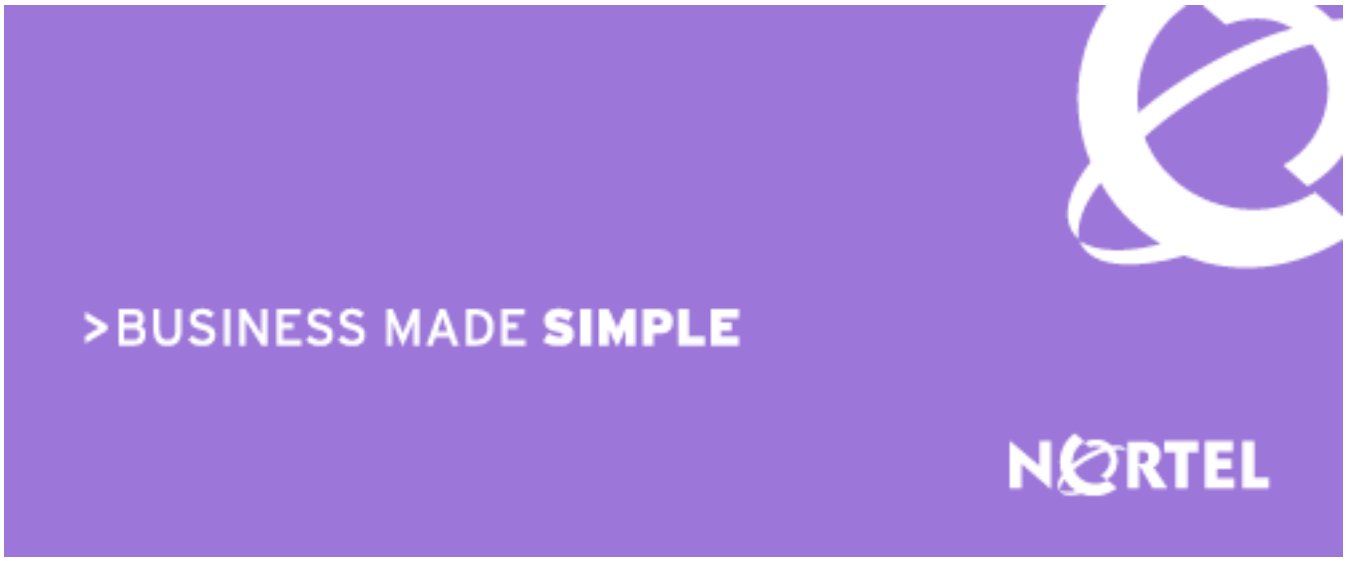


Nortel Healthcare Solutions
Mobile Device Checkout Release 2.0.1

Mobile Device Checkout Release 2.0.1 Administration Guide

Document Date: April 12, 2010
Document Number: NN49010-600
Document Release: 2.1

Copyright © 2010 Nortel Networks. All rights reserved.
NORTEL NETWORKS CONFIDENTIAL: The information contained in this document is the property of Nortel Networks. Except as specifically authorized in writing by Nortel Networks, the holder of this document shall not copy or otherwise reproduce, or modify, in whole or in part, this document or the information contained herein. The holder of this document shall keep the information contained herein confidential and protect same from disclosure and dissemination to third parties and use same solely for the training of authorized individuals.

Nortel and the Nortel logo are trademarks of Nortel Networks.

Red Hat, Red Hat Enterprise Linux, Red Hat Network are registered trademarks of Red Hat, Inc. Linux is a registered trademark of Linus Torvalds.

Microsoft, Windows, ActiveSync, Microsoft Windows 2003 Server, Microsoft Windows 2000 Server, Microsoft Windows Vista and Microsoft Windows XP professional are either registered trademarks or trademarks of Microsoft Corporation.

MOTOROLA and the Stylized M Logo and Symbol and the Symbol logo are registered in the US Patent & Trademark Office. Bluetooth is a registered trademark of Bluetooth SIG.

SynTrack is a trademark of Integrated Business Systems and Services (IBSS)

Ekahau, Ekahau Vision and EPE (Ekahau Positioning Engine) is a trademark of Ekahau

Firefox and the Firefox logos are trademarks of the Mozilla Foundation.

KDT900 is a trademark of America Microsystems, Ltd.

All other product or service names are the property of their respective owners.

Disclaimer
This document contains the best information available at the time of publication in terms of supporting the application and engineering of Nortel products in the customer environment. They are solely for the use by Nortel customers and meant as a guide for network engineers and planners from a network engineering perspective. All information is subject to interpretation based on internal Nortel test methodologies which were used to derive the various capacity and equipment performance criteria and should be reviewed with Nortel engineering primes prior to implementation in a live environment.

The information is subject to change without prior notice. The information in this document does not represent a commitment on the part of Nortel Networks.

Table of Contents

TABLE OF CONTENTS **3**
LIST OF FIGURES **7**
LIST OF TABLES **13**
1 WHAT'S NEW IN THIS RELEASE **14**
2 INTRODUCTION **16**
2.1 PURPOSE AND SCOPE 16
2.2 TARGET AUDIENCE 17
2.3 ASSUMPTIONS 17
2.4 EXCLUSIONS 17
3 MDC SOLUTION OVERVIEW **18**
4 COMPONENTS OVERVIEW **22**
4.1 TELEPHONY NETWORK OVERVIEW 22
4.1.1 Communication Server 1000 ..... *22*
4.1.2 Communication Server 2100 ..... *24*
4.1.3 WLAN Network *24*
4.1.4 WLAN Telephony Manager 2245 ..... *25*
4.1.5 WLAN IP Phone Sets *25*
4.2 MOBILE DEVICE CHECKOUT COMPONENTS 25
4.2.1 MDC Station *26*
4.2.2 MDC Server *27*
4.2.3 MDC Management Station *28*
4.2.3.1 Barcode Specifics 28
4.2.3.2 Barcode Reader 30
4.2.3.3 Barcode Printer 31
4.2.4 Ekahau Real Time Location System *31*
4.2.5 IBSS SynTrack for Healthcare *33*
4.2.6 Ekahau Vision *33*
5 MDC ADMINISTRATION GUI **34**
5.1 RECOMMENDED WEB BROWSER SETTINGS 35
5.2 MDC ADMIN GUI PRESENTATION CONVENTIONS 35
5.2.1 MDC Admin GUI Layout *35*
5.2.2 Password Rules *37*
5.2.3 Format of IP Addresses *37*
5.2.4 MDC Admin GUI Paging, Sort, and Search *37*
5.2.4.1 View using Paging 38
5.2.4.2 View using Sort 39
5.2.4.3 View using Search 41
5.3 LOGIN AND SYSTEM PAGE 43
5.4 CHANGING THE ADMIN DEFAULT PASSWORD AND EMAIL 45
5.5 SELECT LANGUAGE 47
5.6 HELP 47
5.7 CONFIGURE 48
5.8 ADMIN 49
5.8.1 View Admin Users *49*
5.8.2 Insert Admin User *50*
5.8.3 Update Admin User *51*
5.8.4 Delete Admin User *53*

5.9 LOGS AND ALARMS 54
5.9.1 View Logs 54
5.9.2 Print Logs 56
5.9.3 Save Log to File 58
5.9.4 XML Dump of Log 59
5.9.5 Configure Email Recipient for Logs 60
5.9.6 Configure Alarms 62
5.10 NETWORK 64
5.11 LANGUAGE 66
5.12 BACKUP & RESTORE 67
5.12.1 Backup Server 68
5.12.2 Backup Schedule 70
5.12.2.1 Add Backup Schedule 70
5.12.2.2 Update Backup Schedule 72
5.12.2.3 Delete Backup Schedule 73
5.12.3 Manual Backup 74
5.12.4 Restore From Backup Server 75
5.12.5 Restore from Alternate Location 77

6 STATUS, STARTING AND STOPPING THE MDC APPLICATION 80

6.1 STATUS OF THE MDC APPLICATION 80
6.2 STARTING THE MDC APPLICATION 81
6.3 RESTARTING THE MDC APPLICATION 81
6.4 STOPPING THE MDC APPLICATION 82

7 MDC LICENSING AND KEYCODE RETRIEVAL SYSTEM (KRS) 83

7.1 REQUIRED INFORMATION FOR KRS 84
7.2 HIGH-LEVEL OVERVIEW OF PROCESS TO OBTAIN KEYCODE FROM KRS 84
7.3 LOGIN INTO KRS 85
7.4 REGISTER MDC SYSTEM 85
7.5 GENERATE AND RETRIEVE KEYCODE FOR MDC SYSTEM 85
7.6 COPY KEYCODE FILE ONTO MDC SERVER AND APPLY LICENSES 86
7.7 UPDATE LICENSING INFORMATION IN THE MDC APPLICATION 86
7.8 OTHER KRS ACTIVITIES 87
7.8.1 Register for KRS Access 87
7.8.2 Retrieve Keycode for MDC System 87
7.8.3 Generate Try-n-Buy Licenses for MDC System 87
7.8.4 Adding More Licenses to MDC System 88

8 INTEGRATE MDC AND LOCATION SERVICE 89

8.1 REQUIRED INFORMATION FOR INTEGRATING MDC SERVER AND LOCATION SERVER 90
8.2 INTEGRATING MDC SERVER AND LOCATION SERVICE 90
8.3 CONFIGURATION REQUIRED ON SYNTRACK FOR HEALTHCARE 92

9 INTEGRATING MDC SERVER AND CALL SERVER 97

9.1 CONFIGURE AND TEST CONNECTION TO CS 1000 FROM MDC SERVER 97
9.2 CONFIGURE AND TEST CONNECTION TO CS 2100 FROM MDC SERVER 102

10 MANAGING ASSETS (PHONES) 108

10.1 TERMINAL NUMBER FORMAT BASED ON CALL SERVER 109
10.1.1 Terminal Number Format for CS 1000 109
10.1.2 Terminal Number Format for CS 2100 110
10.2 INSERT NEW ASSET 110
10.3 VIEW ASSETS 117
10.4 VIEW OWNER OF ASSETS 119
10.5 UPDATE ASSET FROM VIEW SCREEN 121

10.6 Update Asset from Insert/Update Screen ... 123
10.7 Enable Location Tracking for All Assets ... 129
10.8 Disable Location Tracking for All Assets ... 130
10.9 Delete Asset ... 132
10.10 Bulk loading of Assets ... 134

11 MANAGING USERS ... 138

11.1 Insert New Users ... 139
11.2 View Users ... 145
11.3 View Assets Assigned to User ... 146
11.4 Update Users from View Screen ... 148
11.5 Update Users from Insert/Update Screen ... 150
11.6 Enable Location Tracking for All Users ... 155
11.7 Disable Location Tracking for All Users ... 156
11.8 Delete Users ... 158
11.9 Bulk loading of Users ... 160

12 MANAGING ROLES ... 163

12.1 Overview of Enabling Roles ... 164
12.2 Insert New Roles ... 165
12.3 View Roles ... 170
12.4 Updating Roles from View Screen ... 171
12.5 Updating Role from Insert Role Screen ... 173
12.6 Delete Role ... 177
12.7 Grouping Roles into Categories ... 181
12.7.1 Create a New Category ... 181
12.7.2 View a Category ... 183
12.7.3 Modify a Category ... 185
12.7.4 Delete a Category ... 187
12.8 Role Template ... 189
12.8.1 Create a New Template ... 190
12.8.2 View a Template ... 196
12.8.3 Modify a Template ... 199
12.8.4 Delete a Template ... 204

13 MANAGING MDC STATIONS ... 207

13.1 Add MDC Station ... 207
13.2 View MDC Stations ... 208
13.3 Language on MDC Station ... 210
13.4 Set Message Banner and Help Number for Stations ... 211
13.5 View Station Locations ... 212
13.6 Insert Station Location ... 215
13.7 Modify Station Location ... 218
13.8 Delete Station Location ... 221
13.9 Update MDC Station Information ... 223
13.10 Reboot MDC Station ... 225
13.11 Reboot All MDC Stations ... 226
13.12 Delete MDC Station ... 227
13.13 Relocate MDC Station ... 229
13.13.1 Relocating an MDC Station when Future Location is Known ... 229
13.13.2 Relocating an MDC Station when Future Location is Not Known ... 229

14 USING MDC STATION ... 231

14.1 Check out a phone to a user at an MDC Station ... 231
14.2 Return a phone at an MDC Station ... 234
14.3 Presentation Conventions on MDC Station Screen ... 235

14.4 CHECK OUT A PHONE TO A LOCATION-TRACKED USER 235
14.5 RETURN A PHONE ASSIGNED TO A LOCATION TRACKED USER 235
14.6 RE-ASSIGN A PHONE FROM A USER TO ANOTHER USER AT ANY MDC STATION 236
14.7 ASSIGN A PHONE FROM A USER AND ASSIGN ANOTHER PHONE TO SAME USER AT ANY MDC STATION 236

15 ADDITIONAL HELP 238

16 REFERENCES 239

17 ACRONYMS AND DEFINITIONS 240

18 APPENDIX: LIST OF MDC LOGS 243

19 APPENDIX: UPGRADE MDC SOFTWARE 246

19.1 INFORMATION NEEDED TO UPGRADE MDC 246
19.2 PERFORMING AN UPGRADE OF MDC 247
19.3 VERIFYING UPGRADE OF MDC SOFTWARE 254
19.4 COMPLETING THE UPGRADE OF MDC 255

20 APPENDIX: UNINSTALL MDC SOFTWARE 256

20.1 INFORMATION NEEDED TO UNINSTALL MDC SOFTWARE 256
20.2 PERFORMING AN UNINSTALL OF MDC SOFTWARE 256
20.3 VERIFYING UNINSTALL OF MDC SOFTWARE 258

21 APPENDIX: MDC RPM DEPENDENCIES 259

END OF DOCUMENT 260

List of Figures

Figure 1: Mobile Device Checkout Solution High Level View 19
Figure 2: Mobile Device Checkout Network Topology 21
Figure 3: Communication Server 1000 22
Figure 4: WLAN 2300 Series 25
Figure 5: WLAN Telephony Manager 2245 25
Figure 6: WLAN Handset 6120/40 25
Figure 7: MDC Station – MK1200/MK1250 Scanner kiosk 26
Figure 8: MDC Station – KDT900 Scanner Kiosk 26
Figure 9: Sample design for the storage of handsets and mounting of battery chargers at the MDC Station 27
Figure 10: Barcode Located on the Employee Badge 28
Figure 11: Barcode (1.5”) Placement on the WLAN Handset 6140 29
Figure 12: Barcode (2”) Placement on the WLAN Handset 6140 29
Figure 13: Example of Protective Silicon Cover (zCover) with Universal Belt Clip on WLAN Handset 6140 30
Figure 14: Barcode Placed in Battery Compartment when Protective Cover used on WLAN Handset 6140 30
Figure 15: LS9208 Barcode Scanner 31
Figure 16: Zebra GK420t Barcode Label Printer 31
Figure 17: System screen of MDC Admin GUI 35
Figure 18: Unsaved Changes Warning of MDC Admin GUI 36
Figure 19: Page Control when on first page of View Assets 38
Figure 20: Paging Controls on middle pages of View Assets 39
Figure 21: Paging Controls on Last page of View Assets 39
Figure 22: Sort Tip on Tags Column in View Assets 40
Figure 23: Not Sortable Tip on Delete Column in View Assets 40
Figure 24: View Assets Sorted ascending by Tags column 41
Figure 25: View Assets Sorted descending by Tags column 41
Figure 26: No match for Search of Asset 42
Figure 27: View Assets Search using contains criteria 43
Figure 28: View Assets Search using = criteria 43
Figure 29: MDC Admin Login 44
Figure 30: System screen of MDC Admin GUI 45
Figure 31: Configure screen of MDC Admin GUI 46
Figure 32: Admin Screen of MDC Admin GUI 46
Figure 33: Select Language for MDC Admin GUI 47
Figure 34: Configure Screen for MDC Admin GUI 48
Figure 35: Admin Screen of MDC Admin GUI 50

Figure 36: Insert New Admin User Window 51
Figure 37: Update Admin User on Admin Screen 53
Figure 38: Delete Admin Confirmation Dialog 54
Figure 39: View Logs Screen of MDC Admin GUI 55
Figure 40: View Logs Truncation Dialog 56
Figure 41: Print Dialog from Print Logs 57
Figure 42: Save HTML Document Dialog 59
Figure 43: XML Dump of Logs 60
Figure 44: Logs & Alarms Screen of MDC Admin GUI 61
Figure 45: Configure Email Recipient for Log Digest 62
Figure 46: Logs & Alarms Screen of MDC Admin GUI 63
Figure 47: Configure Alarm Screen on MDC Admin GUI 64
Figure 48: Network Screen on MDC Admin GUI 65
Figure 49: Configuring Languages displayed on MDC Station 67
Figure 50: Backup & Restore Screen on MDC Admin GUI 69
Figure 51: Backup Screen of MDC Admin GUI 69
Figure 52: Backup Server Screen of MDC Admin GUI 70
Figure 53: Backup Screen of MDC Admin GUI 71
Figure 54: Successful Add to Backup Schedule Message 72
Figure 55: Successful Updated Backup Schedule Message 73
Figure 56: Delete Backup Schedule Confirmation Dialog 74
Figure 57: Backup Screen of MDC Admin GUI 75
Figure 58: Restore Screen of MDC Admin GUI 76
Figure 59: Restore from Alternate Location Screen of MDC Admin GUI 78
Figure 60: List of backup images available for Restore from Alternate Location 79
Figure 61: Network Screen on MDC Admin GUI 91
Figure 62: Location Service on MDC Admin GUI 91
Figure 63: Location Server Connection Test in Progress 92
Figure 64: SynTrack for Healthcare Synapse Login Window 93
Figure 65: Selecting SynTrack RFID Administration from SynTrack for Healthcare GUI 93
Figure 66: Selecting SynTrack RFID Administration from SynTrack for Healthcare GUI 94
Figure 67: SynTrack RFID Administration GUI 94
Figure 68: SynTrack RFID Administration GUI 95
Figure 69: Create Tag on SynTrack RFID Administration GUI 95
Figure 70: Tags screen on SynTrack RFID Administration GUI 96
Figure 71: Network Screen on MDC Admin GUI 98
Figure 72: Default Call Server Screen (with Roles) on MDC Admin GUI 99

