 are considered application transactions

- Initial NII (Initial NII destination) Default is 997
- Program Load NII (Program load NII destination) Default is 997

4. Click **OK**. The changes will be noted on the X.25 NII table screen.

CRI NII Table Configuration

To configure an CRI NII lookup table:

CRI is Content Based Routing, A configured Address is the content to be match for the NII route.

Note that a DNIS NII must be configured to use CRI routing

1. On the Config App screen, under Transaction Routing (in the left pane), click on NII Lookup Tables. Click on the “CRI Tab”, the CRI screen appears .

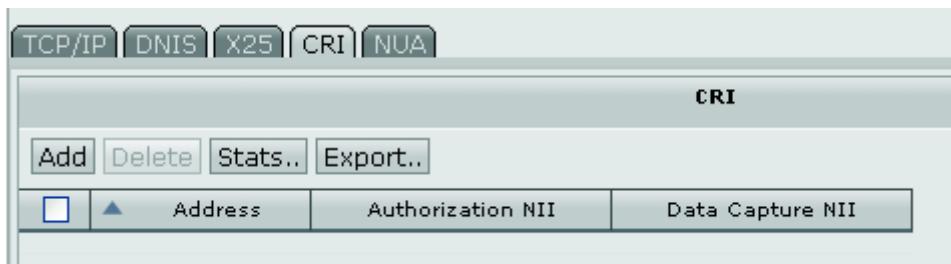


FIGURE 275. CRI NII screen

2. On the CRITAB.
3. Select a downlink on the listing or click **Add**. The CRI Downlink screen appears.

A screenshot of a configuration dialog box titled "CRI". It contains three text input fields: "Address:", "Authorization NII:", and "Data Capture NII:". Each field has a corresponding label to its left.

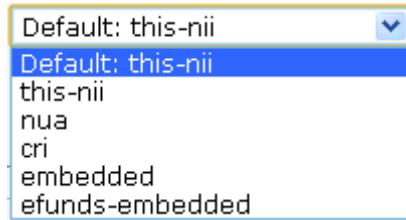
FIGURE 276. CRI NII Configuration screen

- Address (Enter address string route)
- Authorization NII (Enter authorization routing NII for this NII entry)
- Data Capture NII (Enter the Data NII routing for this NII entry)

Note In DNIS NII table “Routing Options”

Configuration

- Routing Type (select the routing type from the pull-down list) Must select CRI as routing type



4. Click **OK**. The changes will be noted on the CRI NII table screen.

NUA NII Table Configuration

To configure an NUA NII lookup table:

NUA is X.25 Network Un-numbered Address, A configured Address is the content to be match for the NII route.

Note that a DNIS NII must be configured to use NUA routing

1. On the Config App screen, under Transaction Routing (in the left pane), click on NII Lookup Tables. Click on the “NUA Tab”, the NUA screen appears .

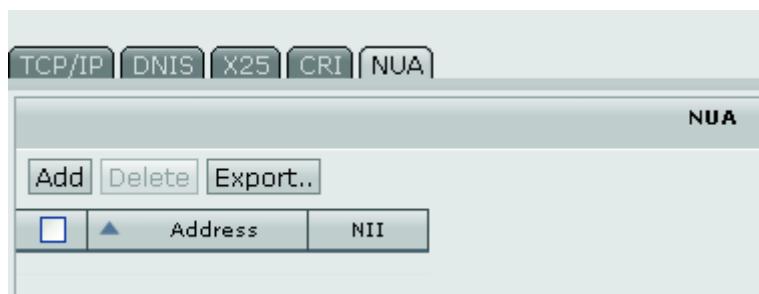


FIGURE 277. CRI NII screen

2. On the MUA TAB.
3. Select a downlink on the listing or click **Add**. The NUA Downlink screen appears.

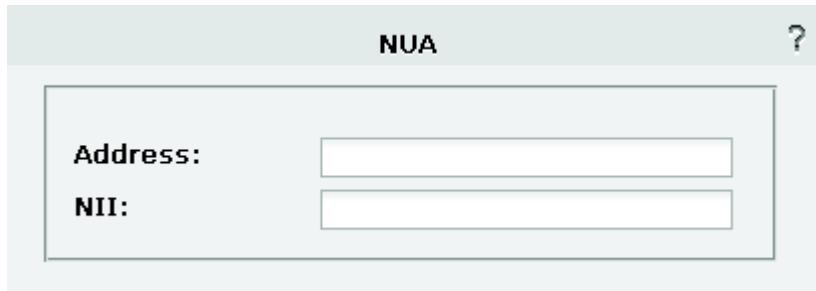
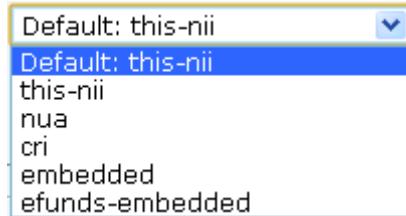


FIGURE 278. CRI NII Configuration screen

- Address (Enter address string route)
 - NII (Enter the NII routing for this entry)
- Note In DNIS NII table “Routing Options”

- Routing Type (select the routing type from the pull-down list) Must select NUA as routing type



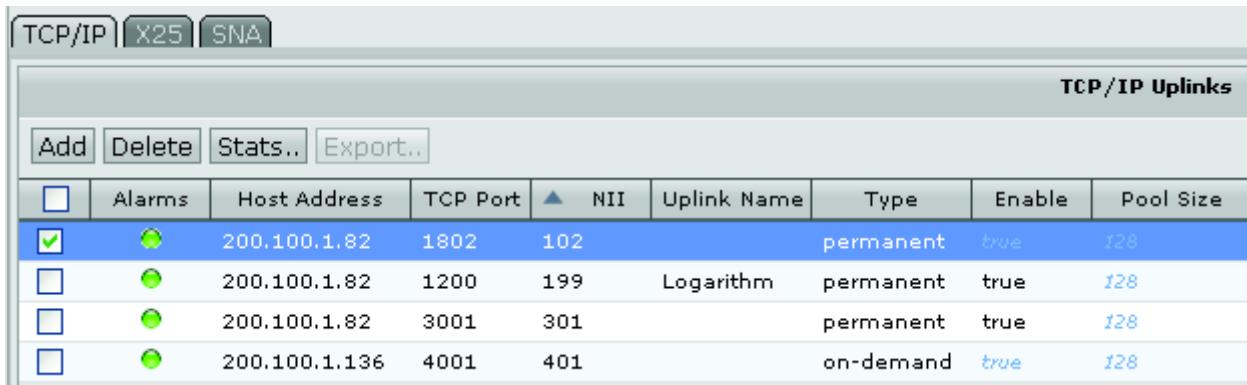
4. Click **OK**. The changes will be noted on the NUA NII table screen.

Uplinks Configuration

TCP/IP Uplink Configuration

To configure an TCP/IP uplink:

1. On the Config App screen, under Transaction Routing (in the left pane), click **Uplinks**. The TCP/IP Uplinks screen appears (default).



The screenshot shows the TCP/IP Uplinks configuration screen. At the top, there are tabs for TCP/IP, X25, and SNA, with TCP/IP selected. Below the tabs is a toolbar with buttons for Add, Delete, Stats.., and Export.. The main area is titled "TCP/IP Uplinks" and contains a table with the following data:

	Alarms	Host Address	TCP Port	NII	Uplink Name	Type	Enable	Pool Size
<input checked="" type="checkbox"/>		200.100.1.82	1802	102		permanent	true	128
<input type="checkbox"/>		200.100.1.82	1200	199	Logarithm	permanent	true	128
<input type="checkbox"/>		200.100.1.82	3001	301		permanent	true	128
<input type="checkbox"/>		200.100.1.136	4001	401		on-demand	true	128

FIGURE 279. TCP/IP Uplinks screen

2. Select from the existing uplinks listed or click **Add**. Clicking **Add** opens the TCP/IP screen.

TCP/IP Uplink

Transaction host Address:	<input type="text"/>
TCP Port:	<input type="text"/>
NII:	<input type="text"/>
Uplink Name:	<input type="text"/>
Session Type:	<i>Default: on-demand</i> <input type="button" value="▼"/>
Enable:	<i>Default: true</i> <input type="button" value="▼"/>
Session Pool Size:	<input type="text" value="128"/>
SSL:	<i>Default: false</i> <input type="button" value="▼"/>
CA Certificate:	<input type="text"/>
Length Field Format:	<i>Default: not-present</i> <input type="button" value="▼"/>
Include Length Field In Length:	<i>Default: false</i> <input type="button" value="▼"/>
Vendor Link Protocol:	<i>Default: false</i> <input type="button" value="▼"/>
Add TPDU if on-demand:	<i>Default: false</i> <input type="button" value="▼"/>
Soft Shutdown:	<i>Default: false</i> <input type="button" value="▼"/>
Keep Alive Timer (msec):	<input type="text" value="10000"/>
Keep Alive Format:	<i>Default: none</i> <input type="button" value="▼"/>
Connect Failed Timer:	<input type="text" value="4500"/>

FIGURE 280. TCP/IP Uplink screen

3. Enter the field information:

- Transaction host IP Address (Enter IP address for the port xxx.xxx.xxx.xxx)
- TCP Port (enter the specific TCP port)
- NII (enter the port's NII) Values 1 to 999 are primary and values 1001 to 1999 are backup NII entries
- Uplink Name (enter descriptive name of uplink port) up to 128 characters
- Session Type (select the session type from the pull-down list) Permanent or On-Demand - Default if On-Demand
- Enable (select whether the uplink is enabled from the pull-down list) Default is disable (false)
- Session Pool Size (enter the size of the session pool. This only applies to the on-demand session type) Default 128 byte
- Secure Socket Layer -SSL- (Enable the use of SSL on this up link) Default is disabled (false)

- CA Certification select (Select certificate to from pull down menu) Certificates are loaded on the main screen under “Files” icon. “Upload” “uplink-ca-cert”.
- Length Field Format (Select field format from pull down menu) Default is no length field

Default: not-present
bcd
hex
hex-4bytes
not-present

- Include Length Field (Enable the counting of length field in the byte count of the message) Default is false
- Use Vendor Link Protocol (select whether the vendor link protocol is used from the pull-down list. This only applies to the TCP/IP interface) Default is false
- Add TPDU if on-demand (select from the pull-down list whether TPDUs are added to requests sent to this uplink if the uplink type is on-demand) Default is false
- Soft Shutdown (select if shutdown is enabled from the pull-down menu) Default is disabled (false)

Note: If true, wait before disabling or deleting an uplink, wait up to two minutes to allow all transactions actively using the uplink to complete before shutting down)

- Keep Alive Timer (hundredths of a second) - (Application keep alive message are sent until the timer expires or another message is sent/received) Default is 10000msec (10seconds)
- Keep Alive Format (Choose keep alive message format from the pull down menu)

Default: none
none
standard
client
server

- Connect Failed timer (Disconnect timer for non-responsive permanent connections in hundredths of a second) Default is 4500 msec (4.5seconds)

4. Click **OK**

X.25 Uplink Configuration

To configure an X.25 uplink:

1. On the Config App screen, under Transaction Routing (in the left pane), click **Uplinks**. The TCP/IP Uplinks screen appears (default).
2. Click on the desired uplink type tab (X25).
3. The X25 Uplinks screen appears.