Figure 73: Default Call Server Screen (without Roles) on MDC Admin GUI 99
Figure 74: CS 1000 Connection Test in Progress on MDC Admin GUI 101
Figure 75: Successful Call Server Connection Test on MDC Admin GUI 101
Figure 76: Confirm Call Server Commit on MDC Admin GUI 101
Figure 77: Dialog requesting restarting MDC application to activate CS 1000 Configuration changes 102
Figure 78: Network Screen on MDC Admin GUI 103
Figure 79: CS 2100 Call Server Screen (with Roles) on MDC Admin GUI 104
Figure 80: CS 2100 Call Server Screen (without Roles) on MDC Admin GUI 104
Figure 81: CS 2100 Connection Test in Progress (with Roles) on MDC Admin GUI 106
Figure 82: Successful Call Server Connection Test on MDC Admin GUI 106
Figure 83: Confirm Call Server Commit on MDC Admin GUI 106
Figure 84: Dialog requesting restarting MDC application to activate CS 2100 Configuration changes 107
Figure 85: View Assets Screen with No Assets 112
Figure 86: Insert/Update Asset Screen (with Get Phone Information button) 113
Figure 87: Insert/Update Asset Screen (without Get Phone Information button) 113
Figure 88: No available license for Asset message 114
Figure 89: Data filled Insert/Update Asset Screen (with Get Phone Information button) 116
Figure 90: Data filled Insert/Update Asset Screen (without Get Phone Information button) 116
Figure 91: View Assets on MDC Admin GUI 118
Figure 92: View Asset with Owner Associated 120
Figure 93: Asset Owner Details with Roles 121
Figure 94: View Assets in MDC Admin GUI 122
Figure 95: Updating Assets from View Assets Screen 123
Figure 96: Warning of Unsaved Modifications to Assets 123
Figure 97: Insert/Update Asset Screen of MDC Admin GUI (with Get Phone Information button) 125
Figure 98: Insert/Update Asset Screen of MDC Admin GUI (without Get Phone Information button) 125
Figure 99: Loaded data on Insert/Update Asset (with Get Phone Information button) 126
Figure 100: Loaded data on Insert/Update Asset (without Get Phone Information button) 126
Figure 101: View Assets on MDC Admin GUI 130
Figure 102: View Assets on MDC Admin GUI 131
Figure 103: Tracking Disabled on all Assets 131
Figure 104: View Assets in MDC Admin GUI 132
Figure 105: Deleting Assets from View Assets 133
Figure 106: Warning of assets marked for Deletion 133
Figure 107: Delete Asset Confirmation Dialog 134
Figure 108: View Users screen of MDC Admin GUI 140
Figure 109: Insert/Update User Screen of MDC Admin GUI (with Get Display Name button) 141

Figure 110: Insert/Update User Screen of MDC Admin GUI (without Get Display Name button) 141
Figure 111: Get Display Name for Insert/Update User..... 143
Figure 112: Unable to retrieve data for Requested DN. 143
Figure 113: Filled Insert/Update User Screen (with Get Display Name button)..... 144
Figure 114: Filled Insert/Update User Screen (without Get Display Name button)..... 144
Figure 115: View Users on MDC Admin GUI 145
Figure 116: View Users with Phone Associated..... 147
Figure 117: Phone Icon details with Roles 148
Figure 118: View Users in MDC Admin GUI 149
Figure 119: Updating Users from View Assets Screen 150
Figure 120: Warning of Unsaved Modifications to Users 150
Figure 121: Insert/Update User Screen of MDC Admin GUI (with Get Display Name button) 151
Figure 122: Insert/Update User Screen of MDC Admin GUI (without Get Display Name button) 152
Figure 123: Load User Data for existing User (with Get Display Name button)..... 153
Figure 124: Load User Data for existing User (without Get Display Name button)..... 153
Figure 125: Unsaved Changes Warning 155
Figure 126: View Users on MDC Admin GUI 156
Figure 127: View Users on MDC Admin GUI 157
Figure 128: Tracking Disabled on all Users 157
Figure 129: View Users in MDC Admin GUI 158
Figure 130: Deleting Users from View Users 159
Figure 131: Warning of users marked for Deletion..... 159
Figure 132: Delete User Confirmation Dialog..... 159
Figure 133: View Roles Screen without Roles 166
Figure 134: Insert Roles Screen (with Get Display Name button) 167
Figure 135: Insert Roles Screen (without Get Display Name button) 167
Figure 136: Unable to retrieve data for Requested DN. 168
Figure 137: Data filled Insert Roles Screen (with Get Display Name button) 169
Figure 138: Data filled Insert Roles Screen (without Get Display Name button) 169
Figure 139: View Roles on MDC Admin GUI 170
Figure 140: View Roles in MDC Admin GUI..... 172
Figure 141: Updating Roles from View Roles Screen 173
Figure 142: Warning of Unsaved Modifications to Roles 173
Figure 143: Insert Roles Screen of MDC Admin GUI (with Get Display Name button) 175
Figure 144: Insert Roles Screen of MDC Admin GUI (without Get Display Name button) 175
Figure 145: Loaded data on Insert Roles (with Get Display Name button)..... 176
Figure 146: Loaded data on Insert Roles (without Get Display Name button)..... 176

Figure 147: View Roles in MDC Admin GUI 179
Figure 148: Deleting Roles from View Assets 179
Figure 149: Warning of roles marked for Deletion 180
Figure 150: Delete Role Confirmation Dialog 180
Figure 151: Sample Role Warning Dialog 180
Figure 152: Categories Screen of MDC Admin GUI 182
Figure 153: New Category on MDC Admin GUI 183
Figure 154: Select Available Role Categories 184
Figure 155: Categories Screen of MDC Admin GUI 185
Figure 156: Categories Screen of MDC Admin GUI 186
Figure 157: Categories Screen of MDC Admin GUI 187
Figure 158: Categories Screen of MDC Admin GUI 188
Figure 159: Delete Category Confirmation Dialog 189
Figure 160: Sample Category in Use Confirmation Dialog 189
Figure 161: Template Screen of MDC Admin GUI 191
Figure 162: Changing Use Categories Warning Dialog 192
Figure 163: Template Using Categories Screen of MDC Admin GUI 192
Figure 164: Removing Category Warning Dialog 193
Figure 165: Category based Role Template on MDC Admin GUI 194
Figure 166: Template Not Using Categories Screen of MDC Admin GUI 195
Figure 167: Non-Category based Role Template on MDC Admin GUI 196
Figure 168: Select Available Role Template on MDC Admin GUI 197
Figure 169: Category Based Template Screen of MDC Admin GUI 198
Figure 170: Non-Category Based Template Screen of MDC Admin GUI 199
Figure 171: Template Screen of MDC Admin GUI 200
Figure 172: Category based Role Template on MDC Admin GUI 202
Figure 173: Non-Category based Role Template on MDC Admin GUI 203
Figure 174: Template Screen of MDC Admin GUI 205
Figure 175: Delete Template Confirmation Dialog 206
Figure 176: Template Assigned to Station Location Warning Dialog 206
Figure 177: View Stations 208
Figure 178: Stations Screen of MDC Admin GUI 210
Figure 179: Configuring Languages displayed on MDC Station 211
Figure 180: Manage Station Screen of MDC Admin GUI 212
Figure 181: Locations Screen without Roles on MDC Admin GUI 214
Figure 182: Locations Screen with Roles on MDC Admin GUI 214
Figure 183: Locations Screen without Roles on MDC Admin GUI 216

Figure 184: Locations Screen with Roles on MDC Admin GUI 217
Figure 185: Insert New Station Location Window (without Roles) 217
Figure 186: Insert New Station Location Window (with Roles) 218
Figure 187: Modifying Station Location (without Roles) 220
Figure 188: Modifying Station Location with Roles 220
Figure 189: Locations Screen without Roles on MDC Admin GUI 222
Figure 190: Locations Screen with Roles on MDC Admin GUI 222
Figure 191: Delete Location Confirmation Dialog 223
Figure 192: Select Station Location on MDC Admin GUI 224
Figure 193: Reboot MDC Station on MDC Admin GUI 225
Figure 194: Reboot MDC Station on MDC Admin GUI 227
Figure 195: View Stations on MDC Admin GUI 228
Figure 196: Delete Station Confirmation Dialog 228
Figure 197: Main MDC Station Screen 232
Figure 198: Scan Device Barcode on MDC Station Screen 232
Figure 199: Scan Employee Badge on MDC Station Screen 233
Figure 200: Select Role Category on MDC Station Screen 233
Figure 201: Select Role on MDC Station Screen 234

List of Tables

Table 1 – MDC logs 243
Table 2 – Required Information for MDC Upgrade 246

1 What's New in This Release

This is a list of changes to the MDC Administration Guide as a result of new functionality and enhancements in Mobile Device Checkout (MDC) Release 2.0:

- Updated Solution Overview and Solution Component descriptions
- Recommend using Code 128A (instead of type 128) for phone and user barcodes
- Support for role assignment during asset checkout. Roles are an optional licensed feature of MDC. When Roles are licensed, related role administrative tasks include:
    - Licensing of Roles
    - Under the Roles sub-task of MDC Admin GUI, the administration of Role involves configuration of roles, role templates and optionally role categories.
    - Under the Station > Locations subtask, the association of role templates to station locations to determine which roles are available for checkout from MDC checkout station.
    - Determining the line assignment for roles and personal DNs on the call server screens of MDC Admin GUI
- Support for a new MDC Checkout Station hardware, AML KDT9000
- Enhancements to the Station screen of MDC Admin GUI:
    - Ability to reboot a single MDC Station or reboot all MDC Stations
    - Selection of station hardware type and Station Graphic template on a per station location basis
    - Enhancements to the Locations screen, including the support for searching and sorting
- Support for backup and restore of Station Graphic customization files
- Support for assets, users, and roles with the call server type, Communication Server 2100 (CS 2100). Call server enhancements include:
    - The ability to configure network connectivity for MDC to the Communication Server 2100
    - Ability to insert assets and users associated with Communication Server 2100
    - Indicating the use of either multiple calls (MCR/MCA) or single call (SCR/SCA) for all users (and roles if applicable) when configuring a call server
    - Removal of Distant Steering Code from Call Server configuration
    - Support for CS 1000 Release 6.0
- Logging sub-task has been renamed to Logs & Alarms in the navigation menu. New functions under Logs & Alarms sub-task are:
    - Configure Alarms to enable monitoring and notification of overdue and inactive assets
- Enhancements to the Admin screens of MDC Admin GUI, including the support for searching and sorting
- Support of MDC Admin GUI on Mozilla Firefox web browser version 3.5.7
- Support for SE Linux enforcement
- Upgrade procedure from MDC Release 1 to MDC Release 2.0
- Password rules are enforced on MDC specific passwords (such administrator and API passwords)
- The API (Application Programming Interface) is an optional feature supporting custom integration of the MDC product with external applications. The API supports notifications, queries and actions. The API feature and associated submenu is not enabled by default. Contact the Nortel Healthcare Solutions Business Team for more information on using the MDC API feature.

- Simplified MDC Admin GUI licensing information refresh procedure: logout and re-login to update of licensing information on MDC Admin GUI
- Rebooting all the MDC Stations to update their content with the restored MDC data following an MDC restore
- Use of port 443 for integration with SynTrack Location Service for enhanced security
- Operation in progress popup dialog when location tracking is disabled for all users

2 Introduction

This document describes the administration procedures and Mobile Device Checkout Administration Graphical User Interface (MDC Admin GUI) for the Mobile Device Checkout (MDC) Healthcare Solution.

2.1 Purpose and Scope

This document will help the administrator understand the administrative and maintenance procedures for the MDC application for MDC Release 2.0. It will also explain the features of the MDC Admin GUI. All procedures and features are described in generic terms, not specific to a particular customer or site.

The document is organized into the following major sections:

- Section 3 *MDC Solution Overview* and Section 4 *Components Overview* provide a description of the MDC Solution and its components.
- Section 5 *MDC Administration GUI* describes the user interface for MDC and associated administrative tasks.
- Section 6 *Status, Starting and Stopping the MDC* Application describes the procedures to get the status of the MDC application and stop or start the MDC application.
- Section 7 *MDC Licensing and Keycode Retrieval System (KRS)* describes the licensing for MDC and interactions with KRS to obtain keycode licenses.
- Section 8 *Integrate MDC and Location Service* describes the procedures and the MDC Admin GUI screens associated with enabling communication between the MDC Server and a Location Service.
- Section 9 *Integrating MDC Server and Call Server* describes the procedures and the MDC Admin GUI screens associated with enabling communication between the MDC server and the call server.
- Section 10 *Managing Assets (Phones)* describes the procedures and the MDC Admin GUI screens associated with managing assets.
- Section 11 *Managing Users* describes the procedures and the MDC Admin GUI screens associated with managing users.
- Section 12 *Managing Roles* describes the procedures and the MDC Admin GUI screens associated with managing roles.
- Section 13 *Managing MDC Stations* describes the procedures and the MDC Admin GUI screens associated with managing MDC Stations.
- Section 14 *Using MDC Station* provides a brief overview of the using the MDC Station to check out and return phones
- Section 15 *Additional Help* describes how to access documentation and Nortel Technical Support for the MDC application.

The following appendices have been included:

- Section 16 *References.*
- Section 17 *Acronyms and Definitions.*
- Section 18 *Appendix: List of MDC Logs* is a list of all the administrative logs generated by MDC.
- Section 19 *Appendix: Upgrade MDC Software* describes the procedure for upgrading the MDC software.
- Section 20 *Appendix: Uninstall MDC Software* describes the procedure for uninstall the MDC software.
- Section 21 *Appendix: MDC RPM Dependencies describes the software package dependencies of the MDC software.*

For a full list of documentation on MDC, refer to NN49010-100 Nortel Healthcare Solutions Mobile Device Checkout Documentation Roadmap.

2.2 Target Audience

This guide is intended for the Solution Engineers (e.g., network engineers, support engineers) responsible for the MDC solution deployments. It is also intended for the information technology administrator responsible for managing the MDC Solution. These engineers and administrator should have an understanding of TCP/IP networks, computer hardware and networks services.

2.3 Assumptions

It is assumed that the document NN49010-501 Nortel Healthcare Solutions MDC Deployment Guide has been completed to install the MDC Server and barcode equipment on the MDC Management Station.

The call server (either Communication Server 1000 (CS 1000) or Communication Server 2100 (CS 2100)) is assumed to be installed and configured and operational. The MDC Release 2.0 Solution only integrates with CS 1000 Releases 5.0, 5.5 and 6.0 and CICM 10.1 MR2 load (which is compatible with SE10, SE11, and SE13) for CS 2100. It is assumed the document NN49010-102 Nortel Healthcare Solutions MDC Customer Preparation Guide has been completed to configure the CS 1000 or CS 2100 for MDC.

WLAN 2300 is assumed to be installed, configured and operational for telephony including theTM2245, higher-density Access Points and associated engineering rules.

If registering tracked users with the Nortel Asset Tracking and Management solution is required, then the applicable components of IBSS SynTrack or Ekahau EPE are assumed to be installed, configured, and operational per the associated documentation for that offer. The MDC Release 2.0 Solution integrates with the Nortel Asset Tracking and Management Release 1.0, 1.1, or 2.1 only.

2.4 Exclusions

This section describes what is not covered in this Administration Guide.

The Administration Guide does not explain the sequence of activities to install and commission an MDC system. For a description of the sequence of steps needed to install and commission the MDC server and solution, refer to NN49010-102 Nortel Healthcare Solutions MDC Customer Preparation Guide and NN49010-501 Nortel Healthcare Solution MDC Deployment Guide.

Communication Server 1000 configuration is not covered in this document.

Communication Server 2100 configuration is not covered in this document.

WLAN 2300 configuration is not covered in this document

Nortel Asset Tracking and Management solution installation and configuration is not covered in this document, except where related to IBSS SynTrack or Ekahau EPE configuration for MDC.

3 MDC Solution Overview

The deployment of WLAN Handsets, such as the Nortel WLAN Handset 6100 series, allows enterprises to give their staff the freedom of mobility without the cost of cellular phone monthly expenses. As an added value, the WLAN Handset 6140 model also provides the user with a push to talk. The Nortel WLAN Handsets seamlessly integrate with the WLAN 2300 Series systems, Communication Server 1000 (CS 1000) and Communication Server 2100 (CS2100).

Currently a problem arises when pools of these handsets are made available for staff members to obtain a handset for a shift. In these environments, assignment of handsets is generally handled manually. Users manually record their name and the Directory Number of the WLAN Handset they selected on a sheet of paper. At some point, an administrator publishes the new list of the new directory number for each person on that shift. As a result, for the first hour there is no handset list. Manually recording names and directory numbers can also result in errors.

The Mobile Device Checkout solution provides a process by which a user of a WLAN Handset can automatically register his handset, allowing a unique directory number associated with the user to be dynamically assigned to the handset. In this solution barcodes are used to identify both the employee and the handset. As well the DN associated with a particular role or function can be assigned to the WLAN Handset allowing clinicians to be reached by dialing a number associated with a role that they are filling.

The ability to easily assign phones to people allows a wider deployment of WLAN phones for various environments, making mobility simpler for the user. This can be of particular importance to shift worker employees such as nurses where mobility is a key factor in performing their job. Casual users can also get a phone as needed. Also, by sharing WLAN phones amongst a larger number of users, there exists the opportunity for a lower cost of deployment.

The Mobile Device Checkout solution also provides an easy and simple way to associate the user with the location client integrated into the WLAN Handset 6100 series. Mobile Device Checkout software registers the user with the Nortel Asset Tracking and Management solution. The Nortel Asset Tracking and Management components are the IBSS SynTrack or Ekahau EPE applications. When a user identified as “To be Tracked” checks out a phone, that user is registered with IBSS SynTrack or Ekahau EPE applications and will now appear on the maps in those applications with the associated user identity.

Figure 1 shows a high-level view of the MDC Solution, including the main components of the solution.

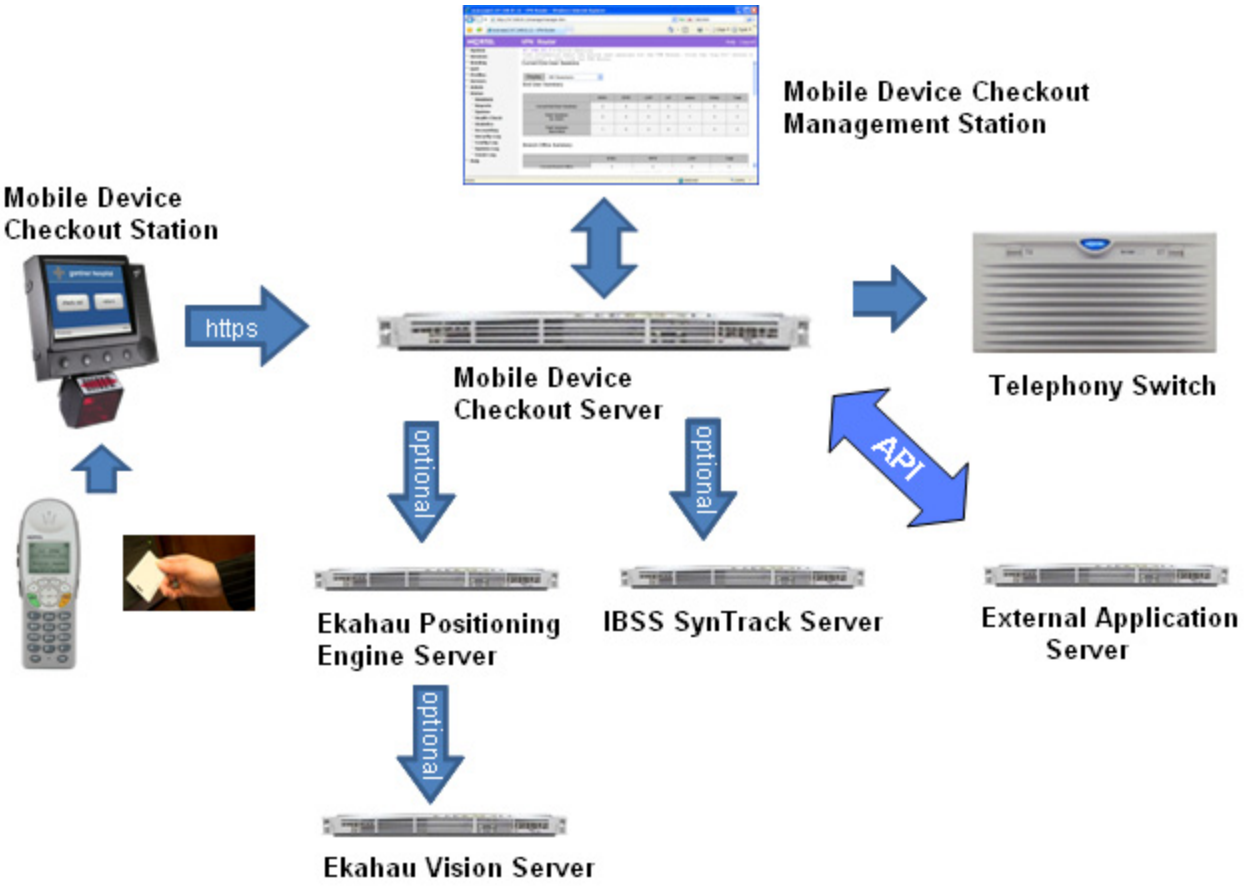


Figure 1: Mobile Device Checkout Solution High Level View

The MDC solution consists of multiple components which are all communicating together to enable the assignment of directory numbers from a corporate directory defined on the telephony switch (e.g. CS 1000 or CS 2100) to a WLAN Handset selected from a pool of WLAN Handsets such as the WLAN Handset 6140. At the same time the location client integrated in the WLAN Handset 6100 series is also associated with the user. The solution uses barcode identification as a preferred method which will be affixed on both the handset and the employee badge.

When a user is associated with the SynTrack or Vision system, their information is available to determine location. This means that they will show up on a location map on the SynTrack or Vision system. Conversely, when they are disassociated their icon will disappear from the location mapping system or, in the case of Vision the icon does not disappear but is de-associated from the user.

The MDC Station is where the user comes to check out and return phones. Phones will all be stored at this location. The station itself consists of a scanner-kiosk with a touch screen interface and an integrated barcode reader. The station is the primary interface with the user, and provides a simple-to-navigate menu system that will guide the user through the checkout and return process. The menu system provided on the station is hosted from the MDC software. The MDC Station can be connected to the corporate network via the WLAN (802.11b/g) or LAN (TCP/IP) network. The MDC Server which hosts the MDC software is connected via TCP/IP to both the corporate network and the telephony switch (e.g. CS 1000 or CS 2100). It is located in the same physical area as the CS 1000 or CS 2100 and contains a secure web server for running the management console and associated database.

The MDC solution is managed using the Management Station which will use a web browser interface to perform administrative tasks. This is also where new users and devices are registered with the MDC database. The MDC

Management Station will give the administrator the ability to remotely manage and modify operational parameters saved in the database. The MDC Management Station is connected to the MDC server via a secure http connection.

The number of MDC Stations, number of WLAN Handsets, and optionally, the number of location-tracked users or use of roles is controlled by licenses. A Keycode Retrieval System (KRS) generated keycode license is required to operate MDC.

The following is a brief description of the MDC Solution main components, shown in Figure 2, which will be described in more detail later:

- **Mobile Device Checkout Station:** is used to check out or return a WLAN Handset by a user. All WLAN phones for the area are stored near the Checkout Station.
- **Mobile Device Checkout Server:** is a Commercial-Off-The-Shelf (COTS) rack mount server with a dual Network Interface Card to accommodate two separate Ethernet IP ports or a single Network Interface Card for all communications. The Mobile Device Checkout Server has all Mobile Device Checkout software and software licenses loaded on it as well as the Red Hat Linux or CentOS Operating System.
- **Mobile Device Checkout Management Station:** is any computer that has the ability to run an Internet Explorer or Mozilla Firefox web browser and has spare ports for the printer and handheld scanner.
- **Handheld Barcode Scanner: is** used at the initiation station to set up new users and devices in Mobile Device Checkout; the Symbol LS9208 General Purpose Bar Code Scanner is recommended and is referred to in this and other MDC documents.
- **Thermal Transfer barcode printer and associated consumables: is** used at the management station to print out barcodes for new users and devices to be registered in Mobile Device Checkout. Thermal transfer printing with performance resin printer ribbon and high-performance labels (sized to fit on the WLAN Handsets and employee badges) is needed to ensure maximum robustness of the barcode; the **Zebra GK420t** thermal transfer Bar Code Label Printer is recommended and is referred to in this and other MDC documents.

The following is a brief description of components related to Mobile Device Checkout, also shown in Figure 2:

- **Communication Server 1000 or Communication Server 2100:** is the telephony switch where the directory numbers of users/roles and terminal number of all user devices, including the WLAN Handsets, resides.
- **WLAN Network Infrastructure:** is the network that contains all the wireless equipment, such as Wireless Security Switches, Access Points and the WLAN Telephony Manager 2245.
- **WLAN Handset 6100 Series:** are essentially the WLAN Handset 6120 and 6140.
- **WLAN Handset battery chargers:** recommended are the quad chargers. These chargers do not require a handset to house the battery for charging, and minimize required charging space.
- **Ekahau Positioning Engine (EPE):** is a real-time- based location system capable of tracking Wi-Fi tags (Wi-Fi enabled devices such WLAN Handset 6100 series with location tag integrated in the handset).
- **IBSS SynTrack for Healthcare:** is the user interface used in combination with the Ekahau Positioning Engine to display the location of any managed asset, including a handset user's location on a map, as well as manage assets.
- **Ekahau Vision: is** the user interface used in combination with the Ekahau Positioning Engine, which is used to display any tag on a map, including the WLAN handsets (Note: this is an

alternate to IBSS SynTrack for Healthcare, used in other verticals; SynTrack and Ekahau Vision are not expected to be deployed at the same site).

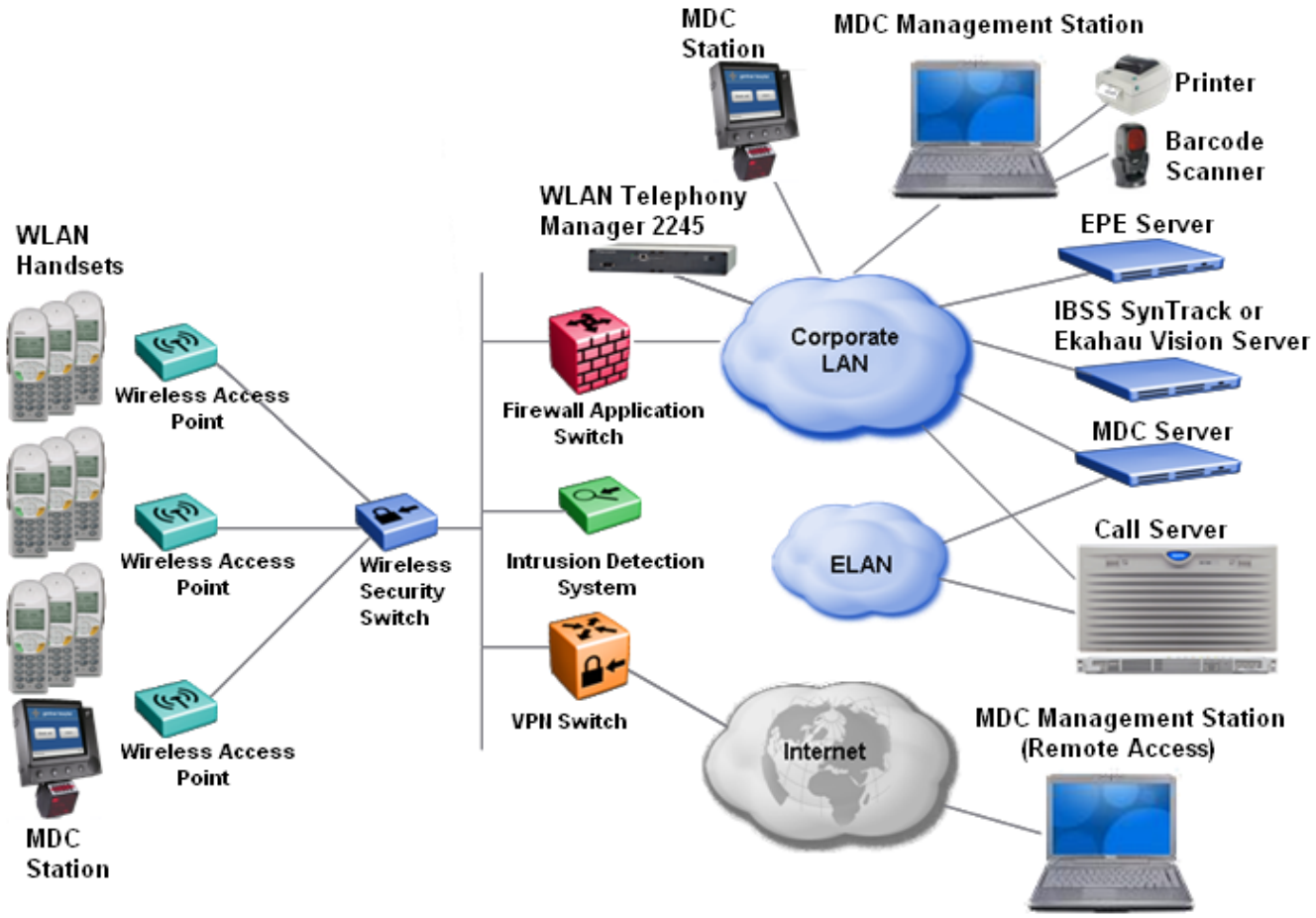


Figure 2: Mobile Device Checkout Network Topology

4 Components Overview

This section provides a detailed description of the MDC solution's components.

4.1 Telephony Network Overview

This section provides a brief overview of the Communication Server 1000 system, Communication Server 2100, WLAN Network and IP Phones.

4.1.1 Communication Server 1000

Communication Server 1000 is a server-based, full-featured IP PBX and the cornerstone of Nortel's Enterprise Unified Communications deployments. It provides the benefits of a converged network plus advanced applications and over 750 world-class telephony features. Fully distributed over IP LAN & WAN infrastructure with built-in reliability and survivability, Communication Server 1000 supports business-critical applications, including unified messaging, customer contact center, IVR, wireless VoIP and IP phones. The CS 1000 supports the WLAN Handset 6000 series, which are the main end user devices used in the MDC Solution.



Figure 3: Communication Server 1000

NOTE: MDC Release 2.0 Solution will only support the CS 1000 release 5.0, 5.5 and 6.0. Any uses of other releases will not be supported by Nortel.

The calling features of the users and handsets registered with the MDC solution are dependent upon how users are configured on the CS 1000. The directory of users is kept based on the information solely in the CS 1000.

Two options are supported by MDC: a) dual TN deployment, and b) shared TN deployment. For both options, the WLAN phones have a unique TN on the Communications Server 1000. When the WLAN phone is returned to the phone pool and properly checked in, the DN of the WLAN phone is changed to the default phone pool assigned number. This number is not published and will not appear in any directory. This number is reachable for testing purposes. Alternately the phone may be disabled when it is returned to the phone pool. Each phone in the phone pool has a unique default DN assigned to it which is listed in the MDC database.

For Dual TN deployment, a user has a unique DN that is assigned to a unique TN. An appropriate phone license is needed for each user as well as each handset. Features can be configured for each individual.

For Shared TN deployment, a group of users shares a TN. Each user has a unique DN that is assigned to that shared TN (the number of DNs associated with each TN is limited by the CS 1000). For a 1120/1140/1150 virtual

IP set with three Key Expansion Modules (KEM) defined, a total of 60 user DNs can be associated with a single TN. Users have features for the group, not the individual. This model means that an individual cannot have a unique set of services (Class-of-Service) assigned to them, such as voice mail, call forwarding, etc., but rather shares the Class-of-Service with a number of other people. This model allows customers to reduce the number of TNs required, if unique Class-of-Service is not needed.

Dual TN Deployment

In this option all phone pool users will have a permanent TN associated with them that may or may not be associated to a physical device such as a wired phone.

When a WLAN phone is checked out by a user it will display the user's DN. Any call to that DN will cause the WLAN phone to ring as well as any permanent phone assigned to that DN. If the user does not answer the call it will take one of the following options based on the configuration of the CS 1000: a) after a predefined number of rings transfer to voicemail if so enabled within the CS 1000, b) after a predefined number of rings call forward to a defined number which may be a central number, c) after a predefined number of rings call forward to a number with a prerecorded message if the system is so equipped with the ability to provide a prerecorded message, this message would be the same for all users called forwarded to this "message" DN.

Any call received by the WLAN phone will display the Caller ID name if so enabled by the caller. Any call made by the WLAN phone will display on the receiving phone the user's caller ID name.

If the user has not checked out a WLAN phone from the pool and they receive a call then it will take one of the following options based on the configuration of the CS 1000. The caller ID number and name will be displayed on the calling party's phone display if so enabled: a) after a predefined number of rings transfer to voicemail if so enabled within the CS 1000, b) after a predefined number of rings call forward to a defined number which may be a central number, c) after a predefined number of rings call forward to a number with a prerecorded message if the system is so equipped with the ability to provide a prerecorded message. This message would be the same for all users called forwarded to this "message" DN.

Shared TN Deployment

When a WLAN phone is checked out by a user it will display the user's DN. Any call to that DN will cause the WLAN phone to ring. If the user does not answer the call it will take one of the following options based on the configuration of the CS 1000: a)after a predefined number of rings transfer to a group voicemail if so enabled within the CS 1000, b)after a predefined number of rings call forward to a defined number based on the group they are part of, or c)after a predefined number of rings call forward to a number with a prerecorded message if the system is so equipped with the ability to provide a prerecorded message. This message would be the same for all users call forwarded to this "message" DN.

Any call received by the WLAN phone will display the Caller ID name if so enabled by the caller. Any call made by the WLAN phone will display on the receiving phone the user's caller ID name.

If the user has not checked out a WLAN phone from the pool and they receive a call, it will take one of the following options based on the configuration of the CS 1000: a) after a predefined number of rings, transfer to a group voicemail if so enabled within the CS 1000,; b) after a predefined number of rings, call forward to a defined number which may be a central number. This will be the same number for the group; or c) after a predefined number of rings call forward to a number with a prerecorded message if the system is equipped with the ability to provide a prerecorded message. This message would be the same for all users called forwarded to this "message" DN.

When the WLAN phone is returned to the phone pool and properly checked in, the DN is changed to the default phone pool assigned number. This number is not published and will not appear in any directory. This number is reachable for testing purposes. Alternatively the phone may be disabled when it is returned to the phone pool. Each phone in the phone pool has a unique default DN assigned to it which is listed in the MDC database.

4.1.2 Communication Server 2100

Communication Server 2100 is a server-based, full-featured IP PBX and is intended for large scale Enterprise Unified Communications deployments. It provides the benefits of a converged network plus advanced applications and over 750 world-class telephony features. Fully distributed over IP LAN & WAN infrastructure with built-in reliability and survivability, Communication Server 2100 supports business-critical applications, including unified messaging, customer contact center, IVR, wireless VoIP and IP phones. The CS 2100 supports the WLAN Handset 6100 series, which are the main end user devices used in the MDC Solution.

The CS 2100 supports both shared LEN and dual LEN models which are similar to the shared and dual TN models on the CS 1000. Also, the call forwarding and voice mail functionality in both models can be setup in a similar fashion to what is described for the CS1000 in Section 4.1.1 *Communication Server 1000*.

4.1.3 WLAN Network

The WLAN 2300 Series is a complete 802.11 solution for enterprises wishing to deploy widespread wireless coverage for today's business, IP Telephony and converged multimedia applications. The solution combines the latest industry standards with a centralized architecture and advanced features to create a secure, cost-effective and highly scalable WLAN infrastructure. The WLAN 2300 Series comprises a portfolio of WLAN Security Switches, a multi-mode Access Point and a Management Software system.

The WLAN Access Point 2332 is controlled by the WLAN 2300 Security Switches and provides multi-mode 802.11 a/b/g wireless service for mobile clients. The 2332 is designed for dense deployments and delivers high-performance mobile connectivity without sacrificing security or manageability.

The WLAN Security Switch 2350 is the smallest switch in the 2300 series and is ideally suited for extending WLAN services to small or branch office environments. The WLAN Security Switch 2350 auto-configures when first connected to the network and can control up to 3 access points. It offers the same features as the larger 2300 switches but in a smaller package. The WLAN Security Switch 2360/2361 is also ideally suited for mid-size office sites or wiring closet deployments, controlling up to 12 access points connected either directly to one of the 8 Ethernet ports or indirectly through a layer 2 or layer 3 network. A dual-power supply option provides improved resiliency for converged services.

The WLAN Security Switch 2382 provides control, management and security for up to 128 distributed access points and is designed for centralized deployments in data centers or at network aggregation points. The 2382 provides the flexibility of using closet PoE switches for connectivity and power to the access points.

The WLAN Management Software system is a comprehensive design and management tool for the WLAN 2300 Series that identifies ideal access point locations on detailed floor plans, configures all devices with a single click and provides granular monitoring and reporting for complete visibility and control over the entire system. Some of the components of the WLAN 2300 Series portfolio are shown in Figure 4: WLAN 2300 Series



Figure 4: WLAN 2300 Series

4.1.4 WLAN Telephony Manager 2245

WLAN IP Telephony Manager 2245 is an Ethernet LAN appliance that works with the AP to provide Quality of Service (QoS) on the wireless LAN. All UNIStim packets to and from the WLAN Handsets 6120 and 6140 pass through the IP Telephony Manager 2245 and are encapsulated for prioritization as they are routed to and from the supported Nortel IP Telephony solution.



Figure 5: WLAN Telephony Manager 2245

4.1.5 WLAN IP Phone Sets

WLAN Handset 6100 Series portfolio gives users the freedom to roam from floor to floor in a building, or around a campus, while still remaining accessible and connected through a powerful, discrete, lightweight device. By seamlessly integrating the IP Telephony system with WLAN infrastructure, users are provided with high-quality mobile voice and data communications throughout the workplace. The portfolio comprises of the WLAN Handset 6120 and 6140, as shown in Figure 6. The 6100 series WLAN Phone contain a location tracking client that works in conjunction with the Ekahau EPE. This allows the location of the device to be tracked through an Asset Management and Tracking solution.



Figure 6: WLAN Handset 6120/40

4.2 Mobile Device Checkout Components

4.2.1 MDC Station

The MDC Station is the primary interaction point for users. Mobile Device Checkout Release 2.0 Solution supports two kiosks: the Motorola MK1200/1250 micro-kiosk and the AML ADT900 scanner kiosk. To check out or return a phone, the user will go to the scanner-kiosk at an MDC Station.

Both scanner-kiosks run the Windows CE operating system. The MK1200/1250 features a ¼ color VGA while the ADT900 supports a full VGA color display. Both devices have touch screens and support for barcode scanning that enables simple user-to-handset association. The MDC User Interface runs as an application on this terminal. The MK1200/1250 supports 802.11b wireless while the ADT900 supports 802.11b/g/n. Both devices can be connected via an Ethernet wired connection and the ADT900 has the added ability to be powered by Power over Ethernet (802.3af).

The scanner-kiosk will initially present the user with the option to select between checking a device out and returning a device. Users will select one of these options and the follow the directions on screen to check out or return a phone. Appropriate error messages are displayed as needed, and a final completion message is provided to indicate to the user that the phone checkout or return has been successful.



Figure 7: MDC Station – MK1200/MK1250 Scanner kiosk



Figure 8: MDC Station – KDT900 Scanner Kiosk

The design of the area around the MDC station is critical. Users need to arrive at the Station, easily collect a phone and a charged battery, and then access the scanner-kiosk.