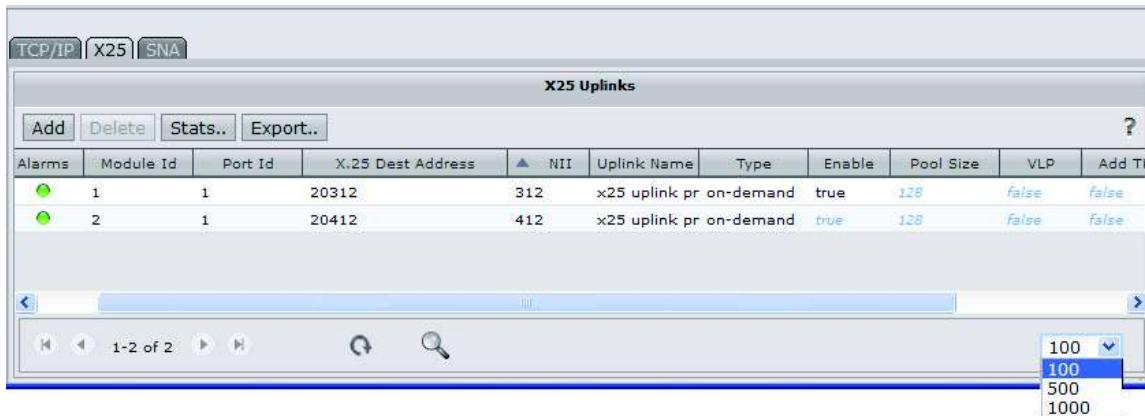
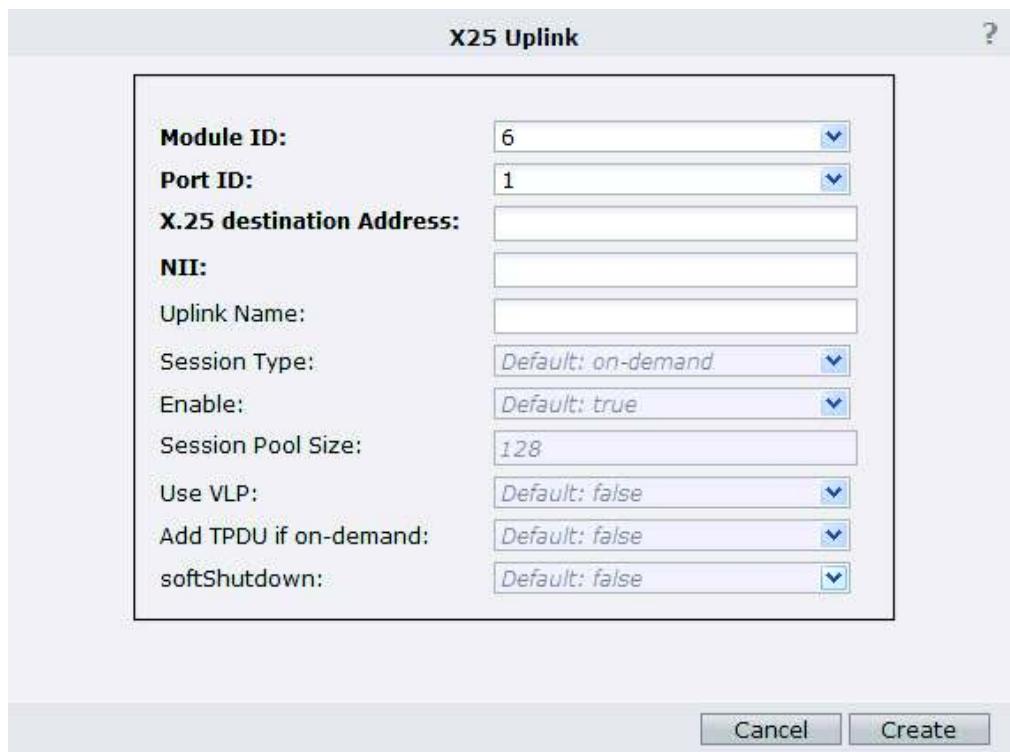


FIGURE 281. X.25 Uplinks screen

4. Select from the existing uplinks listed or click **Add**. Clicking **Add** opens the X25 screen.

**FIGURE 282. X25 Uplink screen**

5. Enter the field information:

- Module ID (enter identifier for the interface port or select from pull-down list)
- Port ID (enter the unique identifier for the port or select from pull-down list)
- X.25 destination Address (enter the destination address)
- NII (enter the port's NII)
- Uplink Name (enter descriptive name of uplink port) up to 128 characters
- Session Type (select the session type from the pull-down list) Permanent or On-Demand - Default if On-Demand
- Enable (select whether the uplink is enabled from the pull-down list) Default is disable (false)
- Session Pool Size (enter the size of the session pool. This only applies to the on-demand session type) Default 128 byte
- Add TPDU if on-demand (select from the pull-down list whether TPDUs are added to requests sent to this uplink if the uplink type is on-demand) Default is false
- Soft Shutdown (select if shutdown is enabled from the pull-down menu) Default is disabled (false)

Note: If true, wait before disabling or deleting an uplink, wait up to two minutes to allow all transactions actively using the uplink to complete before shutting down)

6. Click **OK**.

SNA Uplink Configuration

To configure an SNA uplink:

1. On the Config App screen, under Transaction Routing (in the left pane), click **Uplinks**. The TCP/IP Uplinks screen appears (default).
2. Click on the desired uplink type tab (SNA).
3. The SNA Uplinks screen appears.

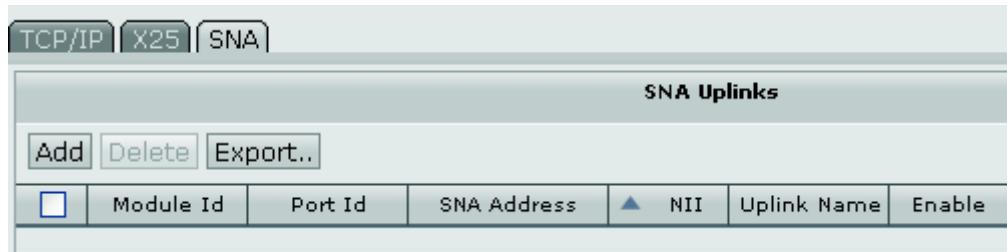


FIGURE 283. SNA Uplinks screen

4. Select from the existing uplinks listed or click **Add**. Clicking **Add** opens the SNA screen.

A screenshot of the SNA Uplink configuration dialog box. It has a title bar "SNA Uplink". Inside, there are several input fields:

- Module ID: A dropdown menu showing "4".
- Port ID: A dropdown menu showing "1".
- SNA Address: An empty text input field.
- NII: An empty text input field.
- Uplink Name: An empty text input field.
- Enable: A dropdown menu showing "Default: true".

FIGURE 284. SNA Uplink screen

5. Enter the field information:
 - Module ID (enter identifier for the interface port or select from pull-down list)
 - Port ID (enter the unique identifier for the port or select from pull-down list)
 - SNA destination Address (enter the destination address) Also used as an unique identifier
 - NII (enter the port's NII)
 - Uplink Name (enter descriptive name of uplink port) up to 128 characters
 - Enable (select whether the uplink is enabled from the pull-down list) Default is disable (false)

6. Click **OK**.

Offline Device Configuration

This type of device configuration is not associated with a specific device, but with a type of device. You can perform many of the same operations as on an active configuration, but instead of configuring an active device, it manipulates records in a database.

Adding an Offline Configuration

1. On the Offline Config Stores screen, click **Add**.



FIGURE 285. Offline Config Stores screen

The Offline Config Store screen appears:



FIGURE 286. Offline Config Store screen

2. Enter the following items:
 - **Name:** The name of the offline store

- **Device Type:** Type of device for this configuration. Choose from the list of supported devices.
- **Device Version:** The version or release of the device that is compatible with this configuration.
- **Config Set:** Optional. Choose from the list or leave it set to “all objects”.
- **Description:** Textual description of this offline store.

3. Click **Create**. A system message appears.



FIGURE 287. Offline Config Store creation confirmation

4. Click **OK**.

Deleting an Offline Configuration

1. On the Offline Config Stores screen, select the configuration.
2. Click **Delete**.

Copying an Offline Device Configuration

To copy an offline device configuration and all of the objects inside it:

1. On the Offline Config Stores screen, select the configuration.
2. Click **Copy**. The Copy Config Store screen appears.



FIGURE 288. Copy Config Store screen

3. Specify the version to match a different release of the device's software/schema. The objects will be migrated to the new schema during the copy operation.
4. Click **OK**. Enter the settings for the new configuration and click **OK**.

Manipulating the Configuration Objects

The **Config App** button on the **Offline Config Stores** screen opens a configuration app on a selected store, allowing you to manipulate the configuration objects in the store.

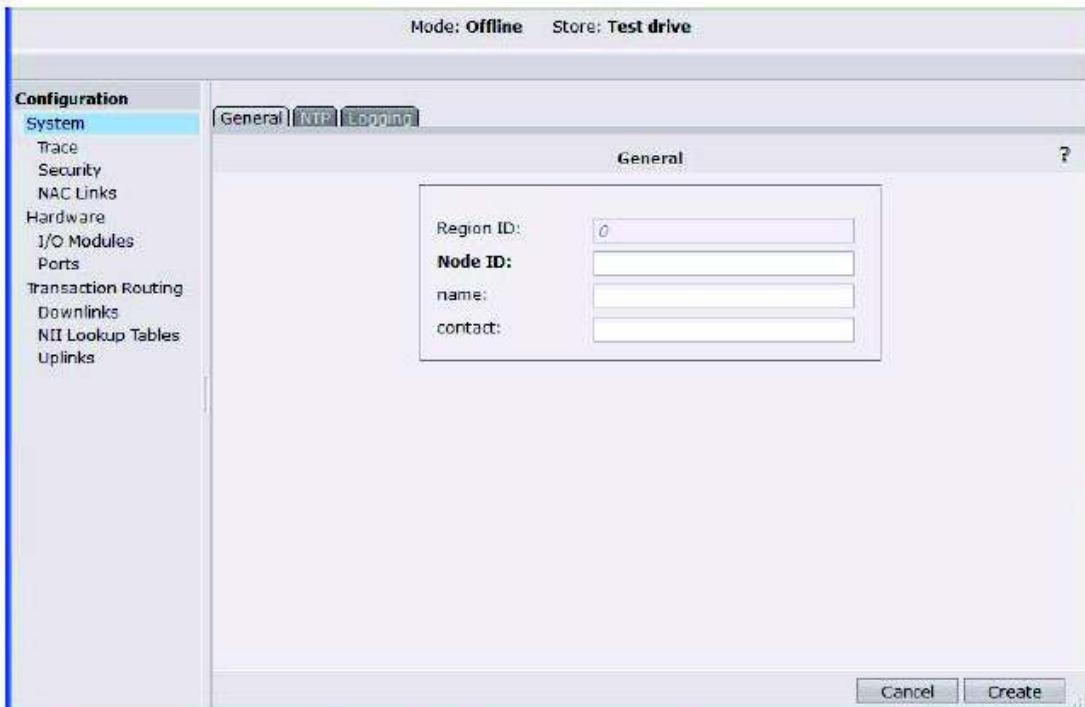


FIGURE 289. Config App screen

This is similar to the online version with the following differences:

- Statistics categories and screen will not display since they only relate in an online context.
- Table buttons that link to statistics or operations screen will not appear.

Downloading a Configuration

The **Download** button on **Offline Config Stores** screen allows you to create a new store and download the configuration from a specific device into the store.

To download:

1. On the **Offline Config Stores** screen, select a configuration.
2. Click **Download**. The **Download Config** screen appears.



FIGURE 290. Download Config screen

3. Enter the following information:

- **Device:** Device where the configuration is coming from
- **Set:** If this device has defined config sets, select the related config set.
- **New Store Name:** Name of the store to put the downloaded config.
- **Description:** Textual description of this offline store.

4. Click **OK**.

Uploading a Configuration

The **Upload** button on the **Offline Config Stores** screen allows you to copy the objects from an offline store into a device and make it the running configuration on the device. The configuration can be uploaded to the device it was downloaded from or to another device of the correct type and version.

To upload a configuration:

1. On the **Offline Config Stores** screen, select a configuration.
2. Click **Upload**. The **Upload Config** screen appears.

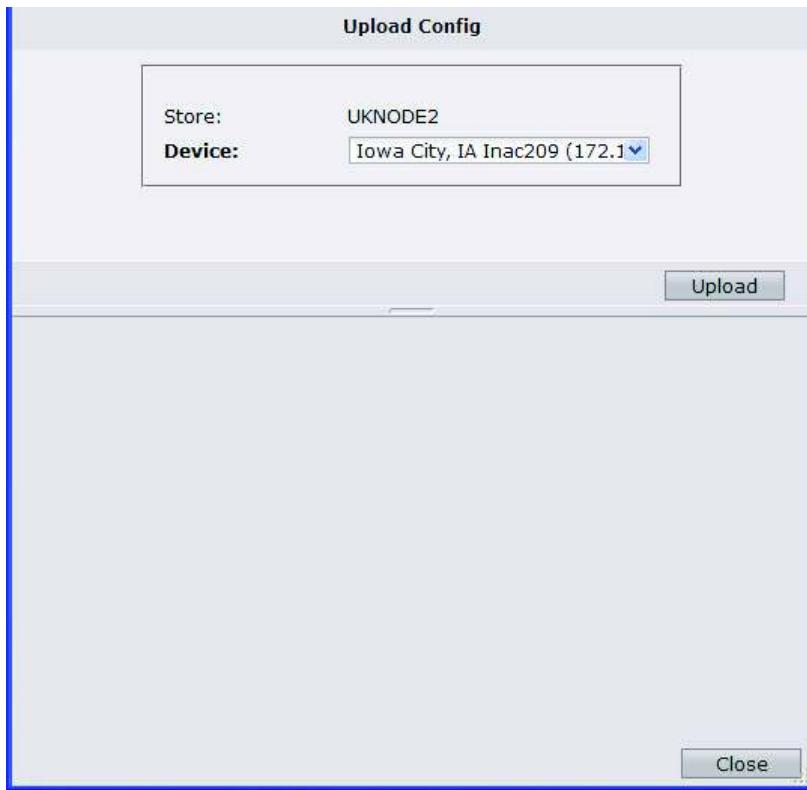


FIGURE 291. Upload Config screen

3. Use the drop-down to select the device.
4. Click **Upload**. The progress of the upload operation displays as it happens.