The MDC Station should accommodate the storage of handsets and charged batteries as well as being able to charge batteries for the handsets. Quad chargers are recommended, and could be mounted on the wall near the

MDC Station scanner-kiosk or in drawers near the handsets. If the MDC Station is in a public area then it should be lockable.

Another consideration is the return of damaged, nonfunctional or contaminated handsets in a manner that they can no longer be checked out. In the case of contaminated handsets in the clinical application of MDC, hospital procedures must be followed to ensure protection of hospital personnel. This will probably mean that contaminated handsets will have to be bagged in a restricted access location.

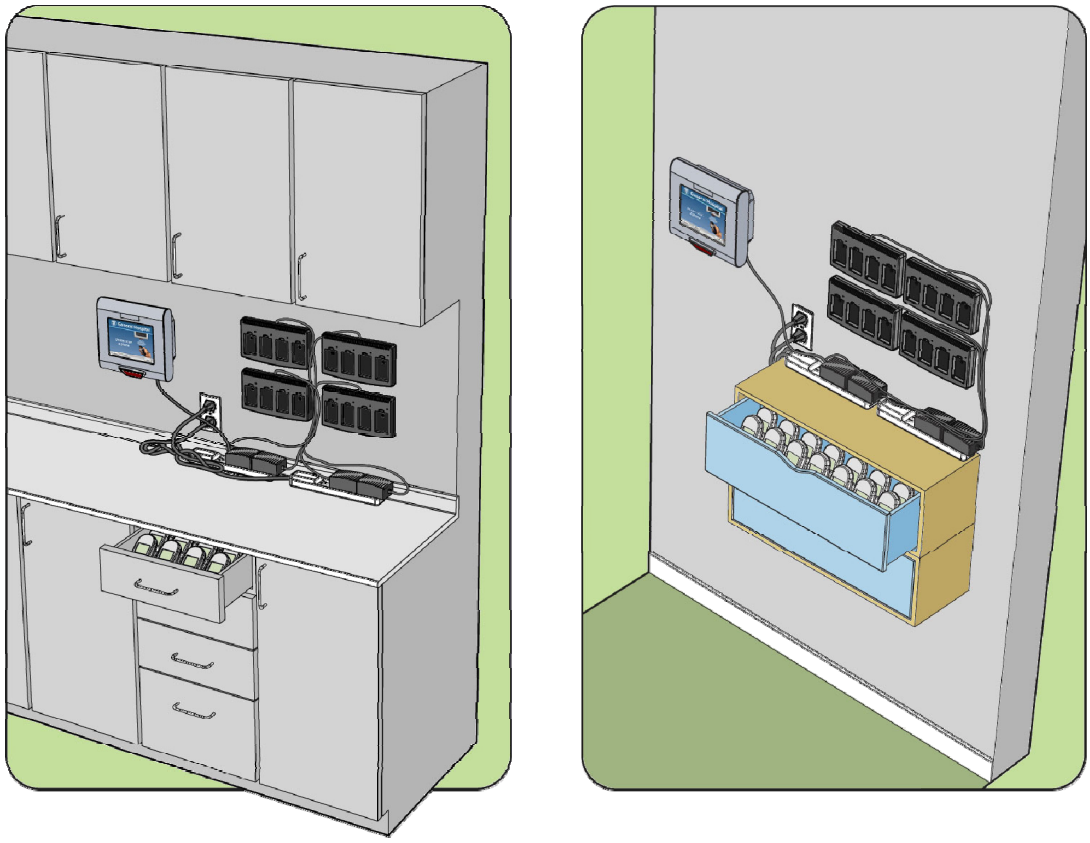


Figure 9: Sample design for the storage of handsets and mounting of battery chargers at the MDC Station

4.2.2 MDC Server

The MDC Server is a COTS rack mount server with a dual NIC card to accommodate two separate Ethernet IP ports with one connected to the corporate network and the other one connected to the call server directly as part of the E-LAN/CS-LAN. A single NIC server configuration can also be used where the Ethernet port connects to both the corporate network and call server OAMP network. The MDC Server communicates with the CS 1000 over an “rlogon” terminal session and in future releases as an SSH session. The MDC Server communicates with the CS 2100 over an unsecure Telnet session as part of the CS-LAN. The MDC Server should be located in the same secure physical area as the CS 1000 or CS 2100. The MDC Server contains a secure web server for running the management console, as well as a database for the associated databases.

4.2.3 MDC Management Station

The Mobile Device Checkout Management Station can be any PC with the ability to run an Internet Explorer or Mozilla Firefox web browser. From the Mobile Device Checkout Management Station, the administrator accesses the Mobile Device Checkout management application over an http interface. A user ID and password are required to access the MDC management menus.

The Mobile Device Checkout Management Station manages the Mobile Device Checkout Stations and the MDC database through the Mobile Device Checkout management application. The MDC Management Station manages license keys for allowing different levels of functionality.

The Mobile Device Checkout Management Station computer should have sufficient ports for a USB-based barcode scanner and a barcode printer (multiple cable options available; USB is assumed). It also runs the barcode label generator software.

NOTE: The Mobile Device Checkout Management Station computer can be used for both the initialization process and the administrative interface for management since the software and hardware requirements are the same.

The following sub-sections will cover the components which will be connected and controlled by the MDC Management Station.

4.2.3.1 Barcode Specifics

Barcode identification is the preferred method for the MDC solution. The barcode-enabled identification utilizes a 1-dimensional code 128A 10 mil barcode on both the handset and the employee ID badge. The barcode uses a thermal transfer printing method to ensure maximum robustness of the barcode. If a barcode is already part of the employee ID badge MDC can use this barcode, provided that it meets the barcode requirements.

Figure 10 shows an example of a barcode on an employee badge. Figure 11 Figure 12and Figure 12 show examples of barcodes attached to a WLAN Handset 6140. The barcode should be place so it does not interfere with the WLAN handset speakerphone. The barcode should also not be attached to the removable battery.



Figure 10: Barcode Located on the Employee Badge



Figure 11: Barcode (1.5”) Placement on the WLAN Handset 6140



Figure 12: Barcode (2”) Placement on the WLAN Handset 6140

Extra consideration is needed to place the barcode label on a WLAN Handset which has a protective silicone cover (e.g. zCover) as shown in Figure 13 . It is recommended the barcode be placed inside the battery compartment as show in Figure 14. Within the battery compartment, to avoid confusion, the existing two 1D barcodes and the 2D barcode should be partially covered by the MDC barcode label. Care should be taken so the human readable model number and serial number are not obscured. With the 2" label the bar code printing must be sized so it is not too big and lays flat on the bottom of the battery compartment. This means the label must be trimmed or run up the sides of the battery compartment. The label should be positioned up near the connectors across the width of the phone to limit shadowing from the case.

Note: Due to the location of the barcode inside the battery compartment of the WLAN Handset, the checkout and return process will be slightly different for the user. During checkouts at the MDC Station, the user will need to scan the phone barcode before putting in the battery. For returns at the MDC Station, the user will need to first remove the battery in order to scan the phone barcode.



Figure 13: Example of Protective Silicon Cover (zCover) with Universal Belt Clip on WLAN Handset 6140



Figure 14: Barcode Placed in Battery Compartment when Protective Cover used on WLAN Handset 6140

4.2.3.2 Barcode Reader

The recommended handheld scanner for the Initialization Station is the Symbol LS9208 General Purpose Bar Code Scanner. The Symbol LS9208 is a high-speed barcode scanner. The 100-line rastering omni-directional scan pattern lets you quickly capture codes no matter how they are presented. To ensure compatibility with new standards, the device supports the GS1 DataBar symbology and 14-digit Global Trade Item Number (GTIN) barcodes. Other handheld barcode scanners capable of scanning 1-dimensional 128A 10 mil barcodes can be substituted for the Symbol LS9208 handheld scanner.



Figure 15: LS9208 Barcode Scanner

4.2.3.3 Barcode Printer

The recommended thermal transfer barcode printer is the **Zebra GK420t**. This thermal transfer printer is a small, cost effective, desktop printer that meets the minimum thermal transfer requirements. It will print up to 4.09" (104mm) width. It has serial, parallel, and USB interfaces, and an optional internal Ethernet (ZebraNet PrintServer II). High-performance resin printer ribbon and high-performance labels are recommended to withstand wear and cleaning solvents. The labels should be 0.5" x 2.0" or similar to fit on WLAN handsets and employee badges. Other thermal transfer printers can be substituted for the **Zebra GK420t**.



Figure 16: Zebra GK420t Barcode Label Printer

4.2.4 Ekahau Real Time Location System

Ekahau Real Time Location System (RTLS) provides a cost effective and accurate positioning solution for locating wireless laptops, PDAs, VoIP phones, Wi-Fi tags and other 802.11 enabled devices using the wireless enterprise networks.

The Ekahau RTLS solution consists of the Ekahau Site Survey, Ekahau Positioning Engine, Wi-Fi Location Tags, and the Ekahau Software Client. This solution can be deployed on any standard 802.11a/b/g WLAN infrastructure; it does not require the installation of proprietary wireless infrastructure or an overlay network.

Ekahau Site Survey - The Ekahau Site Survey (ESS) tool is used to record calibration surveys. A calibration survey is the process of recording 802.11 RSSI values and mapping those values to (x, y) coordinates in a map. The surveys should be recorded in all the locations within maps where device-tracking enablement is sought. The surveys should cover 802.11 a/b/g; 802.11 b/g is used by RFID tags and 802.11a is used by the WLAN phones. Conducting calibration surveys is the first step when deploying Ekahau's RTLS. After a calibration survey has been recorded a map is generated, showing

signal strength by Wi-Fi nodes, network coverage, and signal to noise ratio; changes to the WLAN infrastructure may be required and new calibration surveys may need to be recorded after analyzing this data.

Ekahau Positioning Engine - The Ekahau Positioning Engine (EPE) is the software-based real-time location system capable of tracking Wi-Fi tags, VoIP phones, and Wi-Fi enabled devices (e.g. PDAs, laptops, and other Wi-Fi enable devices). The EPE will use the signal strength measurements received from the devices (e.g. Wi-Fi tags) for estimating the location of the devices. The EPE positioning technology is based on the Ekahau Site Survey signal strength calibration, which is recorded in all the locations where the location of the devices (e.g. Ekahau Wi-Fi tags) is desired to be known.

Wi-Fi Location Tags - For locating assets and people, Ekahau provides the T301-A Wi-Fi location tracking tags. The tags are small active radio devices that are placed in a pocket, clipped to a belt or attached to an asset. The T301-A tags are not rechargeable but the batteries can be replaced when needed. The Wi-Fi tags report their position (in terms of their measured RF signal strengths of audible 802.11b/g APs) periodically at pre-defined time intervals (between 10 sec and 7 days) to the EPE. There is also the possibility of configuring the tags to report their location when they are in motion, or a combination of both periodic and when motion is detected.

Ekahau Software Client - In addition to the Ekahau tags, the Ekahau Position Engine can locate and track any person carrying a Wi-Fi enabled PDA or laptop. To be able to track Wi-Fi devices, the Ekahau Wi-Fi Client must be installed and running on each PC or PDA that is to be tracked. In addition, they must be configured with the IP address of the EPE. There need to be sufficient Ekahau licenses for every location-tracking-enabled software client.

VoIP Phones - The EPE is capable of tracking Nortel's WLAN 6100 Handset. The handsets can be configured to send location update reports to the Ekahau Positioning Engine once every 1 min, 5 min, or 10 min using 802.11a. For MDC, the recommended update time interval is 1 minute. Note that to enable this functionality the wireless handsets needs to have the appropriate firmware version. In addition, they must be configured with the IP address of the EPE. There need to be sufficient Ekahau licenses for every location-tracking-enabled VoIP phone.

Setting up Ekahau RTLS is not described in this document. For further information, refer to the Nortel Healthcare Solution Asset Tracking and Management documentation suite.

4.2.5 IBSS SynTrack for Healthcare

The SynTrack for Healthcare application enables the use of Radio Frequency Identification (RFID) technology to efficiently manage hospital staff and equipment. The application uses RFID tags to track the location of assets, personnel or patients in real time. For the SynTrack for Healthcare application to function, the following functional elements are required in the network: (a) location service engine(s), (b) RFID tags and/or devices such as PDAs, WLAN handsets, and laptops, and (c) any standard WLAN infrastructure. The first two elements are provided by the Ekahau RTLS. The third required element can be any standard WLAN infrastructure.

The SynTrack for Healthcare application receives location updates and other information from the EPE. The MAC address and location updates of the tags and other devices are received by SynTrack every time the EPE calculates new location estimates. The SynTrack for Healthcare application has stored in a database an association between the device's MAC address and the asset, personnel or patient's records. The information received from the EPE coupled with these associations makes it possible to query the SynTrack application for the location of a given asset or individual through the SynTrack for Healthcare web portal. In addition, SynTrack for Healthcare enables the creation of alarms and alerts for assets, personnel or patients (a) based on the location information received (e.g. when an asset or individual leaves/enters a defined zone, or when the number of assets in a given zone [e.g. room] is below/above a given threshold), (b) when the status of any asset changes (e.g. when an asset is in maintenance), or (c) events (e.g. when a tag duress button is pressed).

Setting up IBSS SynTrack for Healthcare is not described in this document. For further information, refer to the Nortel Healthcare Solution Asset Tracking and Management documentation suite.

4.2.6 Ekahau Vision

Ekahau Vision is a multi-user Rich Internet Application (RIA) for quickly locating people and assets using a web browser-enabled workstation, laptop or tablet PC. Utilizing the Ekahau Positioning Engine, Ekahau Vision streamlines manual search processes that traditionally involve time-consuming manual work. Ekahau Vision provides a web interface for finding people and assets based on user preferences, item lists, categories, pre-configured rules, last known location, or simply just by typing in the name of a person.

Setting up Ekahau Vision is not described in this document. For further information, refer to the Nortel Healthcare Solution Asset Tracking and Management documentation suite.

5 MDC Administration GUI

This section describes the MDC Administration Graphical User Interface (MDC Admin GUI) and associated administrative tasks.

The recommended browser for using the MDC Admin GUI is Windows Internet Explorer version 6.0, 7.0, or 8.0 or Mozilla Firefox version 3.5.7. Results are not guaranteed if other web browsers are used.

Only one administrative user should be logged into the MDC Admin GUI at a time. Results are not guaranteed when multiple MDC Admin GUI sessions are used simultaneously. In rare cases, data corruption may occur.

The contents of this section on MDC Admin GUI are:

- Recommended Web Browser Settings
- MDC Admin GUI Presentation Conventions
- Login and System Page
- Changing the admin default password
- Select Language
- Help
- Configure
- Admin
- Logs and Alarms
- Network
- Language
- Backup & Restore

The first description of the MDC Admin GUI is the Logon page. All descriptions of the MDC Admin GUI following the Logon will assume the user is already logged into the MDC Admin GUI.

For a description of the sequence of steps needed to commission the MDC server and solution, refer to:

- NN49010-100 Nortel Healthcare Solutions MDC Documentation Roadmap,
- NN49010-102 Nortel Healthcare Solutions MDC Customer Preparation Guide
- NN49010-501 Nortel Healthcare Solutions MDC Deployment Guide.

In the following descriptions, items in **bold text** are the actual commands or fields.

TIP: New users of MDC Admin GUI should read Section 5.2 *MDC Admin GUI Presentation Conventions* for a description of the MDC Admin GUI screen layout.

WARNING: When using MDC Admin GUI for the first time, it is recommended the default administrator password be changed as soon as possible for security reasons. See Section 5.4 *Changing the admin default password* for the procedure.

WARNING: When using a browser which supports multiple tabs, it is recommended that the administrator always log out of the MDC Admin GUI before closing the web browser tab. Otherwise, as is the normal convention for web browsers, any tab of the web browser session will still have access to the MDC Admin GUI without having to enter in login credentials.

RECOMMENDATION After making configuration changes, it is recommended the user perform a manual backup of MDC configuration and database. The MDC backup server must be provisioned before attempting a manual backup. See Section 5.12.3 *Manual Backup* for the detailed procedure.

5.1 Recommended Web Browser Settings

The following web browser settings are recommended for MDC Admin GUI:

- In Internet Explorer, the "**Initialize and script ActiveX control not marked as safe**" setting should be set to **Enable**. This can be configured under **Tools > Internet Options > Security > Custom Level** under the **Active X Controls and plug-ins** (This path may vary depending on the version of Internet Explorer), If the default setting is left as **Prompt**, the administrator must respond affirmatively in order for MDC Admin GUI to function correctly. Refer to Internet Explorer documentation for further details if needed.
- There are no recommended Mozilla Firefox browser settings however the administrator must respond affirmatively when prompted in order for MDC Admin GUI to function correctly.

5.2 MDC Admin GUI Presentation Conventions

5.2.1 MDC Admin GUI Layout

This is a sample screen from the MDC Admin GUI. It can be used to explain the layout of the MDC Admin GUI screens.

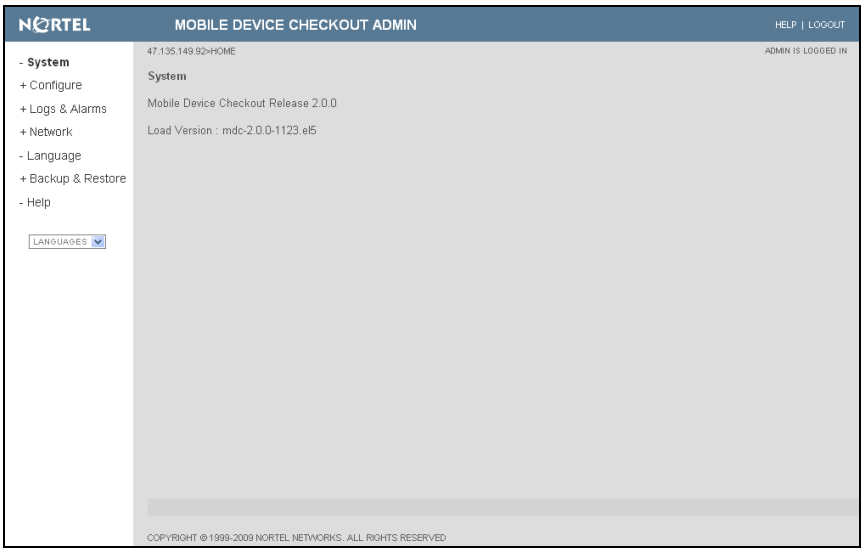


Figure 17: System screen of MDC Admin GUI

The Mobile Device Checkout Admin GUI screens have the following presentation features:

Navigation Menu:

a. The administrative tasks appear as a list in the left navigation menu. The administrative task being used is bolded to help orient the user in the navigation menu. The “+” symbol denotes

further sub-tasks available under an administrative task. When a task with sub-tasks has been selected, the sub-tasks will appear in the left navigation menu and may be selected.

Help & Logout:

b. The Help function is located on the right of the title bar.

c. The Logout function is located on the right of the title bar.

MDC Server IP Address:

d. The IP address of the MDC Server being administered appears at the top of the main task working area.

Administrator Username:

e. The username of the administrator logged in appears at the top right of the main task working area.