Split Dial Routing

The Split Dial Routing feature allows you to define two Transaction NII's within a single DNIS NII Lookup Table entry. This feature only applies if Routing Type is set to "this-nii" within the entry.

Constraints

If Split Dial Routing is enabled, all synchronous dial transactions using this DNIS table entry are routed to the Default Sync NII. All other dial transaction types (Visa Spoofed, Transparent, or Fully Transparent) will be routed to the Standard Routing NII.

Configure Split Dial Routing

1. On Map click on node of the port to be configured for Split Dial Routing
2. Click on tool bar icon "Config App"
3. In "Config App" Screen select "NII Lookup Table" view under "Configuration" (right side bar)
4. Select "DNIS" tab
5. Double click DNIS entry to be Split Dial Routing enabled
6. On the "DNIS" configuration screen select "Routing Options"
7. Select "Routing Type" from drop down menu (must be "this-nii", "Default: this-nii")
8. Enable Split Dial Routing set to "True"
9. Enter "Default Sync NII" value (must be a configured NII value)

CHAPTER 5

Operations

Overview

This section details the basic IntelliView operations. These operations are available for each IntelliView installation regardless of your configuration. They include operations such as:

- Alarms and events
- Statistical collection
- Security

The goals of the alarms and alerts are to:

- accept and store event notifications
- raise and clear alarm states
- maintain the alarm state and notify users when the state changes.

Alarms and Events

IntelliView has an Eventing and Alarm system. Events are stored in a database which allows querying and sorting. An Alarm Corrector examines events and performs alarm actions such as raising and clearing alarms.

Alarms

IntelliView alarms are displayed in multiple ways: icons in the map, tree nodes, and items in a table that can relate to alarms will react when an alarm is raised or cleared.

In the Main screen, map icons and tree nodes indicate with color the worst alarm condition affecting it. In tables, if an alarm is raised against the object shown, an alarm ball is shown indicating the worst alarm condition for that object.

Most alarms are raised and cleared based on Alarm-type events. The system contains a correlation engine that looks at events and applies them to the alarm system. The correlation is based on the following fields: Name, Element, Source Type, and Source ID.

Alarms can be viewed in two places: On the main screen in the lower half alarms can be displayed and by clicking on the Alarm ICON in the tool bar alarms can be displayed.

<input type="checkbox"/>	Time Stamp	Status	Element	Node ID	Name	Severity
<input type="checkbox"/>	2012-09-13 08:11:26.810 +00:00	●	IntelliView	0000	System ID mismatch	Critical
<input type="checkbox"/>	2013-06-01 17:07:13.044 +00:00	●	IntelliView	0000	Invalid License	Critical
<input type="checkbox"/>	2013-07-01 12:45:27.830 +00:00	●	Inac 208 no r 1008		Device Disconnected	Critical
<input type="checkbox"/>	2013-07-01 12:45:27.906 +00:00	●	Inac 207 no r 1107		Device Disconnected	Critical
<input type="checkbox"/>	2013-07-01 12:51:24.142 +00:00	●	Iowa city, IA I 1010		Device Disconnected	Critical
<input type="checkbox"/>	2013-07-01 17:52:06.255 +00:00	●	Phoenix,AZ Ir 1009		Device Disconnected	Critical
<input type="checkbox"/>	2013-07-01 12:45:36.737 +00:00	●	Iowa city, IA I 1010		NAC_LINK_DISCONNECTED	Major
<input type="checkbox"/>	2013-07-01 17:53:21.255 +00:00	●	Phoenix,AZ Ir 1009		TCPIP_UPLINK_UNAVAILABLE	Major
<input type="checkbox"/>	2013-07-01 17:53:21.501 +00:00	●	Phoenix,AZ Ir 1009		TCPIP_UPLINK_UNAVAILABLE	Major

Severity	Acked	Cleared	Assigned	Object Type	Object Key	User cleared
Critical	true	false		EMS	0	false
Critical	true	false		EMS	0	false
Critical	true	false		Device	1017	false
Critical	true	false		Device	1020	false
Critical	false	true		Device	1007	false
Critical	false	true		Device	1016	false
Major	true	false		IntelliNAC/Intellinac_con /intellinac/config	false	
Major	false	false		IntelliNAC/Intellinac_con /intellinac/config	false	
Major	false	false		IntelliNAC/Intellinac_con /intellinac/config	false	
Major	false	false		IntelliNAC/Intellinac_con /intellinac/config	false	

FIGURE 292. Alarm table

The Main Screen Alarm Table and the toolbar selected alarms are the same. The ICON selected table is in a new browser window. Both tables have the abilities and display the same data.

IntelliView alarms contain the following fields:

Field	Description
Created Timestamp (IntelliView)	The IntelliView Timestamp when the alarm was first created
Status	
Element	Element for which the alarm is raised. This could be IntelliView.
Node ID	
Name	Name of the alarm
Severity	The severity of the alarm when it was raised.
Acknowledged	A Boolean value indicating if the alarm has been acknowledged
Cleared	A Boolean value indicating the cleared state.
Assigned	
Object Type	
Object Key	
User Clearable	By default, alarms generated from module modifications are not user-clearable. Instead, it is expected that the device will clear the alarm condition when the problem is resolved.

Each row in the table has a green LED indicating if it is set or cleared. This LED is also colored to indicate the severity.

Alarm balls have the following colors, if set:

- **Critical** - Red
- **Major** - Orange
- **Minor** - Yellow
- **Clear** - Green

If the alarm is not set, the alarm ball is green. The severity of the alarm will remain the severity of the last setting.

If the alarm is not acknowledged, the row will have a background color to indicate that it needs attention. Once the alarm is acknowledged, the background color will be set to the default background color of the table.

For unacknowledged alarms, the background color of the row will be set to the following:

- **Critical** - Red
- **Major** - Orange
- **Minor** - Yellow
- **Clear** - Green.

The table has an **Row selection** check box which allows the user to select a row and acknowledge one or more alarms. The table updates automatically when the state of an alarm

changes. The alarm table also has the ability to export table data to a CSV format stored on the user's desktop based on the table's current sorting and filtering settings.

Alarm Details Screen

Double-clicking on a row in the Alarm table displays the **Alarm Details** screen.

The screenshot shows the 'Alarm' details screen. At the top, there's a table of alarm properties:

Name:	Device Disconnected
Severity:	Critical
Is Clear:	false
Element:	Inac 208 no network connection
Node ID:	1008
Object Type:	Device
Object Key:	1017
Created (IntelliView Time):	2013-06-27 13:44:39.625 +0000
Created (Element Time):	2013-06-27 13:44:39.598 +0000
Last Event (IntelliView Time):	2013-07-01 12:45:27.830 +0000
Last Event (Element Time):	2013-07-01 12:39:50.167 +0000
Assigned To:	<input type="text"/>

Below this is an 'Information' section with tabs: Info (selected), Notes, Details, Events.

Under the 'Info' tab, there are three entries:

- Reason Set: This alarm is raised when connection to the device is lost or can not be established.
- Reason Cleared: This alarm is cleared when connection to the device is established.
- Recommended Actions: Check to see if the device is operating. Check the network for connectivity issues, bad routes. Check the device conenction configuration to see if the correct address, port are being used.

FIGURE 293. Alarms details screen

Field	Description
Name	Name of the alarm
Severity	The severity of the alarm when it was raised.
Is Cleared	A Boolean value indicating the cleared state.
Element	Element for which the alarm is raised. This could be IntelliView.
Node ID:	The node on which the alarm occurred
Object Type	What type of object had the alarm (device, IntelliVIEW, or other)
Object Key	What interface or function caused the alarm
Created Time stamp (IntelliView)	The IntelliView Time stamp when the alarm was first created
Created Time stamp (Element)	The time stamp from the event when the alarm was first created
Last Event Time stamp (IntelliView)	The IntelliView time stamp of the last event to raise or clear the alarm.
Last Event Time stamp (Element)	The time stamp from the event that last raised or cleared the alarm.
Assigned	The alarm can be assigned to a user, Administrator or group

Info Tab	Contains the alarm's general information. The reasons for setting and clearing the alarm are displayed, along with recommended actions.
Notes Tab	Contains notes about this alarm. A note is added to the alarm automatically whenever a user-initiated action on the alarm is taken. A user may add a note of their own as well.
Details Tab	Contains a list of attribute name/value pairs of the last event that modified the alarm. This field allows any set of attribute values to be stored and viewed in the Event Details screen. These are normally set using values of attributes from the notification causing the event.
Events Tab	A simple list of events related to this alarm. The list shows the timestamp and severity of the events that raised and cleared this alarm.

The Alarms screen shows generic text for the alarm describing what typically caused this alarm, how it is cleared, and actions the user might take to remedy the alarm condition.

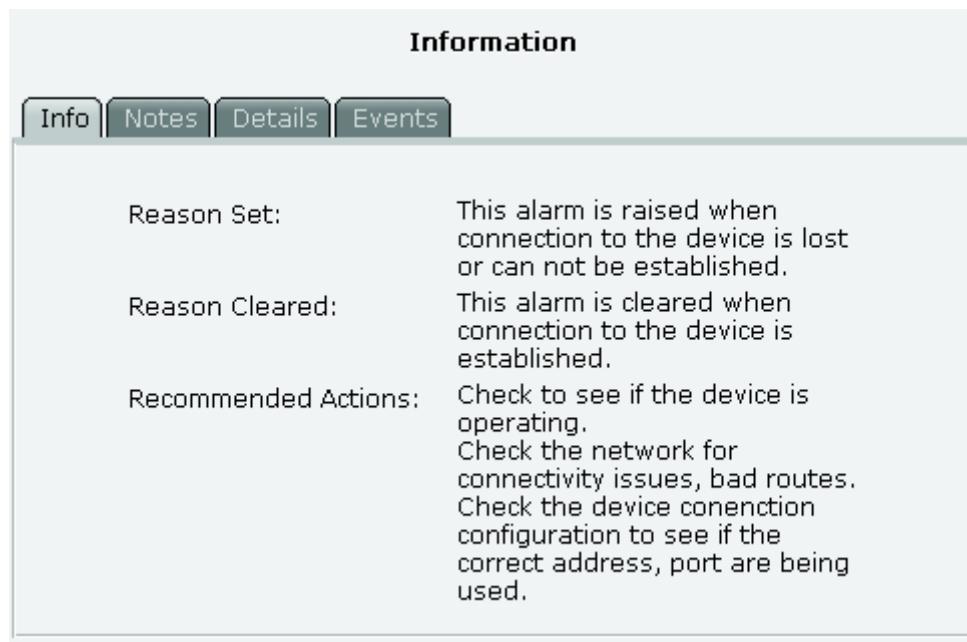


FIGURE 294. Info tab page

Reason Set	What causes this alarm to be raised.
Reason Cleared	What causes this alarm to be cleared.
Recommended Action	What the user could do to help clear this alarm

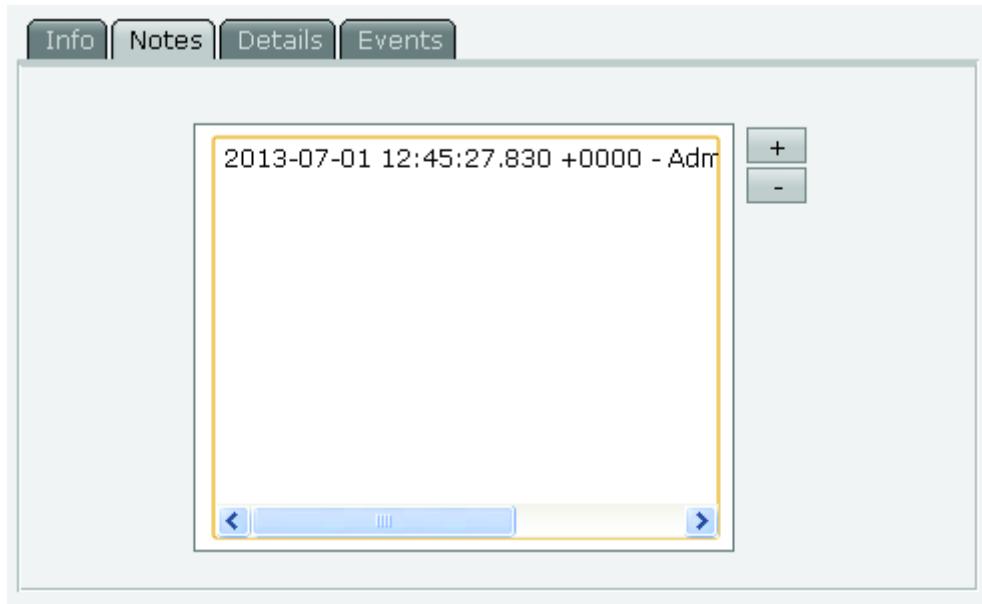


FIGURE 295. Notes tab page

The **Notes** tab page contains a text area that can be used to view notes that have been to the alarm. If the user has Alarms Note permission (see Chapter 3), a text field will be available where they can add a note using the **+ (add)** button. Notes will also be added by the system when an alarm is acknowledged.

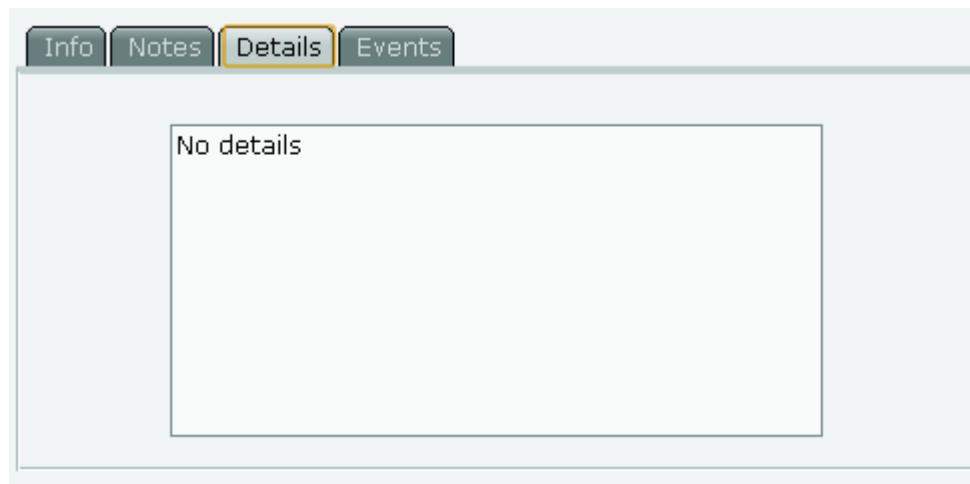


FIGURE 296. Details tab page

The **Details** tab page contains specific information about the particular alarm. The Details field is populated from the Details field of the last event that affected the alarm.

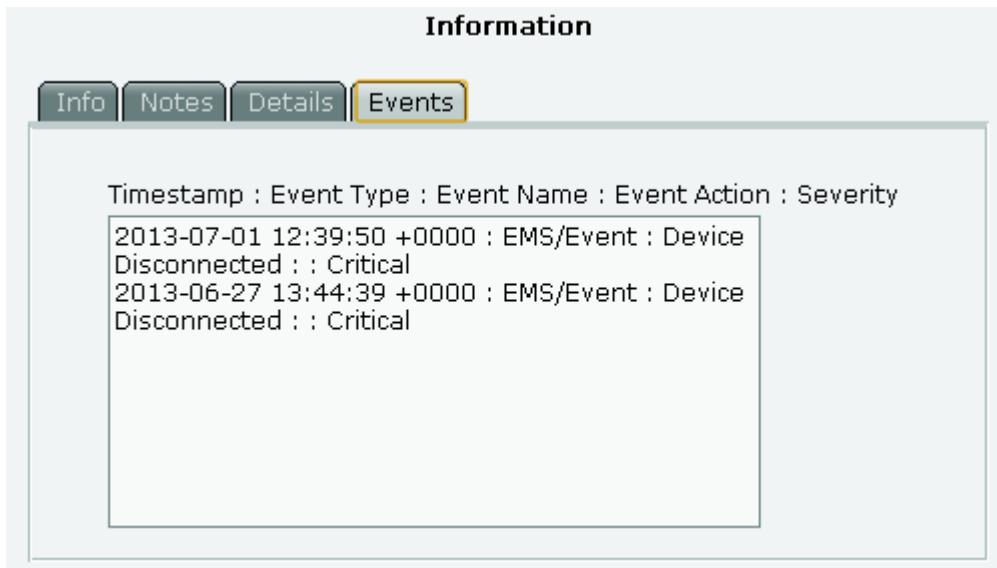


FIGURE 297. Events tab page

The **Events** tab page shows a list of events for the alarm. They are events that caused the alarm to be raised or cleared. The list contains the timestamp of the event, whether the alarm was set or cleared, and the event severity.

Alarms persist along with the events that generated them. Therefore, setting the purge time of events affects the lifecycle of alarms as well. Alarms will not be purged from the system while they are still set or have not yet been acknowledged.

Alarm Rules

Alarm rules are used to raise and clear alarms based on events. This allows an administrator to raise alarms on any event that is placed into the Event system. The alarm is named with the value specified in the **Alarm Name** field. The severity must also be specified or the alarm will be created in the Cleared state. If User Clearable is selected, the alarm will be able to be cleared using the **Clear** button in the Alarm table.

The alarm raised contains the Element ID, Object Type, and Object Key of the alarm even if the values are not specified as Alarm Rule index values.

Alarm Dependencies

Alarms are dependent on the Event System to generate events that will be turned into alarms.

Events

An **Event** represents the storage of information pertaining to an action or state related to a device, or sometimes IntelliView, that is important to log for reasons IntelliView upkeep, alarming, or inspection in the future. Events contain information about configuration changes, state changes, alarm conditions, and warnings or errors that have occurred in the devices. IntelliView will sometimes place information into the Event table concerning the device such as when a connection is lost and regained, but the majority of events are generated by the device itself and sent to IntelliView through a method of notification which is left up to the device.

Notifications

Notifications are handled in the Device Module layer. The module will be notified in a manner which is particular to the device being managed. The Device Module layer will receive this notification and convert it into an IntelliView event.

Events Table

The Events table shows a list of events and updates automatically when new events are added to the system.

	Time Stamp	Element	Event Type	Node ID	Name	Object Type	Object Key	Severity
<input type="checkbox"/>	2012-06-11 09:07:31.386 +00:00	Albany, NY In State	1007	MII_LOST				Info
<input type="checkbox"/>	2012-06-11 09:06:54.493 +00:00	Phoenix, AZ I. Alarm	1010	TCP/IP_UPLINK_UNA	IntelliVIEW/IntelliView_configure ./IntelliView/configuration/uplinks/tcp. Clear			
<input type="checkbox"/>	2012-06-11 09:06:33.140 +00:00	Iowa City, IA - State	1009	MII_DISCOVERED				Info
<input type="checkbox"/>	2012-06-11 09:06:33.137 +00:00	Iowa City, IA - Alarm	1009	TCP/IP_UPLINK_UNA	IntelliVIEW/IntelliView_configure ./IntelliView/configuration/uplinks/tcp. Clear			
<input type="checkbox"/>	2012-06-11 09:06:33.137 +00:00	Iowa City, IA - State	1009	MII_DISCOVERED				Info
<input type="checkbox"/>	2012-06-11 09:05:56.368 +00:00	Phoenix, AZ I. Alarm	1010	TCP/IP_UPLINK_UNA	IntelliVIEW/IntelliView_configure ./IntelliView/configuration/uplinks/tcp. Major			
<input type="checkbox"/>	2012-06-11 09:05:33.012 +00:00	Iowa City, IA - State	1009	MII_LOST				Info
<input type="checkbox"/>	2012-06-11 09:05:33.012 +00:00	Iowa City, IA - Alarm	1009	TCP/IP_UPLINK_UNA	IntelliVIEW/IntelliView_configure ./IntelliView/configuration/uplinks/tcp. Major			
<input type="checkbox"/>	2012-06-11 09:05:33.011 +00:00	Iowa City, IA - State	1009	MII_LOST				Info

FIGURE 298. Events table

An Events table is available on the Main screen to allow users to view incoming events.

If the event has a severity set, the background color of the row is set to the following:

- **Critical** - Red
- **Major** - Orange
- **Minor** - Yellow
- **Clear** - Green

The Events table is able to export table data to a CSV format stored on the user's desktop based on the table's current sorting and filtering.

Double-clicking on a row in the Events table displays the **Event Details** screen.

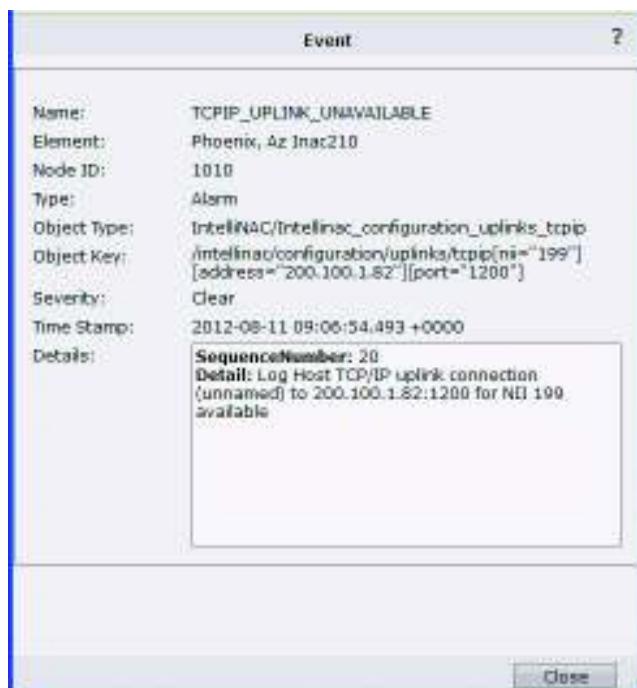


FIGURE 299. Event Details screen

Changing Elements

Elements placed in Maintenance mode will stop collecting events. Events that existed prior to the state change will not be purged, but new events will not be persisted.

Elements which are removed from the system will have their events purged from the database during the database archival phase.

Archiving

Event archiving occurs on a nightly basis at a time configured in IntelliView configuration. Events that are older than the configured age will be removed from the system into a single CSV file in a location specified. Each archived file will be stamped with the date which it is created. The archive will represent all events archived from the system for that day.

The archive settings include:

- Log Table Age Limit (days) - This setting sets how old a row in days a log entry will stay in the log table before it is archived.
- Database Archive File Age Limit (days) - This setting set how many days an archive file will stay in the archive directory before it is archived. This value has no relation to the data in the file. When the file has reached the age limit it will be deleted.
- Archive File Storage Directory - This is the directory which contains the archive files. If this directory is changed and there are archive files already in the directory, the files in the old directory will not be archived.
- Hour To Run (0-23) - The hour of the day to run database archival in a 24-hour day. 0 is midnight, 23 is 11 p.m.
- Minute To Run Archive 0-60 - The minute to run the archive. If a user wishes to archive at 2:30 a.m., the Hour To Run would be set to 2, and the Minute To Run would be set to 30.

Statistical Collection

Statistics are data captured and stored numerically for later retrieval in tabular form. The information can be used to verify the working condition of IntelliView and devices that it is monitoring. Information in IntelliView such as user requests made, alarms processed, and/or database queries made are available. Statistics on device models are also available for each status object in the model.

The values differ for IntelliView and the managed device.

IntelliView statistics include:

- Alarm System: This statistic tracks the alarm system and provides statistics on how many alarms are raised/acknowledged/cleared.
- Database: This statistic tracks read/write times to the database. This statistic is tracked as an object in the event multiple databases are used.
- Event System: This statistic tracks the number of events processed along with some statistics about how long it takes to process events.
- Message System: This statistic tracks the message system which is used internally by IntelliView to pass information from one system to another. It is also used to notify the GUI that changes have taken place and the screen needs to be updated. The statistic shows the number of message passed as well as some statistics on the size of the queue.
- Request Manager: This statistic tracks the requests made by clients and number of requests, and how long requests take.
- Security: This statistic tracks the login/logouts in the system and how many logins were successfully/failed.