Main Task Working Area:

f. The administration task in use will appear in the main task working area.

g. A message banner appears at the bottom of the main task working area. This message banner may contain:

   i. a message result for user-initiated actions

   ii. when applicable, status of licenses usage for the administrative task in use

h. If the user makes changes to fields on the screen but has not saved or committed those changes, a warning will be shown when the user attempts to navigate away from the modified screen. The user can choose to “OK” to discard changes and continue to navigate away from screen, or “Cancel” to remain on the current screen in order to explicitly review, save or commit their changes.

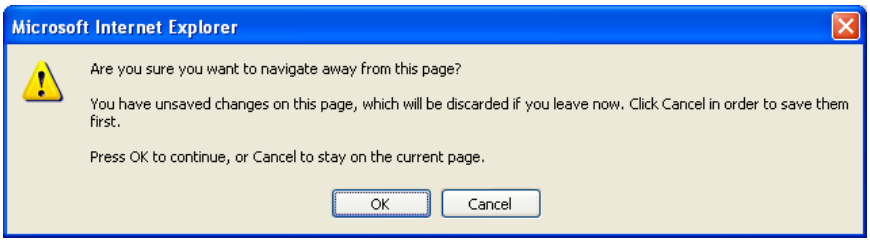


Figure 18: Unsaved Changes Warning of MDC Admin GUI

i. When changing any password field, be sure to highlight the entire field and blank it before entering the new password.

j. Most of the MDC Admin GUI screens do not automatically refresh. The screens will only automatically refresh when the user who is logged in to the session initiates an action. Alternatively, the user may manually refresh/reload the web browser page or re-select the MDC administrative task from the left navigation menu.

   The View Stations screen is the exception as the screen for this administrative task will automatically refresh itself approximately every 30 seconds.

   Note: With the Admin, Station Locations, Asset and User screens, the user-initiated actions such as save, search, sort or paging, are not actions that will refresh the screen content. These actions do not cause the screen content to be updated from the MDC database. These actions merely allow the user to view a different portion of the data already retrieved from the MDC database. On

the Asset and User screens, only actions such as delete or changing all location tracking will cause the screen content to be updated from the MDC database.

TIP: In Windows Internet Explorer or Mozilla Firefox, use function key **F11** to move into/out of full-screen mode.

5.2.2 Password Rules

The MDC Admin GUI enforces the following password rules on new or updated passwords entered on the Admin and API screens:

- Password must be at least 8 characters or longer
- Passwords must contain at least one of each of the following:
  - upper case characters
  - lower case characters
  - digits
  - special characters in the set \".?*()$!&+-=|~{}[]@#%^\"

Note: the default userid **admin** has a default password of **admin.** It is recommended that the default password for the default admin userid be changed as soon as possible after a new installation of MDC. Use the procedure Section 5.4 *Changing the admin default password* for instructions on how to change the default password.

5.2.3 Format of IP Addresses

On the MDC Admin GUI, avoid leading zeros for any IP address inputs. For example, 47.134.236.82 will be accepted, but 47.134.236.082 produces an error dialog with the message "IP Address: Must be a valid IP address".

5.2.4 MDC Admin GUI Paging, Sort, and Search

This section describes the generic viewing features:

- paging
- sort
- search

These are functions available on the View Assets, View Users, View Roles, Admin and Station Location screens of the MDC Admin GUI. Although for illustration purposes the View Assets screens are shown, the concepts described apply to the View Users, View Roles, Admin and Station Location screens as well. For further details on these specific screens, see:

- Section 10.3 *View Assets*
- Section 11.2 *View Users*
- Section 12.3 *View Roles*
- Section 5.8.1 *View Admin Users*
- Section 13.5 *View Station Locations*

5.2.4.1 View using Paging

When there are a large number of items in the list, only some of the items will be displayed on the screen at a time. This is considered a “page.” The page number is shown on the screen along with the total number of available pages at the bottom of the table to help orient the user within the table being viewed. The equivalent row information for these entries in the table is also given in parentheses.

There are a number of options to view other items not displayed on the screen:

- Paging
- Sort
- Search

When there are more items in the list than can be displayed on the screen, the page control buttons at the bottom of the table will become available for use.

- First Page: Clicking the First Page button will display the first page of items in the list. This button is disabled (i.e. grayed out) when the first page of items is already being displayed.
- Previous: Clicking the Previous button will display the previous page of items in the list. This button is disabled (i.e. grayed out) when the first page of items is being displayed, as there is no previous page of items.
- Next: Clicking the Next button will display the next page of items in the list. This button is disabled (i.e. grayed out) when the last page of items is being displayed, as there is no next page of items.
- Last Page: Clicking the Last Page button will displays the last page of items in the list. This button is disabled (i.e. grayed out) when the last page of items is already being displayed.

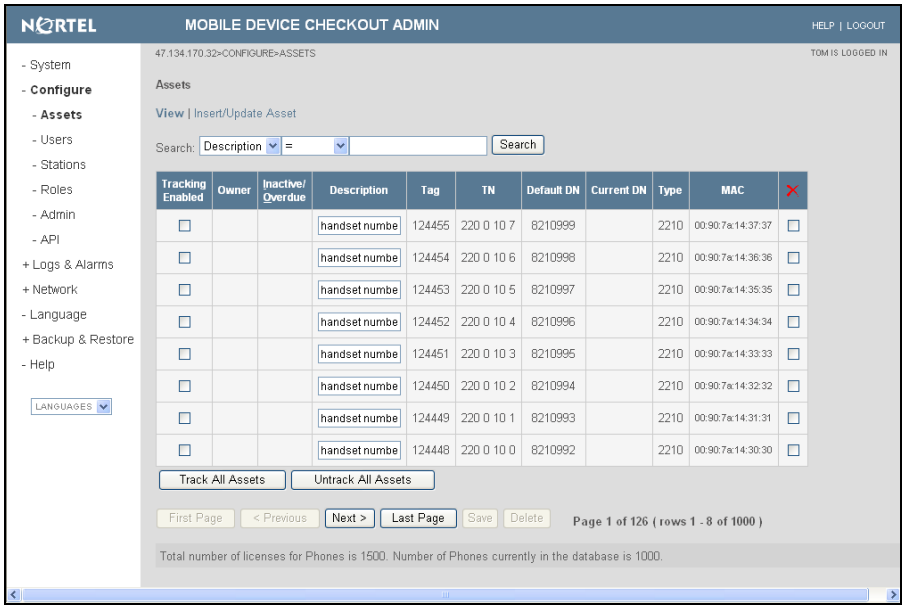


Figure 19: Page Control when on first page of View Assets

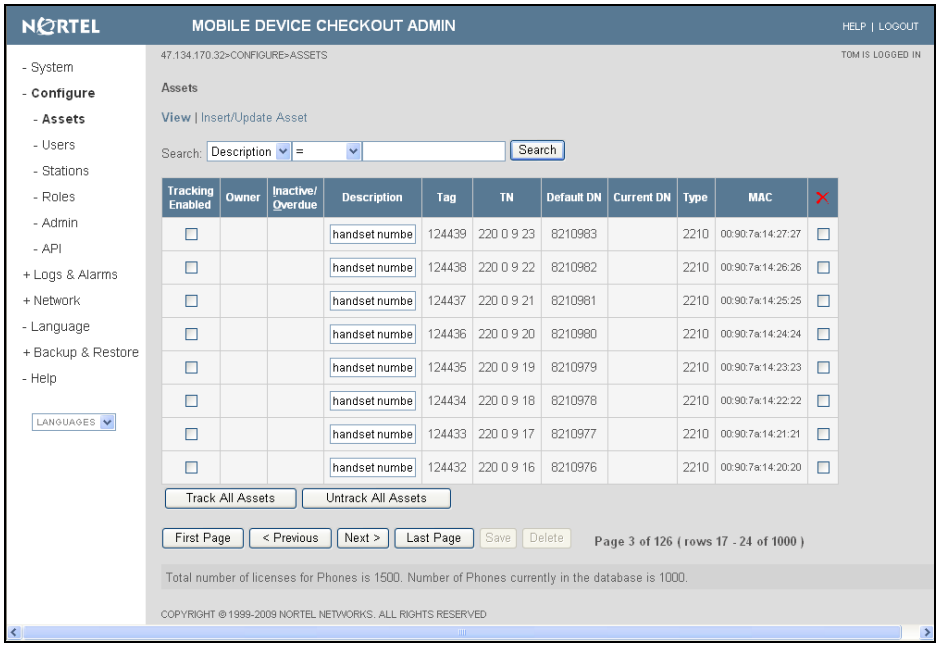


Figure 20: Paging Controls on middle pages of View Assets

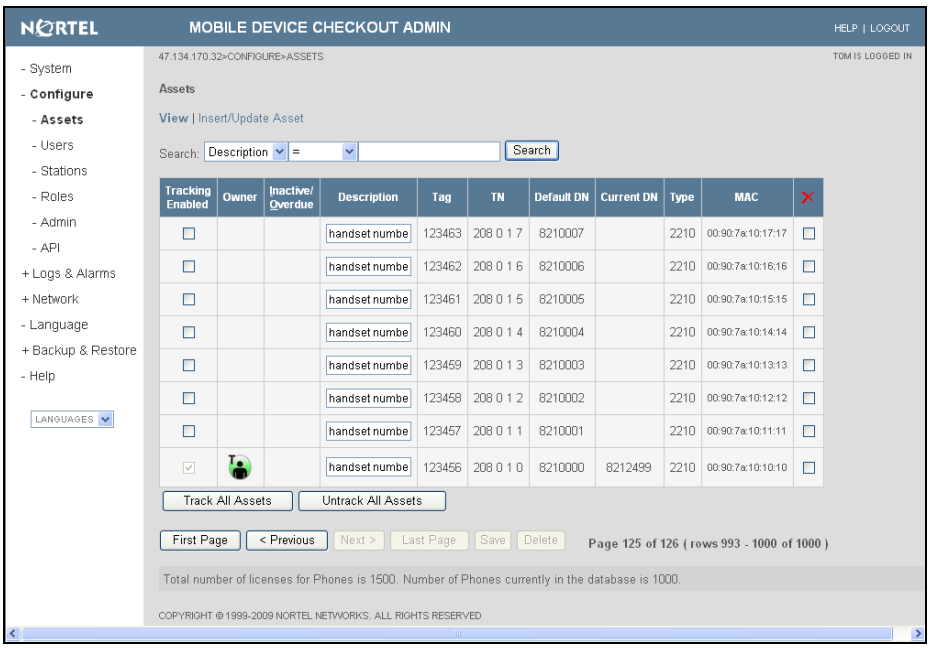


Figure 21: Paging Controls on Last page of View Assets

The following sections describe how to use the sort and search features to view items.

5.2.4.2 View using Sort

In the View screen, the table entries can be sorted by the values in a column by clicking that column's title. The column title will be colored red to highlight which values are sorted. Repeatedly clicking the column title will toggle

between sorting the table in ascending or descending order based on the values in that column. If you place the cursor over the column title, a tip will display to indicate what sort will occur if you click on the column. When you place the cursor over the column title of a column where sorting is not supported, a “Not Sortable” tip will be displayed.

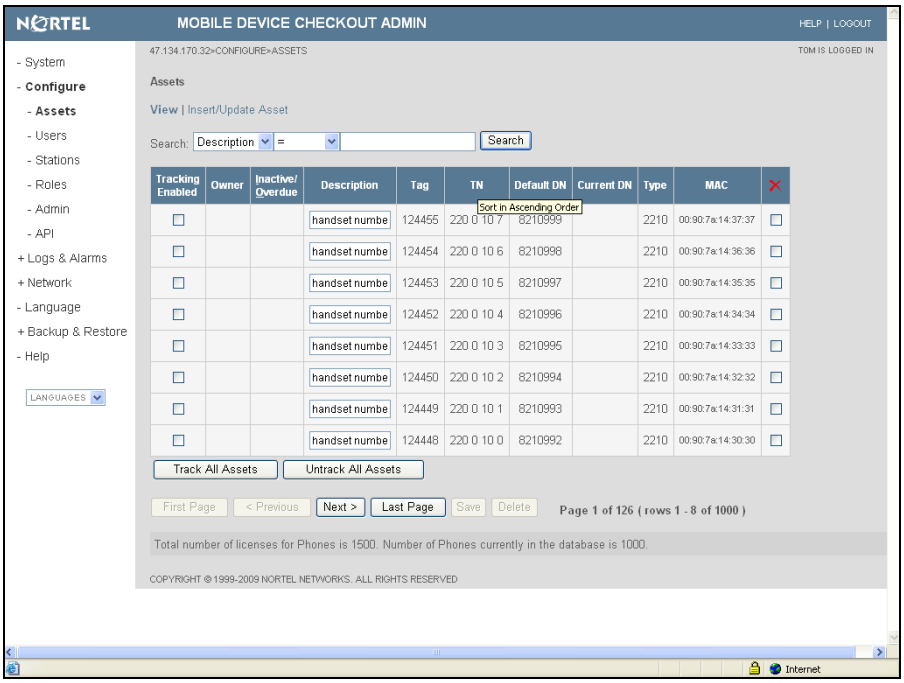


Figure 22: Sort Tip on Tags Column in View Assets

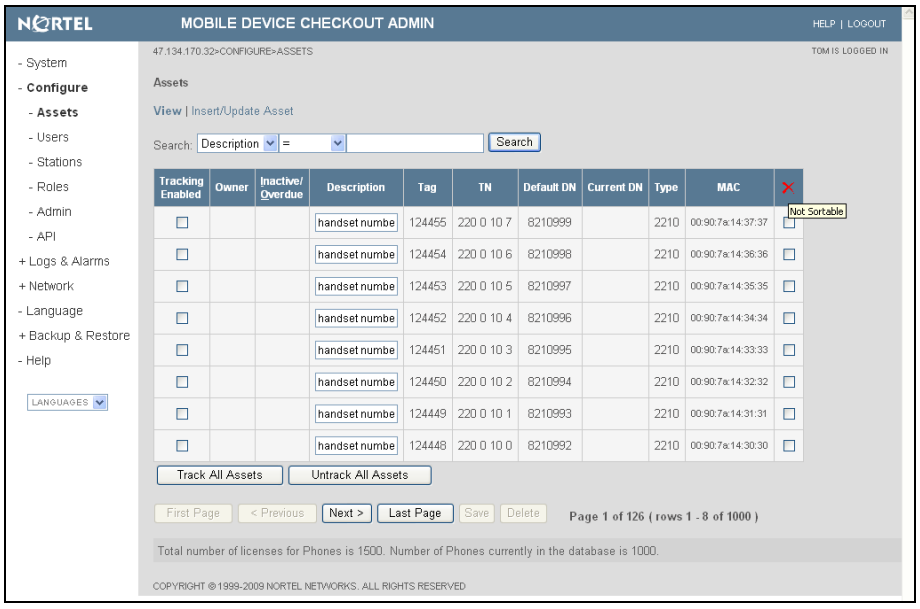


Figure 23: Not Sortable Tip on Delete Column in View Assets

Once sorted, the page control buttons can be used to move through the entries in the table.

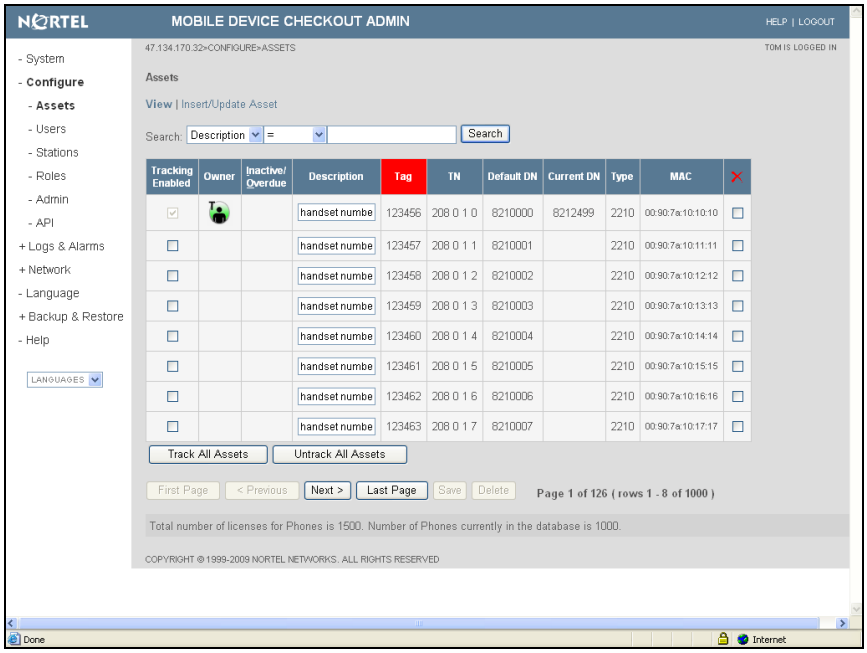


Figure 24: View Assets Sorted ascending by Tags column

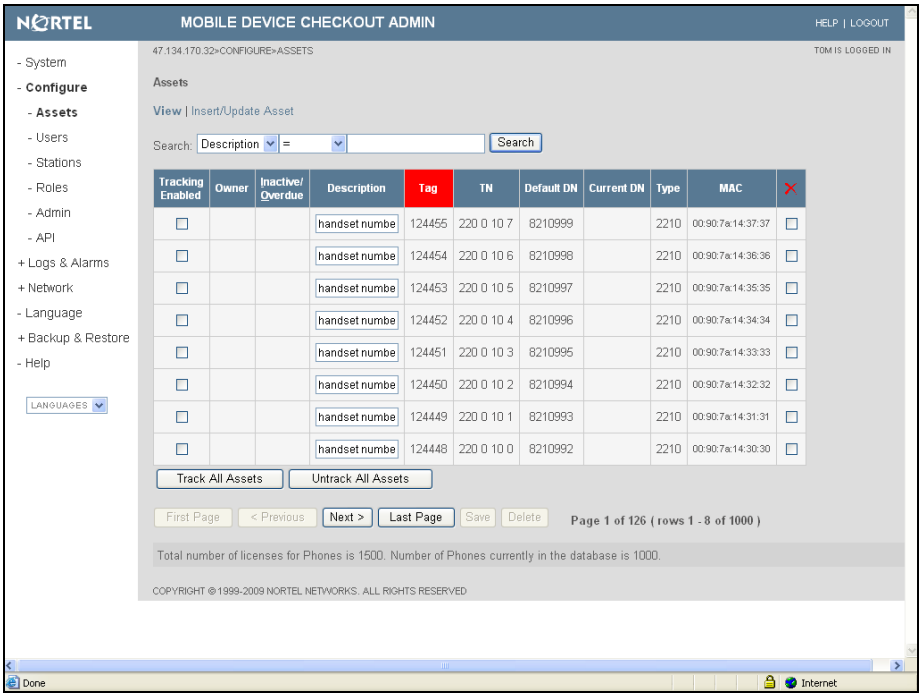


Figure 25: View Assets Sorted descending by Tags column

5.2.4.3 View using Search

Search is a feature available on the View Assets, View Users, View Roles, Admin and Station Location screens of the MDC Admin GUI. Although for illustration purposes, the View Assets screens are shown, the concepts described apply to the View Users, View Roles, Admin and Station Location screens as well.

The View screen supports a search capability. The search function is located above the table. To use the search function, you need to define the search criteria:

1. In the first search field, use the pulldown menu to select the column you want to search in.
2. In the second search field, use the pulldown menu to select the match criteria. The options for match criteria are “=” or “contains”.
3. In the third search field, type the text pattern for the match. Note: The search is case insensitive.
4. Click the **Search** button to find the first item matching the search criteria. The search is always in the forward (downward) direction from the current location in the table.
5. Click the **Search** button again to find the second item matching the search criteria.