IntelliNAC statistics include:

- PSTN ports (Analog)
- Downlinks
 - PSTN
 - TCP-IP
 - X.25
 - X.25 LAPB
 - X.25 Serial
- Ethernet Ports
- NAC to NAC Links
- NII CRI Lookup table
- NII DNIS Lookup table
- NII TCP-IP Lookup table
- NII X.25 lookup Table
- NII Learned
- PSTN ports (Digital)
- POS Protocols
- POS Transactions

- Uplinks
 - SNA
 - TCP-IP
 - X.25
 - X.25 LAPB
 - X.25 Serial

Statistics Viewing

There are two ways to show the Statistical collection:

One:

On the Main screen select **Statistics**

From the pull down menu select **Show Statistics**

Two:

On the Main screen **Right click** on the IntelliVIEW symbol

From the pull down menu select **Statistics**

From the extended pull down menu select **Show Statistics**

The **Statistics Selection** screen allows you to select statistics type, and if applicable, the object type and object to display.

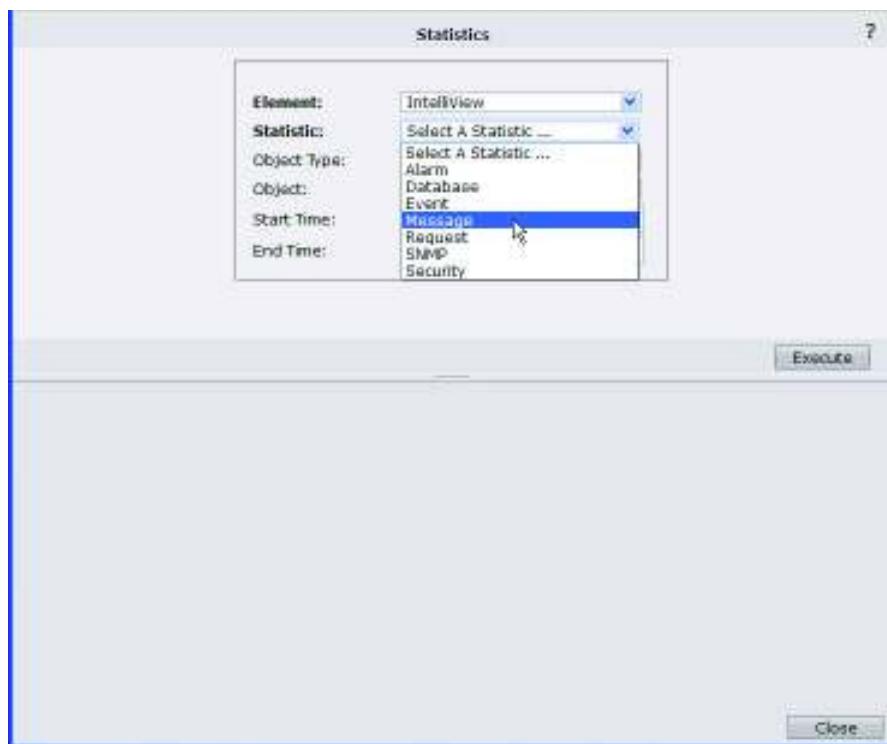
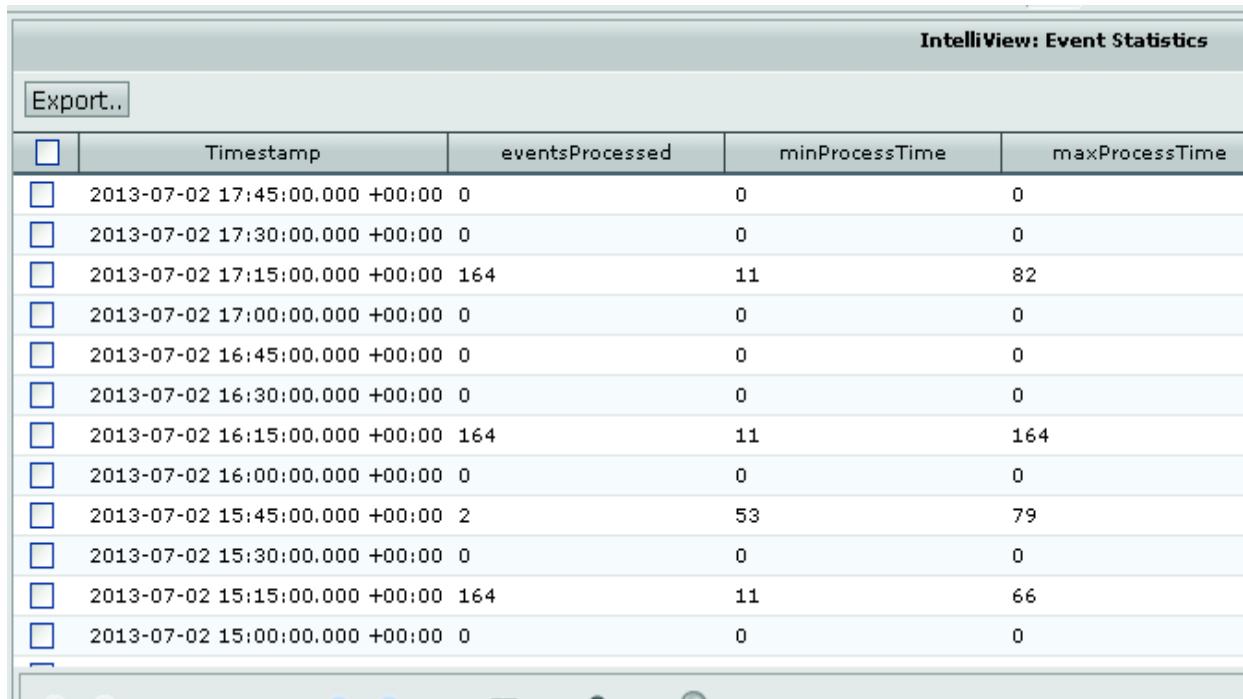


FIGURE 300. Statistics Selection screen

The fields include:

- **Element:** This field is filled in when the screen appears with the value for which the toolbar was pressed, IntelliView or any of the devices that IntelliView is managing. This value can be changed by the user so that any element's statistics can be viewed.
- **Statistic:** This value is populated with the available statistics types that are collected for the selected device.
- **Object:** The user can select which object to view the table of collected statistics. Some statistics do not require an object specification, but for interface and similar statistics, you must select an object.
- **Start/End Time:** These fields are used to set a time range for the values presented in the table section.



The screenshot shows a table titled "IntelliView: Event Statistics". The table has columns: a checkbox column, "Timestamp", "eventsProcessed", "minProcessTime", and "maxProcessTime". The data rows show various timestamp entries and their corresponding event counts and processing times. An "Export.." button is visible at the top left of the table area.

	Timestamp	eventsProcessed	minProcessTime	maxProcessTime
<input type="checkbox"/>	2013-07-02 17:45:00.000 +00:00 0	0	0	0
<input type="checkbox"/>	2013-07-02 17:30:00.000 +00:00 0	0	0	0
<input type="checkbox"/>	2013-07-02 17:15:00.000 +00:00 164	11	82	164
<input type="checkbox"/>	2013-07-02 17:00:00.000 +00:00 0	0	0	0
<input type="checkbox"/>	2013-07-02 16:45:00.000 +00:00 0	0	0	0
<input type="checkbox"/>	2013-07-02 16:30:00.000 +00:00 0	0	0	0
<input type="checkbox"/>	2013-07-02 16:15:00.000 +00:00 164	11	164	164
<input type="checkbox"/>	2013-07-02 16:00:00.000 +00:00 0	0	0	0
<input type="checkbox"/>	2013-07-02 15:45:00.000 +00:00 2	53	79	79
<input type="checkbox"/>	2013-07-02 15:30:00.000 +00:00 0	0	0	0
<input type="checkbox"/>	2013-07-02 15:15:00.000 +00:00 164	11	66	164
<input type="checkbox"/>	2013-07-02 15:00:00.000 +00:00 0	0	0	0

FIGURE 301. Statistics Display example screen

Export - Export a CSV file (Auto starts a browser download to your local machine)

Manual Statistically Repository management

Statistic directory repository can be managed (export, delete, Collect and Reset)

There are two ways to manually manage the Statistical collection:

One:

On the Main screen select **Statistics**

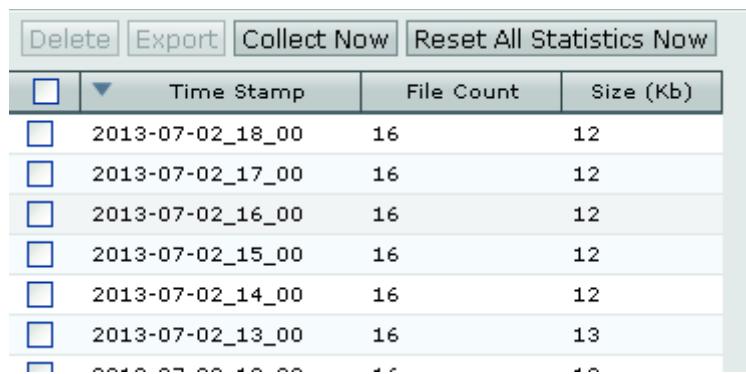
From the pull down menu select **Manage Stat. Repository**

Two:

On the Main screen **Right click** on the IntelliVIEW symbol

From the pull down menu select **Statistics**

From the extended pull down menu select **Manage Stat. Repository**



<input type="checkbox"/>	Time Stamp	File Count	Size (Kb)
<input type="checkbox"/>	2013-07-02_18_00	16	12
<input type="checkbox"/>	2013-07-02_17_00	16	12
<input type="checkbox"/>	2013-07-02_16_00	16	12
<input type="checkbox"/>	2013-07-02_15_00	16	12
<input type="checkbox"/>	2013-07-02_14_00	16	12
<input type="checkbox"/>	2013-07-02_13_00	16	13
<input type="checkbox"/>	2013-07-02_12_00	16	12

FIGURE 302. Statistics directory screen

- Delete - Deletes selected entries
- Export - Exports selected entry as a CSV file (Auto starts a browser download to your local machine)
- Collect Now - Forces an immediate collection of statistics from assigned devices
- Reset All Statistics Now - Forces an immediate reset of statistics of the assigned devices

Manual Collect Statistics

Statistic directory repository can be managed (export, delete, Collect and Reset)

There are two ways to manually manage the Statistical collection:

One:

On the Main screen select **Statistics**

From the pull down menu select **Collect Now**

Two:

On the Main screen **Right click** on the IntelliVIEW symbol

From the pull down menu select **Statistics**

From the extended pull down menu select **Collect Now**

Collect Now - Forces an immediate collection of statistics from assigned devices

Manual Reset All Statistics Now

Statistic directory repository can be managed (export, delete, Collect and Reset)

There are two ways to manually manage the Statistical collection:

One:

On the Main screen select **Statistics**

From the pull down menu select **Reset All Statistics Now**

Two:

On the Main screen **Right click** on the IntelliVIEW symbol

From the pull down menu select **Statistics**

From the extended pull down menu select **Reset All Statistics Now**

Reset All Statistics Now - Forces an immediate reset of statistics of the assigned devices

Exporting Statistics

Statistic directory repository can be export to your local machine.

Note only one directory at a time can be exported.

One:

On the Main screen select **Statistics**

From the pull down menu select **Show Statistics**

Two:

On the Main screen **Right click** on the IntelliVIEW symbol

From the pull down menu select **Statistics**

From the extended pull down menu select **Show Statistics**

Select statistic to export by

- Selecting the device
- Selecting the statistic to be exported
- Select Object type if applicable
- Select Object if applicable: (port, IP address, Protocols, NII's, etc..)
- Start/End Time: Set a time range for the values presented in the table section.

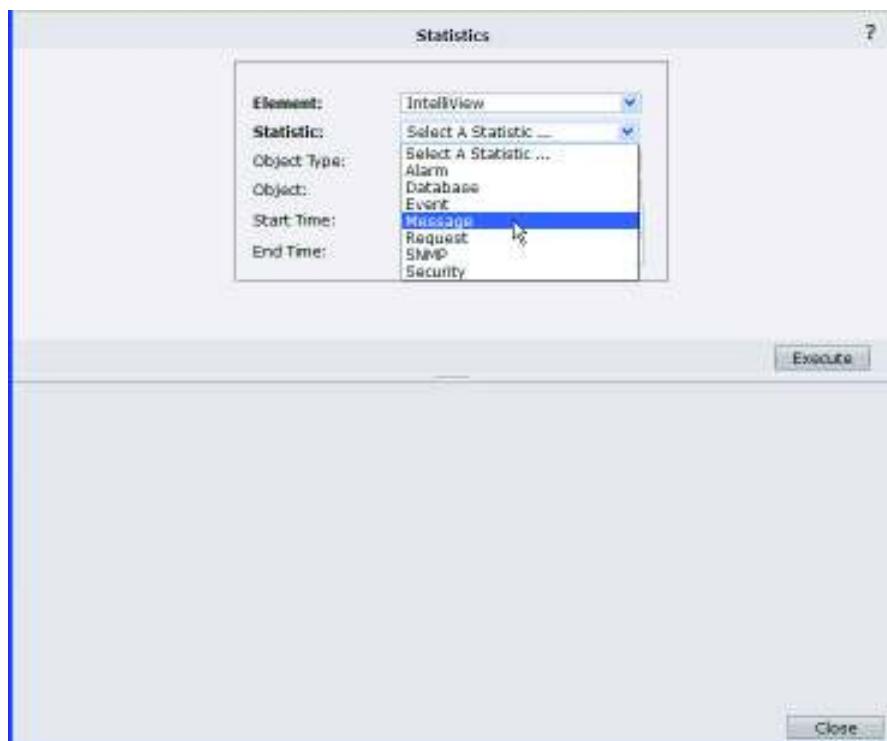


FIGURE 303. Statistics Selection screen

IntelliView: Event Statistics				
<input type="button" value="Export.."/>				
	Timestamp	eventsProcessed	minProcessTime	maxProcessTime
<input type="checkbox"/>	2013-07-02 17:45:00.000 +00:00	0	0	0
<input type="checkbox"/>	2013-07-02 17:30:00.000 +00:00	0	0	0
<input type="checkbox"/>	2013-07-02 17:15:00.000 +00:00	164	11	82
<input type="checkbox"/>	2013-07-02 17:00:00.000 +00:00	0	0	0
<input type="checkbox"/>	2013-07-02 16:45:00.000 +00:00	0	0	0
<input type="checkbox"/>	2013-07-02 16:30:00.000 +00:00	0	0	0
<input type="checkbox"/>	2013-07-02 16:15:00.000 +00:00	164	11	164
<input type="checkbox"/>	2013-07-02 16:00:00.000 +00:00	0	0	0
<input type="checkbox"/>	2013-07-02 15:45:00.000 +00:00	2	53	79
<input type="checkbox"/>	2013-07-02 15:30:00.000 +00:00	0	0	0
<input type="checkbox"/>	2013-07-02 15:15:00.000 +00:00	164	11	66
<input type="checkbox"/>	2013-07-02 15:00:00.000 +00:00	0	0	0

FIGURE 304. Statistics record example screen

- Select the record to export (only one at a time)
- Click **Export**

A download will start. The CSV file will download to the machine you are using your browser on.

The CSV format file structure (column headers) will be based on the statistic record exported.

```
"Timestamp","address","port","name","callsAccepted","callsRejected","callsTotal"
"2013-07-03 12:30:00.000 +00000","172.16.1.210","1221","172..210:1221","0","0",''
"2013-07-03 12:15:00.000 +00000","172.16.1.210","1221","172..210:1221","0","0",''
"2013-07-03 12:00:00.000 +00000","172.16.1.210","1221","172..210:1221","0","0",''
"2013-07-03 11:45:00.000 +00000","172.16.1.210","1221","172..210:1221","0","0",''
"2013-07-03 11:30:00.000 +00000","172.16.1.210","1221","172..210:1221","0","0",''
"2013-07-03 11:15:00.000 +00000","172.16.1.210","1221","172..210:1221","0","0",''
"2013-07-03 11:00:00.000 +00000","172.16.1.210","1221","172..210:1221","0","0",''
"2013-07-03 10:45:00.000 +00000","172.16.1.210","1221","172..210:1221","0","0",''
"2013-07-03 10:30:00.000 +00000","172.16.1.210","1221","172..210:1221","0","0",''
-----
```

FIGURE 305. Statistics CSV example screen

Electronic Funds Transfer Security

EFTSec TPDU Pass Through

Identifies a message as an EFTSec message and automatically routes the message to an EFTSec server.

Constraints

When internal EFTSec processing is disabled, and an

EFTSEC Operation

The EFTSec pass thru feature works as follows:

EFTSec message is received, identified by a TPDU ID of 0x70, the IntelliNAC automatically routes the entire message to the appropriate uplink using the destination NII. The 0x70 TPDU ID is maintained by the IntelliNAC. When a host response is returned to the terminal, the maintained TPDU source and destination fields are swapped and placed in the TPDU header, and the TPDU ID is set to the standard value of 0x60.

The EFTSec TPDU message format is described below. The number of bits in each field is shown in the header as a subscript.

TPDU			EDS				
TPDU ID ₈ = 0x70	NII ₁₆	SRC ₁₆	Control 4	KIN ₁₂	Start ₁₆	Length ₁₆	Checksum ₈

FIGURE 306. EFTSec Message Format

CHAPTER 6

Diagnostics

Overview

This section details the diagnostic capabilities of IntelliView. These capabilities are available for each IntelliView installation regardless of your configuration. They include operations such as:

- Serial interfaces (X.25, SNA, RS232 or V.35)
- Analog PSTN
- Digital PSTN (ISDN, CAS and CCS) T1 or E1

The goals of the diagnostics is to:

- Validate physical interface operation
- Trouble shoot operational issues
- Help analysis network congestion.

Media Trace

The Media Trace feature is used to capture additional interface level data when the standard Log Viewer trace data is insufficient to diagnose the problem. The Media Trace is supported on all currently supported I/O Modules and is enabled or disabled by the Toggle Trace button on the Operational Status Ports screen.

Constraints

The system allows multiple concurrent media trace operations on the Serial I/O Modules but the PSTN cards are limited to one active media trace operation at a time. As a protection feature, if

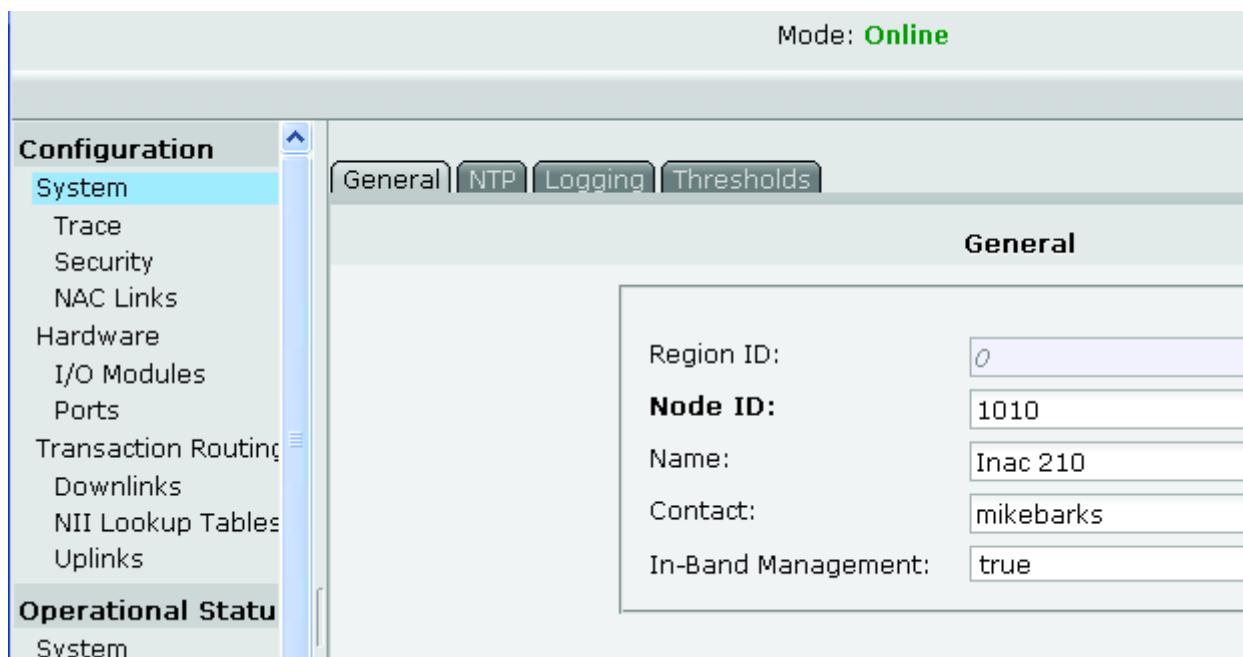
the media trace is accidentally left on it will automatically shut off after recording 2.2 million lines of trace data.

Media Trace Operation

Enable Trace

To enable or disable Media Trace on a given port, select the port and click on the “Toggle Trace” button. See step by step below. The system will ask for confirmation and then indicate the current state of the trace. Repeat for multiple Serial port traces. Note if a second PSTN trace is enabled, the system will terminate first trace. Note: confirmation will be prompted for termination.

1. On Map click on node of the port to traced
2. Click on tool bar icon “Config App”



3. Select “Ports” view under “Operational Status” (right side bar)

The screenshot shows the IntelliView User Guide interface for Media Trace. On the left, there are two vertical navigation menus:

- Configuration**:
 - System
 - Trace
 - Security
 - NAC Links
 - Hardware
 - I/O Modules
 - Ports
 - Transaction Routing
 - Downlinks
 - NII Lookup Tables
 - Uplinks
- Operational Status**:
 - System
 - Security
 - NAC Links
 - Networking
 - Hardware
 - Control Module
 - Resources
 - Sensors
 - I/O Modules
 - Ports** (highlighted with a blue background)
 - Transaction Routing

The main panel on the right displays a table titled "Media Trace" with the following data:

	Port Id	Name	IPAddress
<input type="checkbox"/>	1	Management	172.16.1.210
<input type="checkbox"/>	2	eth 1	172.16.3.210
<input type="checkbox"/>	3	inband for 20	172.16.2.210
<input type="checkbox"/>	4	remote	20.20.20.70

Below the table are tabs for "Ethernet", "PSTN", "DSO Ch Status", and "Analog". At the top of the main panel, there are buttons for "Media Trace" and "Export..".

4. Select port to be traced "Port Tab"
5. Select "Port" to be traced and click "Media Trace"

The system will ask for confirmation and then indicate the current state of the trace.