If there is an item matching the text pattern criteria in the selected column, the View screen will be updated to display the matching item. The item matching the search criteria will be highlighted in the table. Clicking the **Search** button again will initiate a search for the next match, searching in the forward (downward) direction from the current location in the table. The View screen will be updated to display the next matching item, which will be highlighted in the table.

If there are no further matches for the search criteria in the list of remaining items, a popup dialog will appear to tell the user that the end of the list has been reached. The user will be prompted for whether they wish to continue the search from the beginning of the table (click OK) or if they wish to stop the search (click Cancel).



Figure 26: No match for Search of Asset

If there are no matches for the search criteria, the “end of the list has been reached” popup dialog will continue to appear to tell the user no match has been found.

If you use the page controls or sort function after performing a search, the matching item may no longer be shown on the screen even though there is a search criteria defined. The same is true if you define a search criterion but do not click the Search button.

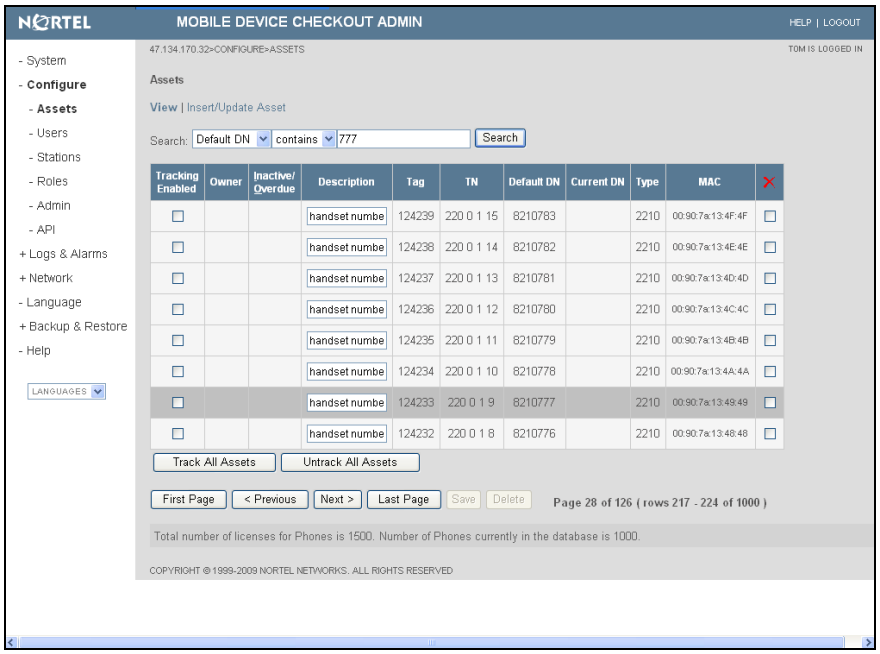


Figure 27: View Assets Search using contains criteria

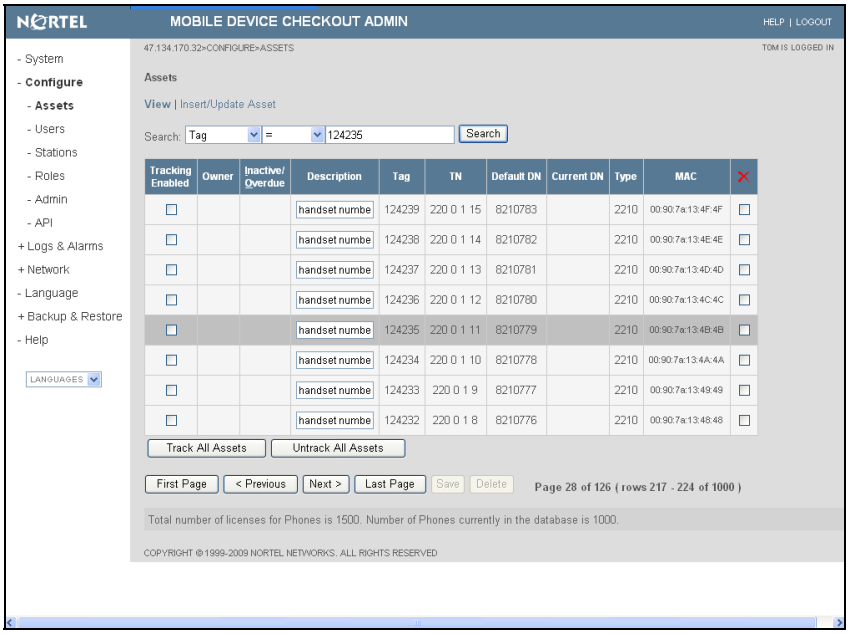


Figure 28: View Assets Search using = criteria

5.3 Login and System Page

Description:

This procedure describes how to log in to the MDC Administration GUI and the contents of the System page.

Note: The MDC Administration GUI uses Secure Socket Layer (SSL) connection to the MDC server. The MDC application is delivered with the default Apache security certificates. This may cause security alert when you

connect to the MDC Admin GUI. To eliminate these warnings, you can choose to install certificates signed by a trusted authority.

Required information:

- IP address of MDC Server
- MDC Admin GUI administration username and password
- Default MDC Admin GUI administration username is **admin** with an initial password of **admin**

Steps:

1. On the MDC Management Station, open a Windows Internet Explorer (IE) or Mozilla Firefox web browser and type into the address pane **https://<IP Address of MDC Server>/mdc/admin.**
2. Depending on the web browser you are using and its configuration:
    a. With Windows Internet Explorer (IE) web browser, depending on the IE setting, you may see a popup Security Alert related to certificates. If this occurs and you are confident with your connection to the MDC Server, click the **Yes** button.
    b. With Mozilla Firefox web browser, you may see a “This Connection is Untrusted”. If this occurs and you are confident with your connection to the MDC Server:
        i. Expand the **I understand the Risks** section
        ii. Click the **Add Exception …** button.
        iii. Click the **Confirm Security Exception** button on the Add Security Exception dialog box.
3. The MDC Admin login page appears.

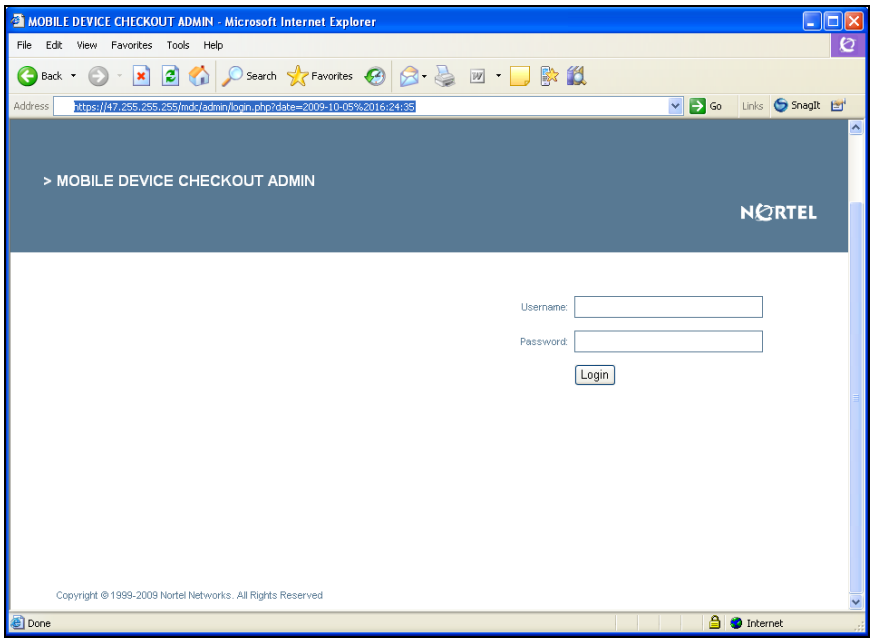


Figure 29: MDC Admin Login

4. If this is the first time you are using the system following a new installation, the default administrator username created by the system is **admin** and its default password is **admin.**

WARNING: It is recommended that the default password for the admin be changed as soon as possible after a new installation of MDC. Refer to Section 5.4 *Changing the admin default password* for instructions on how to change the default password.

Type in the following information:

a. **Username:** administration user name

b. **Password**: password for administration username

5. Click the **Login** button.
6. The System window of the Mobile Device Checkout Admin appears with the following features:
   a. The Mobile Device Checkout Application Release and Load Version will be shown on the main task working area.



Figure 30: System screen of MDC Admin GUI

5.4 Changing the admin default password and email

Description:

This procedure describes how to change the password of the admin user.

Required information:

- New password for default admin user
- Email address for admin user
- [Optional] First name and last name of the default admin user

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.

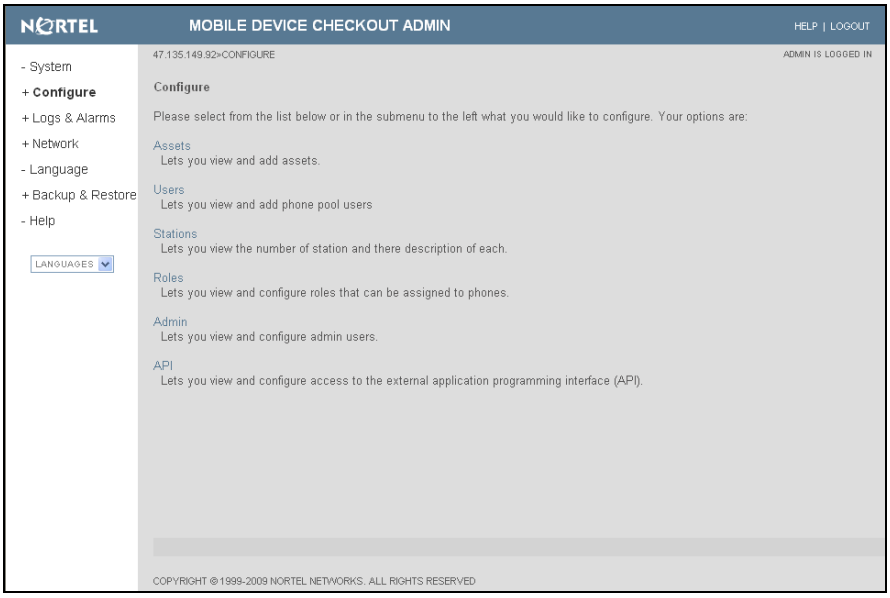


Figure 31: Configure screen of MDC Admin GUI

3. Click **Admin** from either the main task area or the Configure submenu on the left navigation menu.
4. The Admin screen appears. It displays a list of all the administrative users in a table.

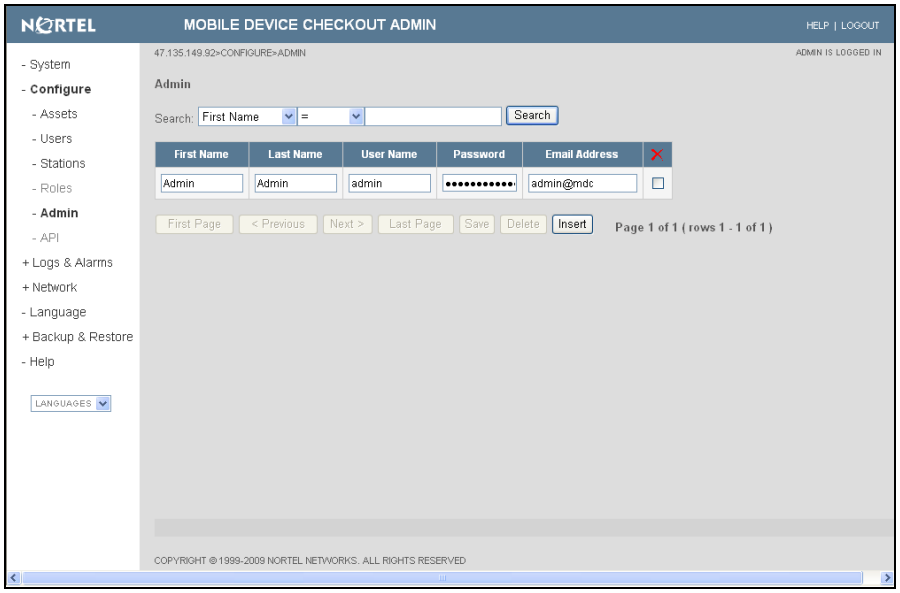


Figure 32: Admin Screen of MDC Admin GUI

5. Locate the default admin user in the table. The default admin entry has “admin” as User Name. Update the admin entry in the table:

a. Change the password by placing the cursor on the Password field. Highlight the entire field and blank it before entering the new password. Type in the new **Password**. The new password must adhere to the password rules described in Section 5.2.2 *Password Rules*.

b. Update the **Email Address** with the email address of the administrator.

c. [Optional] Update the **First Name** and **Last Name** with the name of the admin administrator.

6. Click the **Save** button at the bottom of the table.
7. A message indicating the success of the action will be displayed...

5.5 Select Language

Description:

This procedure describes how to select the language used for the MDC Admin GUI.

Required information:

- Language for MDC Admin GUI

Steps:

1. On the Mobile Device Checkout Admin GUI, you will see a “Languages” pulldown menu at the bottom of the navigation menu on the left of the screen. Select the desired language to be used for the MDC Admin GUI from the pulldown menu selections.



Figure 33: Select Language for MDC Admin GUI

2. The browser will be reset to the System screen of the Mobile Device Checkout Admin GUI using the selected language.

5.6 Help

Description:

This procedure describes how to access the help for MDC Admin GUI.

Required information:

None

Steps:

1. From the MDC Admin GUI, click the **Help** task on the left navigation menu.
2. The Help screen of the MDC Admin appears.
3. Click on **Emergency Contact Number**.
4. A separate browser window will appear showing the Nortel Technical Support page. On the right side of the screen will be a list titled **CALL US**.
5. Call the support number for your region.

5.7 Configure

The Configure screen is a list of the items which can be configured and managed through of the MDC Admin GUI.

The Configure screen is accessed with these steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.

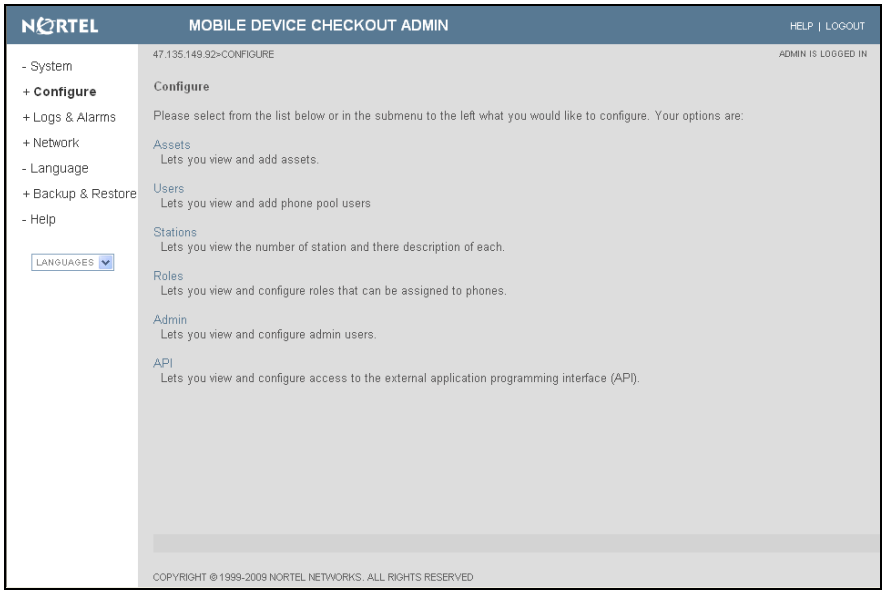


Figure 34: Configure Screen for MDC Admin GUI

For more information on the Configure submenus, refer to:

- Section 10 *Managing Assets (Phones)* for a description of procedures and the MDC Admin GUI screen associated with managing assets.
- Section 11 *Managing Users* for a description of procedures and the MDC Admin GUI screen associated with managing users.
- Section 13 *Managing MDC Stations* for a description of procedures and the MDC Admin GUI screen associated with managing MDC Stations.

- Section 12 *Managing Roles* for a description of procedures and the MDC Admin GUI screen associated with managing roles.

  WARNING: The support of roles is controlled by license. Ensure that you have sufficient licenses for roles. If the licensing information has changed within the last 5 hours, you may need to manually refresh the licensing information using the procedure described in Section 7.7 *Update Licensing Information in the MDC.* Without sufficient licenses for roles, the administrative screens relating to roles will not be accessible.

- Section 5.8 *Admin* for a description of procedures and the MDC Admin GUI screen associated with managing administrative users.

The API (Application Programming Interface) is an optional feature supporting custom integration of the MDC product with external applications. The API supports notifications, queries and actions. The API feature and associated submenu is not enabled by default. Contact the Nortel Healthcare Solutions Business Team for more information on using the MDC API feature

5.8 Admin

This section describes procedures and MDC Admin GUI screens associated with managing the administration users for MDC Admin GUI.

The following procedures are described:

- View Admin Users
- Insert Admin User
- Update Admin User
- Delete Admin User

5.8.1 View Admin Users

Description:

This procedure describes how to view the list of administrative users of MDC Admin GUI.

Required information:

None

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Admin** from either the main task area or Configure submenu on the left navigation menu.
4. The Admin screen appears. It displays a list of all the administrative users in a table.

   The columns in the Admin table are:

   - First Name: Text field with the first name of the administrator.
   - Last Name: Text field with the last name of the administrator.
   - User Name: Text field with the login user name for the administrator.
   - Password: Text field with the login password for administrator. Note: To edit, it is recommended to highlight the entire field and blank it before entering the new password.

- Email Address: Text field with the email address of the administrator.
- Delete: This field is checked to delete the administrator user from MDC.

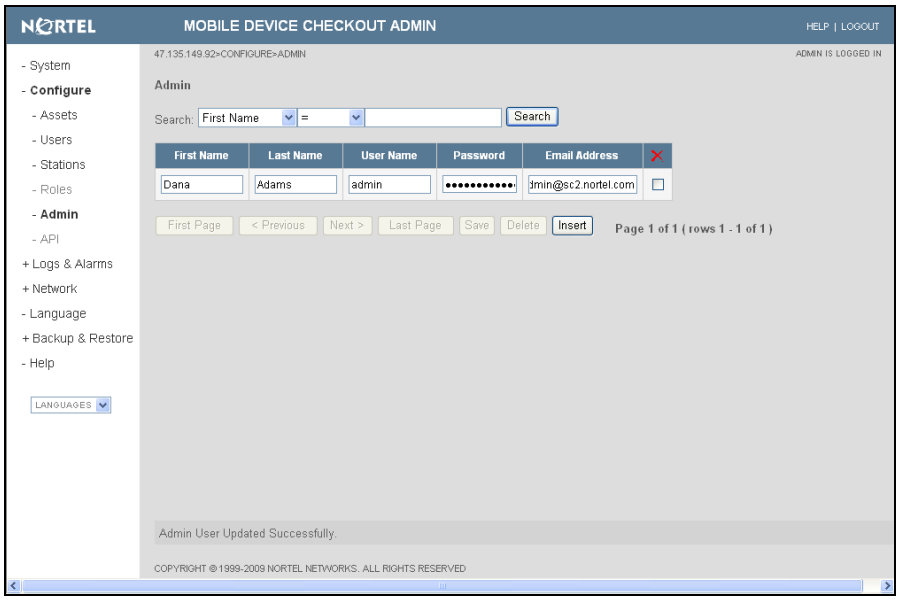


Figure 35: Admin Screen of MDC Admin GUI

When there are a large number of administrative users in the list, only some of the administrative users will be displayed on the screen at a time. This is considered a “page.” The page number is shown on the screen along with the total number of available pages at the bottom of the table to help orient the user within the view asset table. The equivalent row information for these entries in the administrative users table is also given in parentheses.