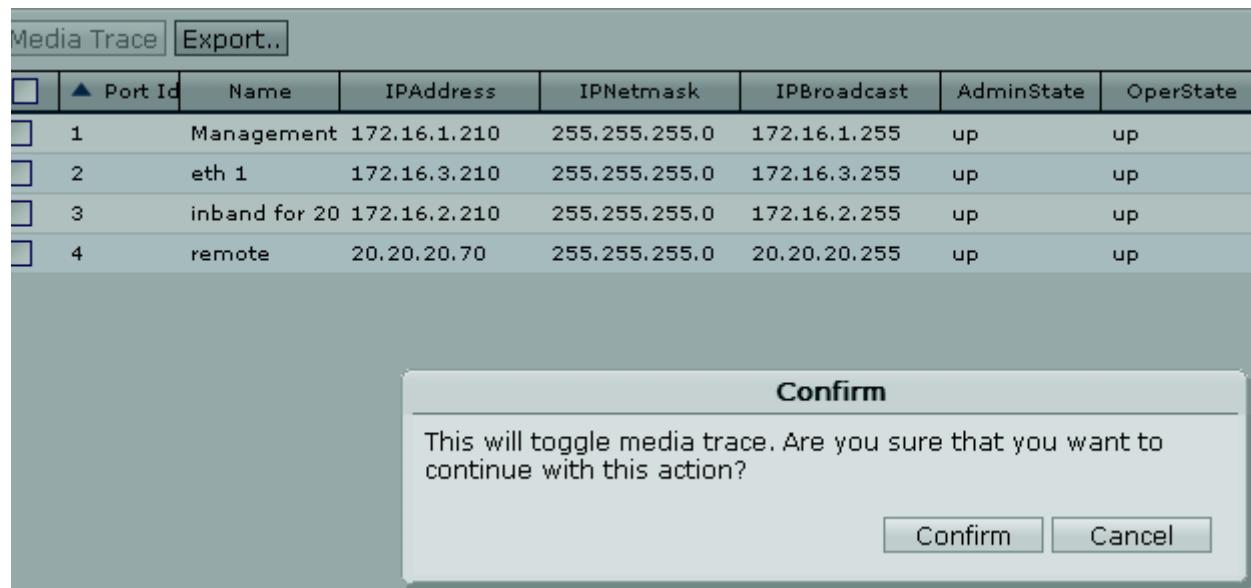


FIGURE 307. Trace Toggle Confirmation

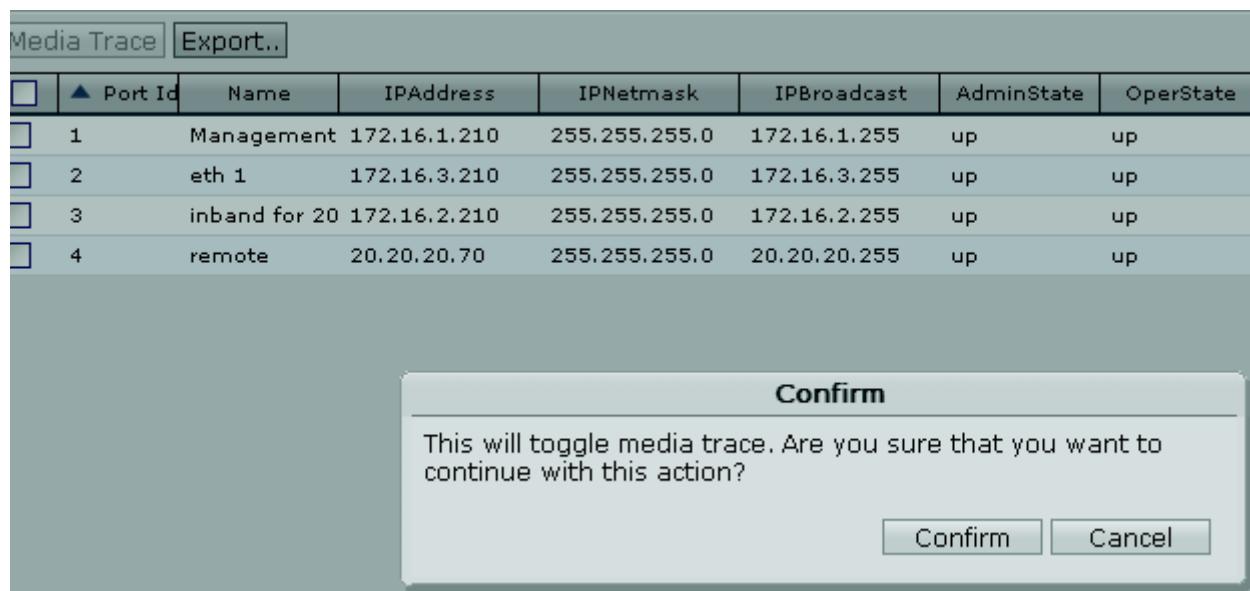
Disable Trace

To disable Media Trace on a given port, select the port and click on the “Toggle Trace” button. See step by step below. The system will ask for confirmation and then indicate the current state of the trace.

FIGURE 308. Trace Disable

1. On Map click on node of the port to traced
2. Click on tool bar icon “Config App”
3. In “Config App” Screen select “Ports” view under “Operational Status” (right side bar)
4. Select “Port Tab” to be traced
5. Select “Port” to be traced and click “Media Trace”

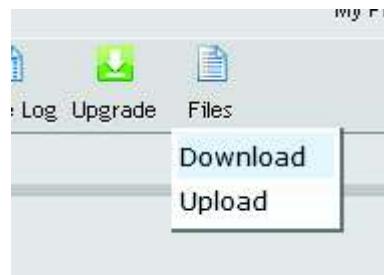
The system will ask for confirmation and then indicate the current state of the trace.

**FIGURE 309. Trace Disable Confirmation**

View Trace Activity

To view all active media trace operations, go to “File” tab, select “diag-tracefile” and click the “List” button. An active media trace operation is indicated by updates to the File Size or Created timestamp as viewed after a Refresh operation.

1. On Map click on node of the port being traced
2. Click on tool bar icon “Files”



3. In “File Type” Screen select “Diag-tracefile” click “List”



4. View the file size incrementing

Files on Device: Phoenix,AZ Inac209 In Band

File Type: **diag-tracefile**

[Li]

Device File Listing

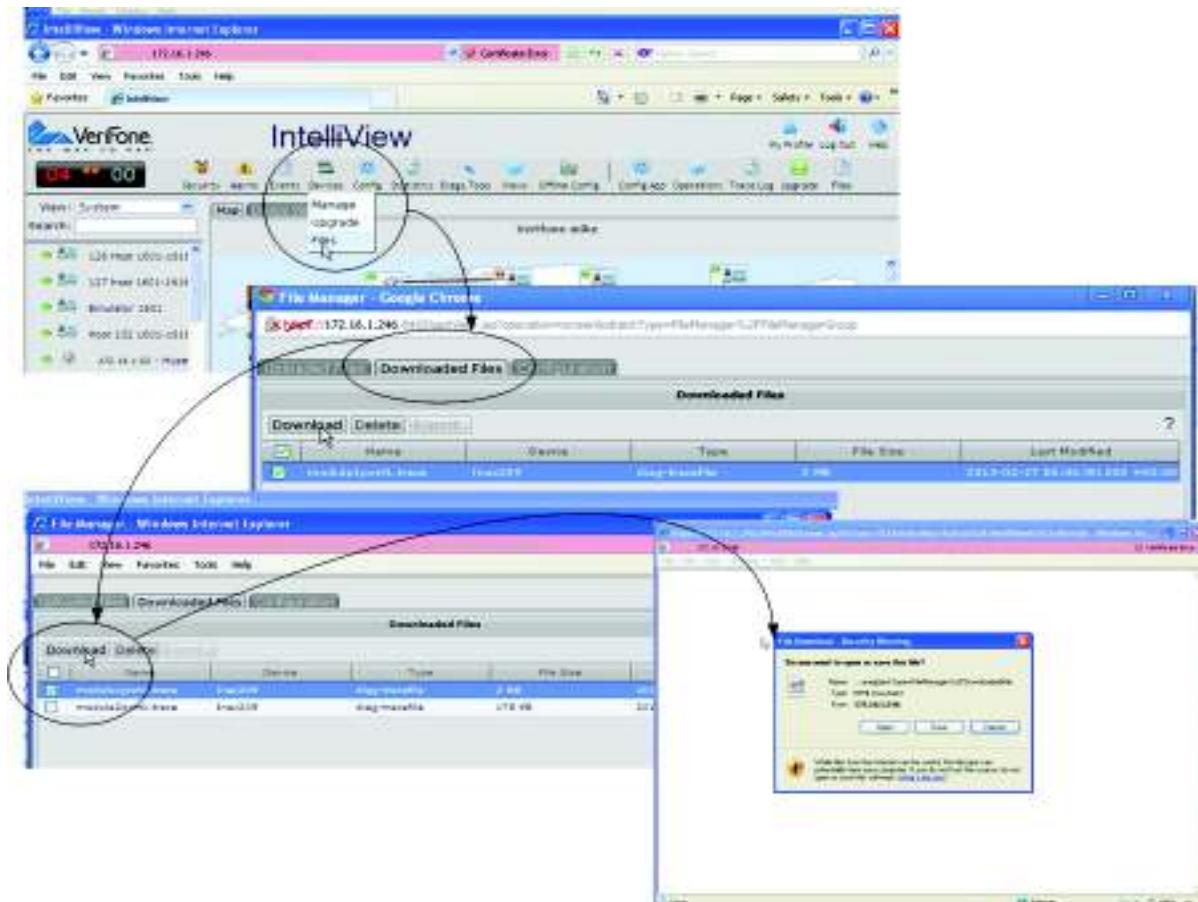
[Download from Device](#) [Delete](#) [Export..](#)

	Name	Type	File Size	Created
<input type="checkbox"/>	ethernetPort4.trace	diag-tracefile	20 KB	2013-07-02 10:15:17.000 +0
<input type="checkbox"/>	ethernetPort3.trace	diag-tracefile	0 bytes	2013-07-02 10:11:43.000 +0

FIGURE 310. Trace Activity Status

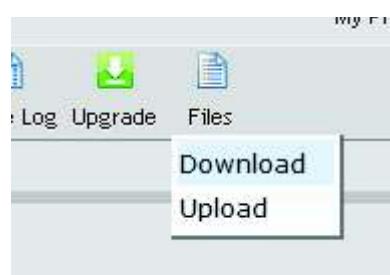
View Trace Data

To view the trace data is a two step process, first you must download the trace file from the IntelliNAC to IntelliView. Second download the trace file from IntelliView to a local service (PC)



with basic edit tools).

- 1.
2. On the Main screen (Map page) select “file” icon in the tool bar (far right)
3. Select download from pull down menu



4. Ensure “File Type” is “diag-tracefile”



5. Select file to be downloaded (note file name as it will be needed later)
6. Click "Download from Device"

Device File List			
	Name	Type	File Size
<input checked="" type="checkbox"/>	ethernetPort4.trace	diag-tracefile	258 KB
<input type="checkbox"/>	ethernetPort3.trace	diag-tracefile	0 bytes

7. Click "OK" to confirm

Once the image has been downloaded to IntelliView, you can download it to your PC and save it to your local drive. The file can be viewed with a basic word processor program.

8. Return to "Main Screen" (Map View)
9. Click on the "Devices" icon tool bar (fourth from the left) select "files"
10. On "Files" screen select "Download Files" tab
11. Select trace file to be downloaded (use remembered file name and INAC node)

Recommended that you save the file in a known location before viewing.

Typical view of trace file.

```
Starting trace... (Press ENTER to exit)

INCOMING      Len=62  TimeStamp=33387  Feb 26 08:29:03 987402 [1/100s]
Raw (HEX)      03 00 10 10 40 02 10 30 38 01 00 0E 80 00 00 00

OUTGOING      Len=2   TimeStamp=33387  Feb 26 08:29:03 987414 [1/100s]
Raw (HEX)      03 21

OUTGOING      Len=5   TimeStamp=33387  Feb 26 08:29:03 987435 [1/100s]
Raw (HEX)      01 20 10 10 21

OUTGOING      Len=16  TimeStamp=33390  Feb 26 08:29:03 990493 [1/100s]
Raw (HEX)      01 22 10 0F 0B 55 20 31 22 03 11 00 01 00 00 00
```

FIGURE 311. Downloaded Trace file from IntelliNAC

Transaction Trace

The transaction trace utility consists of an IntelliNAC processor and the Logging application. The processor is used to retrieving logs, polling for logs, and other trace log communication with an IntelliNAC. The application is a core IntelliView module and is used to store, manage, and view trace logs from an IntelliNAC.

To utilize, the IntelliNAC must be configured for trace logging through the Config application and the IntelliNAC device in IntelliView must periodically check for new trace logs (as a managed element). Once the trace logs have been downloaded and given to the Logging application, the Travel Log Viewer can be used to examine the logs using the buttons on the various configuration screens.

Logging Application Permissions

There are four privilege levels:

- **None:** The viewer is not available to the user
- **View:** The user can display logs and the GUI menu choice is visible
- **Manage:** The user can set properties for the Logging Application
- **Action:** If available, the user is allow to the Fetch Now function.

Note: Because the Transaction Trace utility communicates with IntelliNAC devices through IntelliView, the Configuration and Manage Devices permissions also apply.

Trace Collection

The settings for trace collection are part of the Managed Element screen for IntelliNAC device properties:

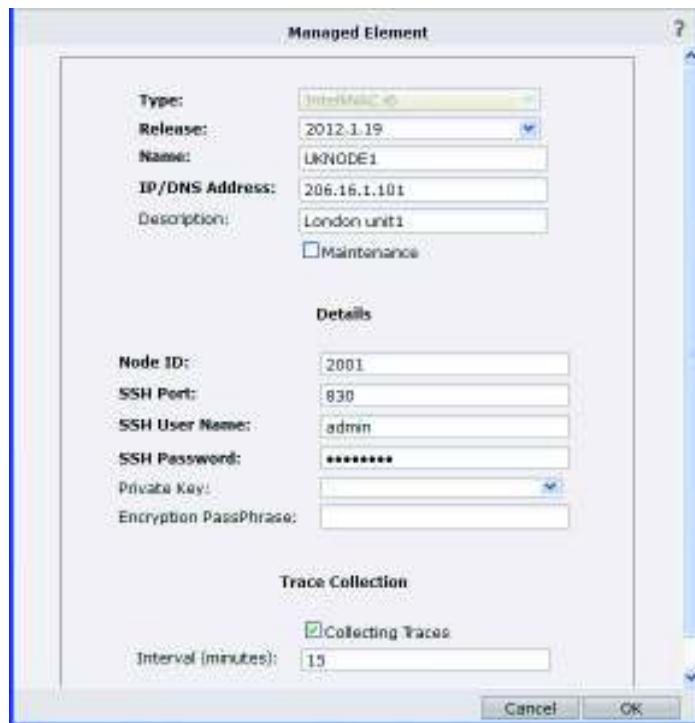


FIGURE 312. Managed Element screen - trace collection settings

- **Collecting Traces:** Select to enable regular polling of the device and to allow downloading of the latest trace logs from the device
- **Interval (minutes):** This is the number of minutes the system will wait until checking again after checking for new files, downloading, and processing of any new trace logs.

Trace Log Viewer

The **Trace Log** displays the specific transaction trace logs of an IntelliNAC device. It is available from the toolbar and the right-click menu of an IntelliNAC device if the user has at least view privileges for the Logging Application.