There are a number of options to view other administrative users not displayed on the screen:

- Paging
- Sort
- Search

See Section 5.2.4 *MDC Admin GUI Paging, Sort, and Search* for a description of paging, sorting and searching and an explanation of how to use these features.

5.8.2 Insert Admin User

Description:

This procedure describes how to add a new administrative user for the MDC Admin GUI.

Required information:

- First Name and Last Name for administrative user
- User Name and Password for administrative user. The password must adhere to the password rules described in Section 5.2.2 *Password Rules*.
- Email address of administrator user

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Admin** from either the main task area or Configure submenu on the left navigation menu.
4. The Admin screen appears. It displays a list of all the administrative users in a table.
5. Click the **Insert** button at the bottom on the table to add a new administrator user. A popup window will appear to enter the new administrator information:
    - **First Name**: Text field with the first name of the administrator.
    - **Last Name**: Text field with the last name of the administrator.
    - **User Name**: Text field with the login user name for the administrator.
    - **Password**: Text field with the login password for administrator. The password must adhere to the password rules described in Section 5.2.2 *Password Rules*.
    - **Email Address**: Text field with the email address of the administrator.

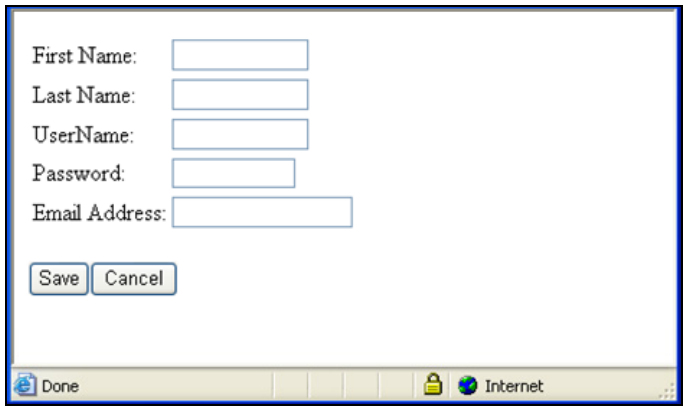


Figure 36: Insert New Admin User Window

6. Click the **Save** button to create a new administrative user.
7. A message indicating the success of the action will be displayed. If successful, the Admin table will be updated with the newly added administrative user.

5.8.3 Update Admin User

Description:

This procedure describes how to update information for a previously provisioned administrative user of the MDC Admin GUI.

Required information:

- User Name of administrative user which will be updated
- One or more updated information items:
    - User Name of administrative user
    - Password of administrative user. The new password must adhere to the password rules described in Section 5.2.2 *Password Rules*.

- First Name of administrative user
- Last Name of administrative user
- Email address of administrative user

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Admin** from either the main task area or the Configure submenu on the left navigation menu.
4. The Admin screen appears. It displays a list of all the administrative users in a table.

   Note: The **Save** button, below the Admin table, does not become enabled until there are changes made to entries in the Admin table.
5. Locate the Admin table entry that needs to be updated. See the procedures on View Admin for options to sort and search the Admin table. The following fields can be updated from the Admin screen for this administrative user.
   - **First Name**: Text field with the first name of the administrator.
   - **Last Name**: Text field with the last name of the administrator.
   - **User Name**: Text field with the login user name for the administrator.
   - **Password**: Text field with the login password for the administrator. Note: To edit, it is recommended to highlight the entire field and blank it before entering the new password. The new password must adhere to the password rules described in Section 5.2.2 *Password Rules*.
   - **Email Address**: Text field with the email address of the administrator.

   Once changes have been made to fields in the Admin table, the **Save** button, below the table, becomes enabled to indicate that there are Admin entries which have been modified. You can modify multiple entries in the Admin table. If you use the page control buttons, the entries you have modified may not be displayed on the screen.

   If you attempt to navigate away from the View Assets screen while there are unsaved changes, a warning dialog will pop up.

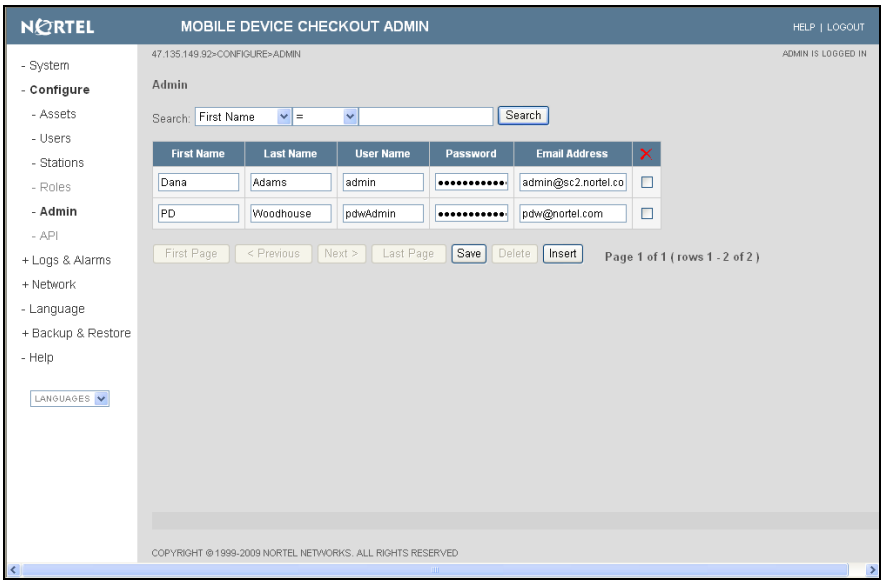


Figure 37: Update Admin User on Admin Screen

6. Click the **Save** button at the bottom of the table to save all the updates to the Admin table.
7. A message indicating the success of the action will be displayed. If successful, the Admin table will be updated with the modified administrative user changes entered.

5.8.4 Delete Admin User

Description:

This procedure describes how to delete an administrative user of the MDC Admin GUI.

WARNING: It is recommended to save any changes made to administrative users in the View screen prior to deleting administrative users. The Save button is enabled when there are unsaved changes. A warning will be given if there are unsaved updates to other entry rows in the Admin table that might be lost.

Required information:

- User Name of administrative user which will be deleted.

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Admin** from either the main task area or the Configure submenu on the left navigation menu.
4. The Admin screen appears. The main Admin screen displays a list of all the admin users in a table format.

   Note: The **Delete** button, below the Admin table, does not become enabled until there are entries marked for deletion from the administrator table.
5. Locate the table entry of the admin user(s) you want to remove. .See the procedures on View Admin for options to sort and search the Admin table. Check the box in the **Delete** column (rightmost column in the table) to delete a particular administrative user. Once any administrative user has been marked for deletion from the Admin table, the **Delete** button, below the table, becomes enabled to indicate that there

are pending deletions. You may mark multiple assets for deletion. If you use the page control buttons, the entries you have marked for deletion may no longer be displayed on the screen.

If you attempt to navigate away from the Admin screen while there are administrative users marked for deletion, a warning dialog will pop up.

6. Click the **Delete** button, below the Admin table, to delete the marked administrative user(s).
7. A delete confirmation popup dialog will appear. Click **OK** to confirm deleting the admin user.

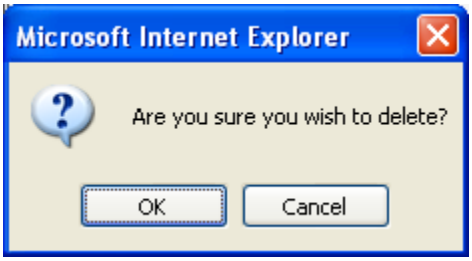


Figure 38: Delete Admin Confirmation Dialog

8. A message indicating the success of the action will be displayed. If successful, the Admin screen will be updated and the deleted administrative users will be removed from the list of administrative users.
9. Any user who is currently logged into the MDC when their administrative user account is deleted will be forced to the initial Mobile Device Checkout Admin Login screen on their next action. Note: having multiple simultaneous users on the MDC Admin GUI is not recommended. Only one administrative user should be logged into the MDC Admin GUI at a time. Results are not guaranteed when multiple MDC Admin GUI sessions are used simultaneously. In rare cases, data corruption may occur.

5.9 Logs and Alarms

This section describes the procedures and the MDC Admin GUI screens associated with managing the administrative MDC logs and configuring alarms.

The list of logs generated by MDC is listed in Section 18 *Appendix: List of MDC Logs*.

The following procedures are described:

- *View Logs*
  - *Print Logs*
  - *Save Log to File*
  - *XML Dump of Log*
- *Configure Email Recipient for Logs*
- *Configure Alarms*

5.9.1 View Logs

Description:

This procedure explains how to view the MDC logs.

Note:

- By default, a maximum of 30 days of logs are available for viewing.

- The View Logs screen is not dynamically updated. If you are viewing logs which include the current day, you need to manually refresh the logs displayed to view any newly generated logs.
- A maximum of 2000 logs will be displayed at a time. If the number of logs that meet the log search filter exceeds this amount, the most recent 2000 logs that meet the filter criteria are shown and a dialog will pop up recommending the user narrow their log search filter.

Required information:

- None

Steps:

1. From the MDC Admin GUI, click the **Logs & Alarms** task on the left navigation menu.
2. The Logs & Alarms screen of the Mobile Device Checkout Admin appears.
3. Click **View Logs** from either the main task area or the Logs & Alarms submenu on the left navigation menu.
4. The View Logs screen appears. By default, the logs for the current day and all log severities will be displayed. Selected log severities are color coded for easier viewing:
    a. EMERG and CRIT logs are red.
    b. ERR logs are orange.
    c. WARNING logs are gold.
    d. All other logs (INFO, NOTICE, and ALERT) are white.

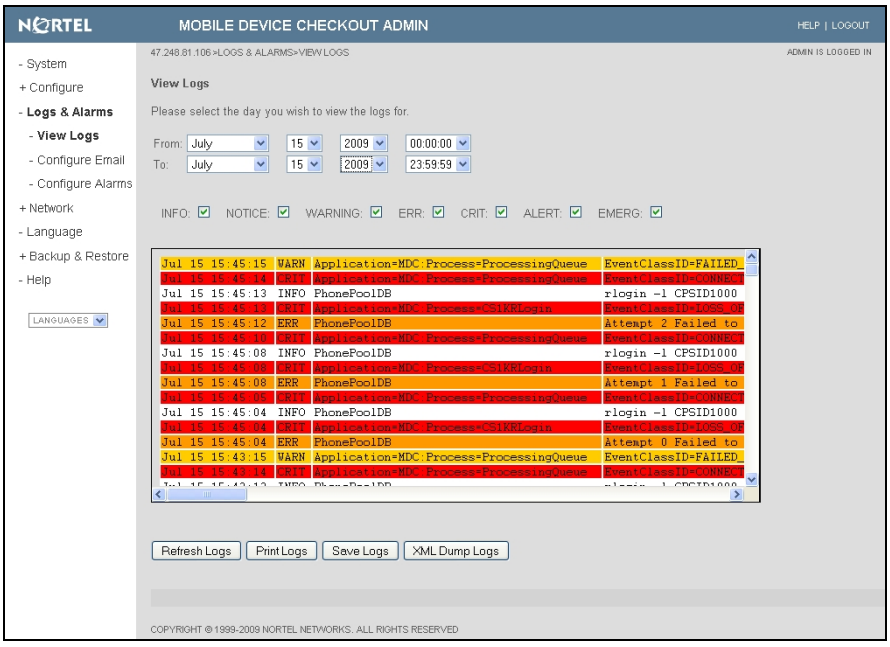


Figure 39: View Logs Screen of MDC Admin GUI

5. The user may filter the logs displayed by the following criteria:
    a. **Date Range:**

i. **From:** Select the starting Month, Day, Year and Time from the pulldown menu. By default, the day will be today's date. The Time is specified HH:MM:SS using 24 hour clock. The default start time is 00:00:00.

ii. **To:** Select the starting Month, Day Year, and Time from the pulldown menu. By default, the day will be today's date. The Time is specified HH:MM:SS using 24 hour clock. The default end time is 23:59:59.

b. **Log Severity:** Select the log severities you wish to view by checking the corresponding log severity checkboxes. More than one log severity can be selected. The log severities available are: INFO, NOTICE, WARNING, ERROR, CRIT, ALERT and EMERG. By default, all log severities will be selected.

Note: the filter criteria are not preserved when you leave the View Logs screen.

Note: A maximum of 2000 logs will be displayed at a time. If the number of logs that meet the log search filter exceeds this amount, the most recent 2000 logs that meet the filter criteria are shown and a dialog will pop up recommending the user narrow their log search filter.

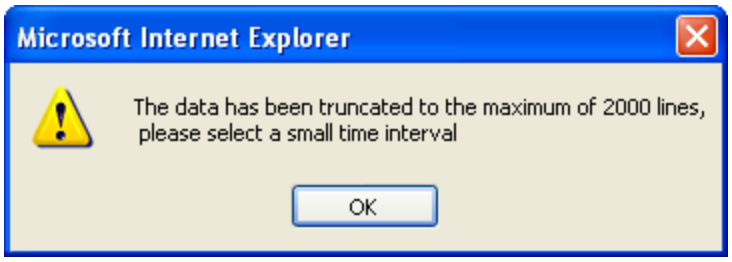


Figure 40: View Logs Truncation Dialog

Note: The logs displayed will be updated each time the filter criterion is changed.

6. The view logs screen is not dynamically updated. If you are viewing logs which include the current day, you need to manually refresh the logs displayed to view recent new logs. This is done by clicking the **Refresh Logs** button.

5.9.2 Print Logs

Description:

This procedure describes how to print the logs.

Note:

- By default, a maximum of 30 days of logs are available for viewing
- The view logs screen is not dynamically updated. If you are viewing logs which include the current day, you need to manually refresh the logs displayed to view any newly generated logs.
- A maximum of 2000 logs will be displayed at a time. If the number of logs which meet the log search filter exceeds this amount, the most recent 2000 logs that meet the filter criteria are shown and a dialog will pop up recommending the user narrow their log search filter.

Required information:

- Name of printer

Steps:

1. From the MDC Admin GUI, click the **Logs & Alarms** task on the left navigation menu.
2. The Logs & Alarms screen of the Mobile Device Checkout Admin appears.
3. Click **View Logs** from either the main task area or the Logs & Alarms submenu on the left navigation menu.
4. The View Logs screen appears. By default, the logs for the current day and all log severities will be displayed. Certain log severities are color coded for easier viewing.
5. The logs displayed can be filtered by date, time, and severity as described in Section 5.9.1 *View Logs*
6. Click the **Print Logs** button to print the displayed logs.
7. A separate browser window will appear, showing the logs formatted for printing. This new window will be an updated snapshot of the logs. Depending on the log filter criteria, these logs may differ from the logs shown in the View Logs windows. Certain log severities are color coded for easier viewing:
    a. EMERG and CRIT logs are red.
    b. ERR logs are orange.
    c. WARNING logs are gold.
    d. All other logs (INFO, NOTICE, and ALERT) are white.

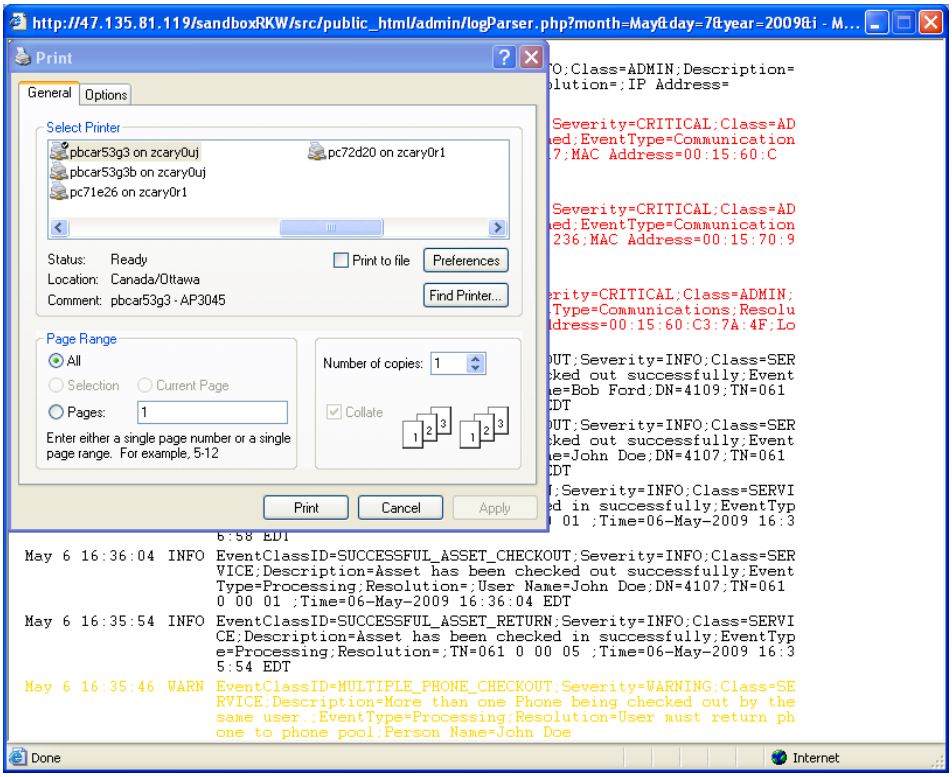


Figure 41: Print Dialog from Print Logs

8. At the same time, a Print popup dialog will also appear. **Select** the printer where you wish to print the logs. Click **Print** to start the printing of the logs. Both the Print dialog and formatted log windows will close.

5.9.3 Save Log to File

Description:

This procedure describes how to save the logs in a tab delimited file.

Note:

- By default, a maximum of 30 days of logs are available for viewing.
- The view logs screen is not dynamically updated. If you are viewing logs for the current day, you need to manually refresh the logs displayed to view any newly generated logs.
- A maximum of 2000 logs will be displayed at a time. If the number of logs which meet the log search filter exceeds this amount, the most recent 2000 logs that meet the filter criteria are shown and a dialog will pop up recommending the user refine their log search filter.
- Each line in the file is a separate log. Each log has the following tab delimited fields:
    - Date
    - Log Severity
    - Host
    - Logger
    - Log message

Required information:

- Name for saved logs file
- Folder on local computer for saved logs file

Steps:

1. From the MDC Admin GUI, click the **Logs & Alarms** task on the left navigation menu.
2. The Logs & Alarms screen of the Mobile Device Checkout Admin appears.
3. Click **View Logs** from either the main task area or the Logs & Alarms submenu on the left navigation menu.
4. The View Logs screen appears. By default, the logs for the current day and all log severities will be displayed. Certain log severities are color coded for easier viewing.
5. The logs displayed can be filtered by date, time, and severity as described in Section 5.9.1 *View Logs*.
6. Click the **Save Logs** button to print the displayed logs. An updated snapshot of the logs will be generated. Depending on the log filter criteria, these logs may differ from the logs shown in the View Logs windows.
7. In Internet Explorer, a separate small browser window will appear. This is a temporary window which is not intended for viewing and should be ignored. A Save HTML Document popup dialog will also appear. Enter the following information:
    a. **File name:** Name of the log file. Default file name is “logs”.
    b. **Save as type:** Select file type from the pulldown menu. Default file type is “Text File (*.txt).
    c. **Language:** Select from the pulldown menu. Default language is “Unicode”.
    d. **Save in**: Select the folder where you wish to save the file.
    e. Click the **Save** button to save the log file as specified.