	Timestamp	Microsecond	transaction	class	text
	2012-08-11 12:39:29 +00:00	297605	14622	TRANS_PROCESSING	Transaction failed (jHost connect error)
	2012-08-11 12:39:29 +00:00	297599	14622	CALL_CONTROL	Call disconnect received by downlink
	2012-08-11 12:39:29 +00:00	297547	14622	TRANS_PROCESSING	Logging record sent to NII 299 (status: 3C)
	2012-08-11 12:39:29 +00:00	297536	14622	TRANS_PROCESSING	Logging record sent to NII 199 (status: 3C)
	2012-08-11 12:39:29 +00:00	297525	14622	PROTO_PROCESSING	{END} Logging data (length: 116): 47 02 00 70 00 D1
	2012-08-11 12:39:29 +00:00	297458	14622	UPLINK	{DISCONNECT_HOST} Uplink successfully disconnected
	2012-08-11 12:39:29 +00:00	297423	11722	TRANS_PROCESSING	Transaction failed (jHost connect error)
	2012-08-11 12:39:29 +00:00	297380	11722	TRANS_PROCESSING	Logging record sent to NII 299 (status: 3C)
	2012-08-11 12:39:29 +00:00	297369	11722	TRANS_PROCESSING	Logging record sent to NII 199 (status: 3C)
	2012-08-11 12:39:29 +00:00	297257	11722	PROTO_PROCESSING	{END} Logging data (length: 116): 47 02 00 70 00 D1
	2012-08-11 12:39:29 +00:00	297237	11722	CALL_CONTROL	Call disconnect received by downlink
	2012-08-11 12:39:29 +00:00	297289	11722	UPLINK	{DISCONNECT_HOST} Uplink successfully disconnected
	2012-08-11 12:39:29 +00:00	294695	13165	TRANS_PROCESSING	{CONNECT_HOST} Status set to 'Host connect error'
	2012-08-11 12:39:29 +00:00	294691	13165	UPLINK	{CONNECT_HOST} Uplink connect attempt failed
	2012-08-11 12:39:29 +00:00	294667	13432	TRANS_PROCESSING	{CONNECT_HOST} Status set to 'Host connect error'
	2012-08-11 12:39:29 +00:00	294661	13432	UPLINK	{CONNECT_HOST} Uplink connect attempt failed
	2012-08-11 12:39:29 +00:00	292674	13165	UPLINK	{CONNECT_HOST} TCP/IP uplink [address:port: 200.1]
	2012-08-11 12:39:29 +00:00	292667	13165	UPLINK	{CONNECT_HOST} Uplink found on INAC_001502A255
	2012-08-11 12:39:29 +00:00	292647	13165	DOWNLINK	{GET_TPOU} TPOU removed from PQS request (0x40 2)
	2012-08-11 12:39:29 +00:00	292629	13165	DOWNLINK	{START} Data received from PQS (132 bytes)
	2012-08-11 12:39:29 +00:00	292527	13432	UPLINK	{CONNECT_HOST} TCP/IP uplink [address:port: 200.1]

FIGURE 313. Trace Log Viewer

Two date/time fields are used to scope the time of the trace logs that are of interest to the user. Note, it is not necessary to enter a value in either field, but performance can be noticeably slowed if the entire log must be filtered or sorted.

The fields are:

- **Start Time:** Log entries before this time will not be displayed
- **End Time:** Log entries after this time will not be displayed

Click the **Apply** button to apply the start and end time filters to retrieve the resultant log entries.

The start and end time remain in effect for all sorting and filtering operations as well as refreshing the data in the table.

Log Table Controls

The log table controls work a bit different from the rest of the tables:

- **New Data Available**

When the Logging Application receives new data from the device, the highlighted Refresh icon indicates this and a change to the tooltip. Click on the icon to refresh the data in the view. Depending on the filter settings, sort order, start and end times, there may be no noticeable change to the view when refreshed.

- **Paging Controls**

Sorting and the default sort order of chronologically the most recent entries shows the last page as the first page. Paging controls to the next, previous, and first page of the sorted data set are available.

- Page Size Selection

Page size sets the size of the pages of data and the maximum number of rows that will be displayed at once in the table.

- Sorting and Filtering

Sorting can be performed on the Timestamp column only. The default order is the most recent log entries first. Filtering can be performed on all of the columns except the Timestamp column.

- Buttons

The buttons provided by the trace log output table direct the user to other portions of the IntelliNAC management:

- **Trace Control:** Enable/disable tracing on the IntelliNAC. The Trace Control and Trace Rules buttons launch screens from the Device Configuration application which communicate directly with the IntelliNAC. Current communication with the IntelliNAC is required. The user must have view privilege in the Configuration permission to see the configuration and view/modify to make modifications.
- **Trace Rules:** Manage the trace rules defined on the IntelliNAC
- **Trace Collection:** Manage the collection of trace logs from the IntelliNAC. Trace Collection opens up the Devices screen. This requires view privilege in the Managed Devices permission to see the settings and view/modify to change the settings.
- **Fetch Logs:** Tells the IntelliNAC to immediately roll the latest trace log output into a CSV file. The Fetch Logs button invokes an operation on the IntelliNAC and requires the user to have action privilege for the Logging Application and communication with the IntelliNAC. The operation results are displayed as a confirmation on the screen. The operation may have succeeded, but there is no guarantee that a file or new data will result. If there is no trace log data available on the IntelliNAC to roll to a CSV file, then no new data will become available.
- **Export:** Export the table to a CSV file

Log Application Configuration

Trace logs age out from the system as a task simultaneous with Database Archiving. Files which are older than the age limit are deleted. The **Trace Log Age Out** setting is located on the Log App Configuration screen.

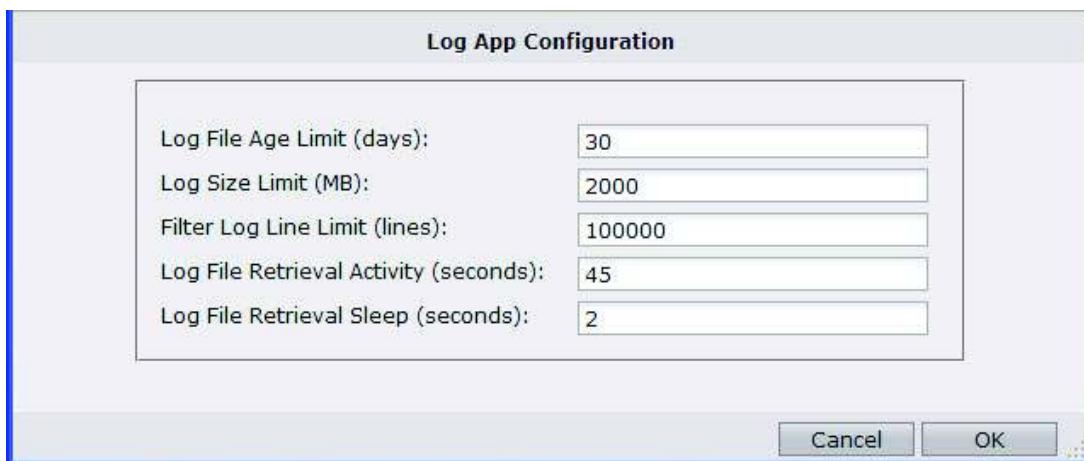


FIGURE 314. Log Application Configuration screen

The IntelliNAC from which to collect logs must be configured with tracing enabled and trace rules to establish parameters for collecting the trace logs.

Log File Management

The Logging Application uses files on the file system and only loads a page of the trace logs one at a time. Each page requested by the Trace Log Viewer requires going back to the files' system to get the next page.

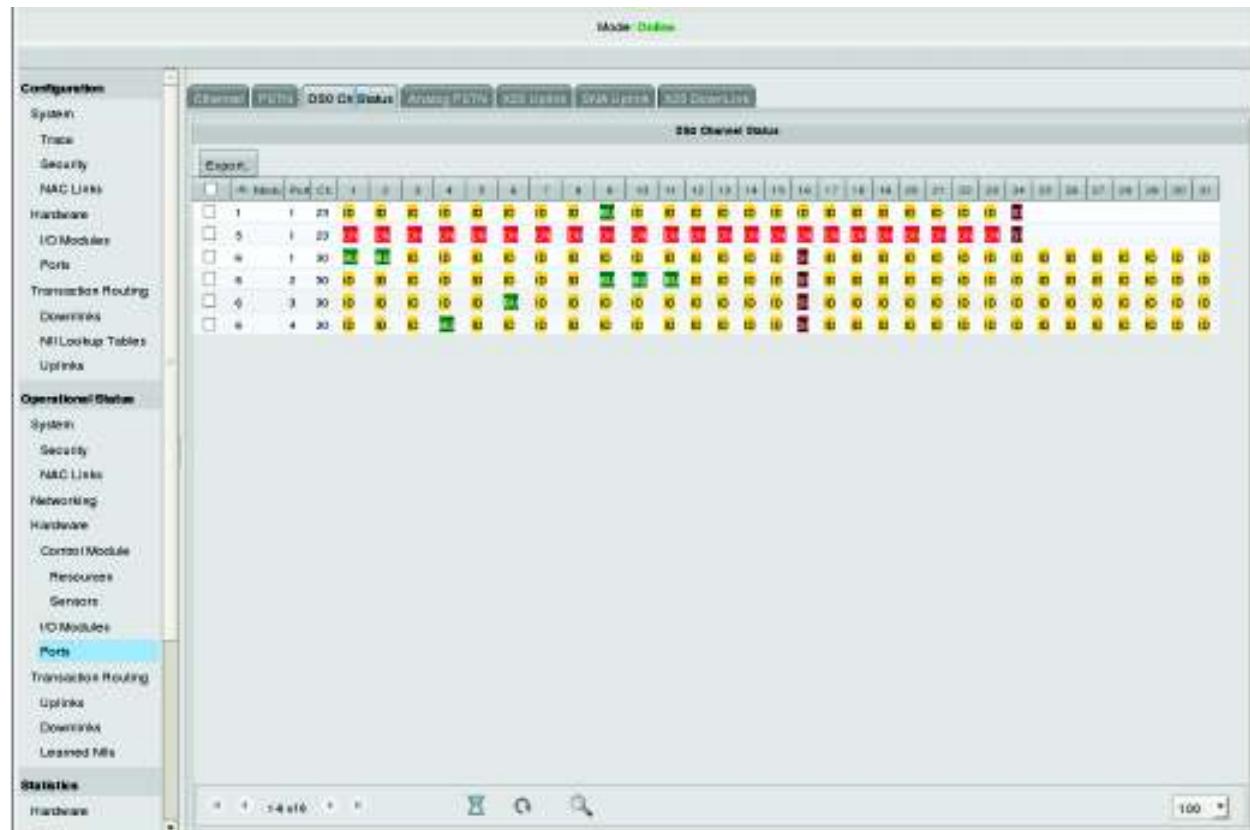
If an empty file (only contains a header) is given to the Logging Application, the file is immediately deleted from the file system.

The Trace Log depends on the Logging Application to provide a viewer with filter and sorting capabilities on its dataset. It also relies on the Logging Application to manage the trace log files after they have been downloaded and given to the Logging Application.

Note: The Logging Application assumes the files given to it are CSV formatted with chronologically ordered lines from the beginning of the file to the end of the file. A header is the first line in the file.

DS0 Channel Display

The DS0 Channel Display feature is used to capture additional DS0 interface level activity when the standard Log Viewer trace data is insufficient to diagnose the problem. The DS0 is supported on all currently supported Digital PSTN I/O Modules.



Constraints

The DS0 Channel Display is a snap shot of the state of the DS-0 channels. To refresh the display click the circle arrow located in the lower edge of the screen.

View DS0 Channel Status

- 12.On Map click on node of the port to be displayed
- 13.Click on tool bar icon “Config App”
- 14.In “Config App” Screen select “Ports” view under “Operational Status” (right side bar)
- 15.Select “DS0 CH Status” tab to be traced

To refresh the display click the circle arrow located in the lower edge of the screen

FIGURE 315. DS0 Status Display

BK	Blocked (Royal Blue 2)	Channel is blocked by Switch
BU	Busy (Medium Forest Green)	Channel is in use.
ID	Idle(Gold 1)	Channel is Idle and available
SI	Signaling (Indian Red)	Signaling Channel (non – B Channel). Channel 24 on T1 and Channel 16 on E1 trunks.
DN	Down (Red)	Trunk is down due to administrative action or external influences (affects all channels on the port)
NH	No Host (Dark Slate Gray)	No Host Transaction NII is available. This status is global and affects all ports and all channels in the chassis.