    The tab delimited file will be available in the location selected.

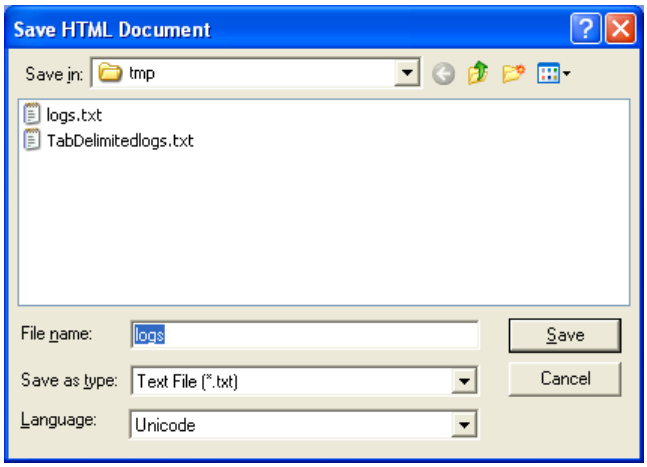


Figure 42: Save HTML Document Dialog

On browsers that don't support directly saving a file (e.g. Firefox), a separate browser window will appear along with a popup dialog instructing the administrator select the entire content of browser screen and copy/paste it to a file. Click **OK** to acknowledge the popup dialog. While there are no constraints on the file type used, copying into an Excel spreadsheet will provide optimal results and allow the administrator to use sort and filters features. **Close** the browser window when you have finish saving the contents.

5.9.4 XML Dump of Log

Description:

This procedure explains how to view the logs in XML format

Note:

- By default, a maximum of 30 days of logs are available for viewing.
- The view logs screen is not dynamically updated. If you are viewing logs which include the current day, you need to manually refresh the logs displayed to view any newly generated logs.

Required information:

- [optional] Printer
- [optional] Name for saved logs file
- [optional] Folder on local computer for saved logs file

Steps:

1. From the MDC Admin GUI, click the **Logs & Alarms** task on the left navigation menu.
2. The Logs & Alarms screen of the Mobile Device Checkout Admin appears.
3. Click **View Logs** from either the main task area or the Logs & Alarms submenu on the left navigation menu.
4. The View Logs screen appears. By default, the logs for the current day and all log severities will be displayed. Certain log severities are color coded for easier viewing.
5. The logs displayed can be filtered by date, time, and severity as described in Section 5.9.1 *View Logs*
6. Click the **XML Dump Logs** button to print the displayed logs.

7. A separate browser window will appear, showing the logs in XML format. This new window will be an updated snapshot of the logs. Depending on the log filter criteria, these logs may differ from the logs shown in the View Logs windows.

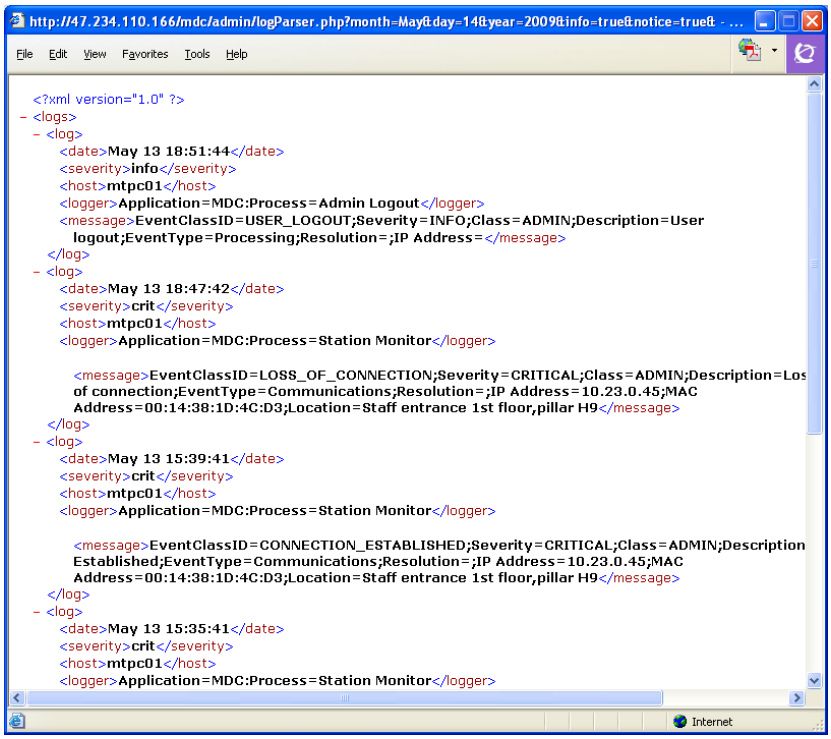


Figure 43: XML Dump of Logs

8. As with any other Windows Internet Explore window, these options (and others) are available:
    a. Select **Save As** from the **File** menu if you want to save the contents of the window. The default file name is “logParser.php”.
    b. Select **Print** from the **File** menu if you want to print the contents of the window.

5.9.5 Configure Email Recipient for Logs

Description:

This procedure describes how to configure an email recipient for the MDC administrative logs (i.e. class = ADMIN). Any critical or emergency administrative logs are emailed immediately as they occur. All other MDC administrative logs are added to a daily log digest which is emailed once a day.

Note: the daily MDC administrative log digests are stored in /var/opt/nortel/ebs/mdc/digest on the MDC server. Their naming convention is YYYYMMDD e.g. 20090917 is the MDC log digest from Sept 17, 2009. All the log digest files are compressed except for the current day. The log digest file is emailed as an attachment. After the log digest file has been successfully emailed, the file is moved to /var/opt/nortel/ebs/mdc/digest/keep. Only successfully emailed log digests will be deleted after the configured number of retention days has elapsed from the date the file was first created.

Required information:

- Email address of recipient

- Email address of sender
- Name of sender
- Hostname of SMTP Server
- SMTP port number
- Number of days to retain the log digest file from the date the file was created.

Steps:

1. From the MDC Admin GUI, click the **Logs & Alarms** task on the left navigation menu.
2. The Logs & Alarms screen of the Mobile Device Checkout Admin appears.

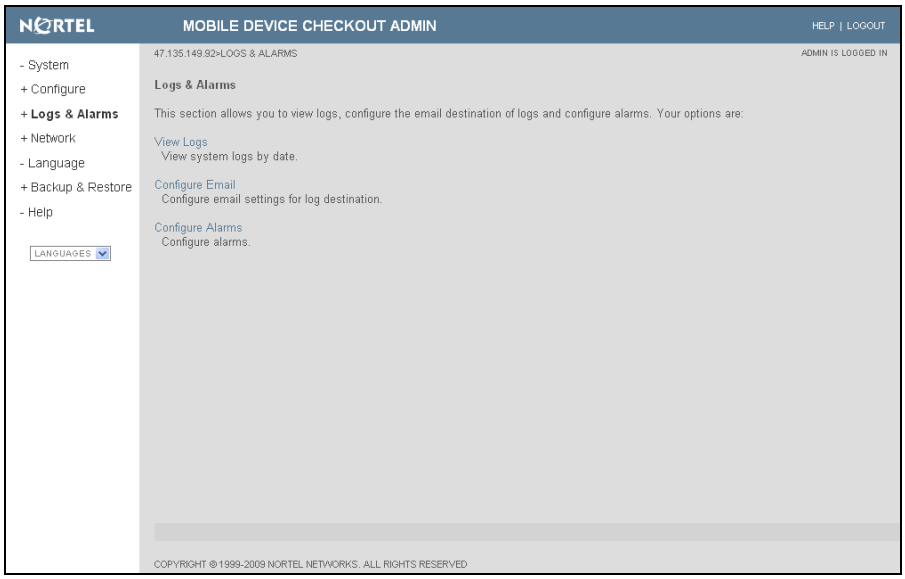


Figure 44: Logs & Alarms Screen of MDC Admin GUI

3. Click **Configure Email** from either the main task area or the Logs & Alarms submenu on the left navigation menu.
4. The Configure Email screen appears.

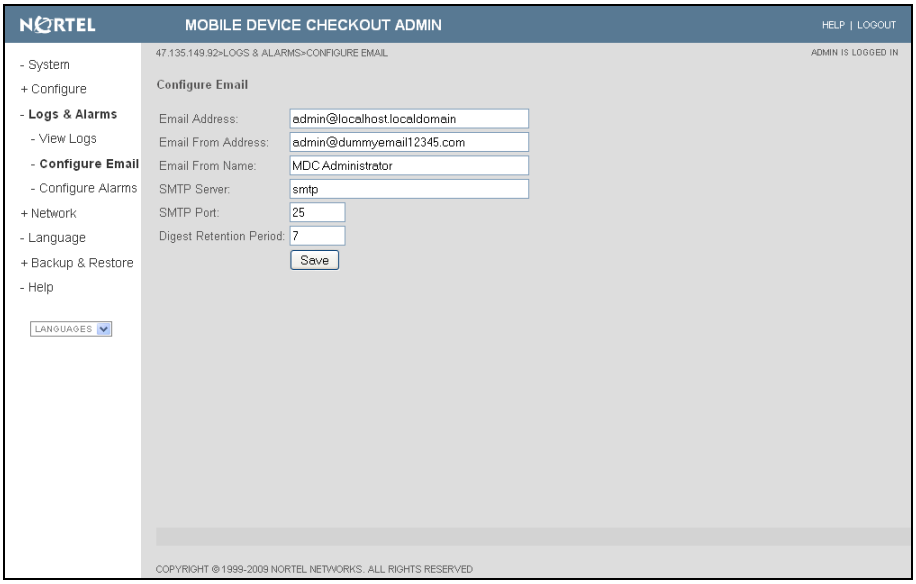


Figure 45: Configure Email Recipient for Log Digest

5. To configure the email for log digest notification, type in the following parameters:
    a. **Email Address**: recipient email address to which to send the log digest notification email(s)
    b. **Email From Address**: originating address sending the log digest notification emails
    c. **Email From Name:** name of originator sending log digest notification emails
    d. **SMTP Server**: hostname of SMTP Server
    e. **SMTP Port:** port used to send SMTP messages. The default SMTP port is 25.
    f. **Digest Retention Period:** number of days to retain log digest files from the date the file was first created. Default value is 7 days. Maximum value is 30 days.
6. Click the **Save** button to save the email configuration for log digest notification.
7. A message indicating the success of the action will be displayed.

5.9.6 Configure Alarms

Description:

This procedure describes how to configure and enable alarms on MDC. Each of the following type of alarms can optionally be configured:

- Enabling notification when assets have been inactive for the specified number of hours.
- Enabling notification when assets have been checked out for longer than the specified number of hours.

These notifications allow the operator to identify phones which have been either been lost, stolen or inadvertently not returned after a shift. Each type of alarm can be enabled independent of the others alarms. Setting the specified number of hours to zero will disable that type of asset monitoring.

When an enabled asset monitoring situations occurs, a log notification is generated specifying:

- the details of the asset involved
- the last user who checked out this asset (if applicable)
- the date and time when the asset was last checked out (if applicable)

When enabled, the active/overdue status is shown on a per asset basis on the View Asset screen. For further details, see Section 10.3 *View Assets*.

Required information:

At least one of the following is needed:

- [Optional] number of hours after which an asset is considered checked in (inactive) for too long
- [Optional] number of hours after which an asset is considered checked out (active) for too long

Steps:

1. From the MDC Admin GUI, click the **Logs & Alarms** task on the left navigation menu.
2. The Logs & Alarms screen of the Mobile Device Checkout Admin appears.

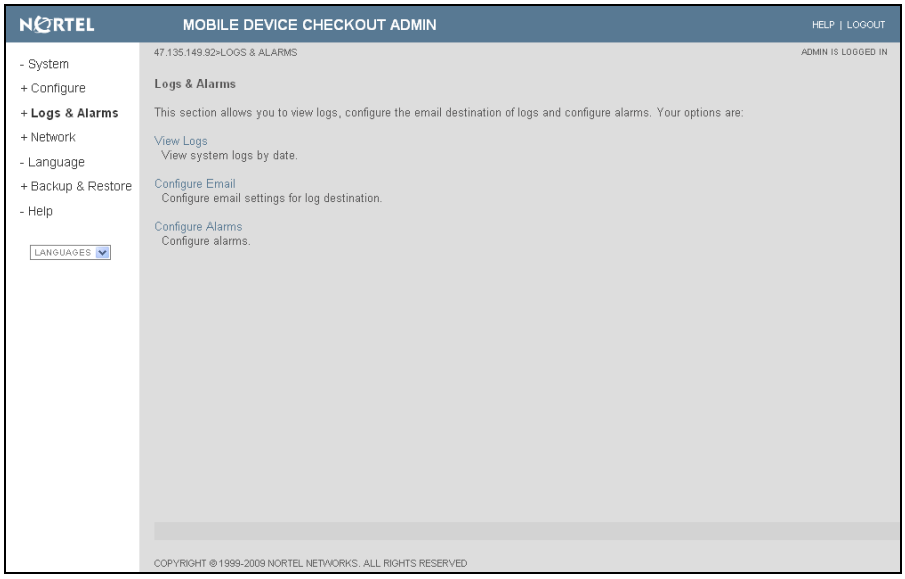


Figure 46: Logs & Alarms Screen of MDC Admin GUI

3. Click **Configure Alarms** from either the main task area or the Logs & Alarms submenu on the left navigation menu.
4. The Configure Alarms screen appears.



Figure 47: Configure Alarm Screen on MDC Admin GUI

5. To configure the following type of asset monitoring:
    a. **Asset Inactivity (returned) Timeout (in hrs)**: Type in the maximum number of hours an asset can be checked in (i.e. inactive). For phones which are inactive for longer than this period, a log notification will be generated. Setting this value to zero will disable any inactive asset monitoring.
    b. **Asset Overdue (checked-out) Timeout (in hrs)**: Type in the maximum number of hours an asset can be checked out (i.e. actively used by a user). For phones which are active for longer than this period, a log notification will be generated. Setting this value to zero will disable any overdue asset monitoring.
6. Click the **Save** button to save the asset monitoring configuration.
7. A message indicating the success of the action will be displayed.

5.10 Network

The Network screen is a list of the network connections which can be configured through of the MDC Admin GUI.

The Network screen is accessed with these steps:

1. From the MDC Admin GUI, click the **Network** task on the left navigation menu.
2. The main Network screen will appear.

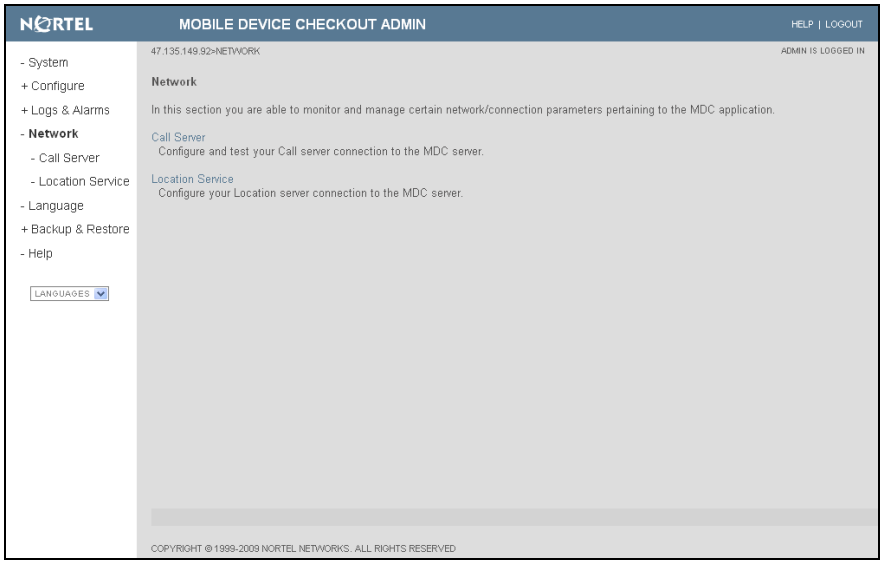


Figure 48: Network Screen on MDC Admin GUI

For more information on Network submenus:

- For the **Call Server** submenu, refer to Section 9 *Integrating MDC Server and Call Server* for a description of configuring call server connection to MDC. Further information related to integrating MDC with the call server can be found in:
  - Section 10 *Managing Assets (Phones)* for the description of the procedures and MDC Admin GUI screens associated with managing assets.
  - Section 11 *Managing Users* for the description of the procedures and MDC Admin GUI screens associated with managing users.
  - Section 12 *Managing Roles* for the description of the procedures and the MDC Admin GUI screens associated with managing roles.
- For the **Location Service** submenu, refer to Section 8.2 *Integrating MDC Server and Location Service* for a description of configuring location service connection to MDC. For further information related to integrating MDC with location service:
  - The following sections describe the different options for enabling/disabling location tracking on assets:
    - Section 10.7 *Enable Location Tracking for All Assets*
    - Section 10.8 *Disable Location Tracking for All Assets*
    - Section 10.5 *Update Asset from View Screen*
    - Section 10.6 *Update Asset from Insert/Update Screen*
    - Section 10.2 *Insert New Asset*
  - The following sections describe the different options for enabling/disabling location tracking on user:
    - Section 11.6 *Enable Location Tracking for All Users*
    - Section 11.7 *Disable Location Tracking for All*
    - Section 11.4 *Update Users from View Screen*

- Section 11.5 *Update Users from Insert/Update Screen*
- Section 11.1 *Insert New Users*

- A description of licensing related to location service is described in Section 7 *MDC Licensing and Keycode Retrieval System (KRS)*

5.11 Language

Description:

This configures the languages which will be supported in the MDC stations and the order in which the languages will appear on the MDC stations. By default, English is selected. If nothing is selected, the default language used on the MDC station will be English.

WARNING: This procedure is service affecting when the MDC Station is rebooted.

See Section 13 *Managing MDC Stations* for further information on managing MDC Stations.

Required information:

- Languages and order of these languages on the MDC Station

Steps:

1. From the MDC Admin GUI, click the **Language** task on the left navigation menu. (This is the first occurrence of Language in the navigation list and not the pulldown menu at the bottom of the list).
2. The Language screen of the Mobile Device Checkout Admin appears.
3. Using the following actions, select the languages and the order in which the languages will appear on the MDC Station:
    a. Uncheck the boxes of all languages which should not appear on the MDC Station.
    b. For each language to be supported on the MDC Station, click the check box beside the language to select it for inclusion.
    c. Re-organize the list of supported languages into the order in which they need to appear on the MDC Station by clicking the **up** or **down** selection beside a language to move its position in the list.

    For each action, a pop-up dialog will appear to remind the user that this change will not take effect until the MDC Stations have been restarted. Click the **OK** button. A successful language update message will also appear. Continue configuring until the necessary languages have been selected and their order arranged.

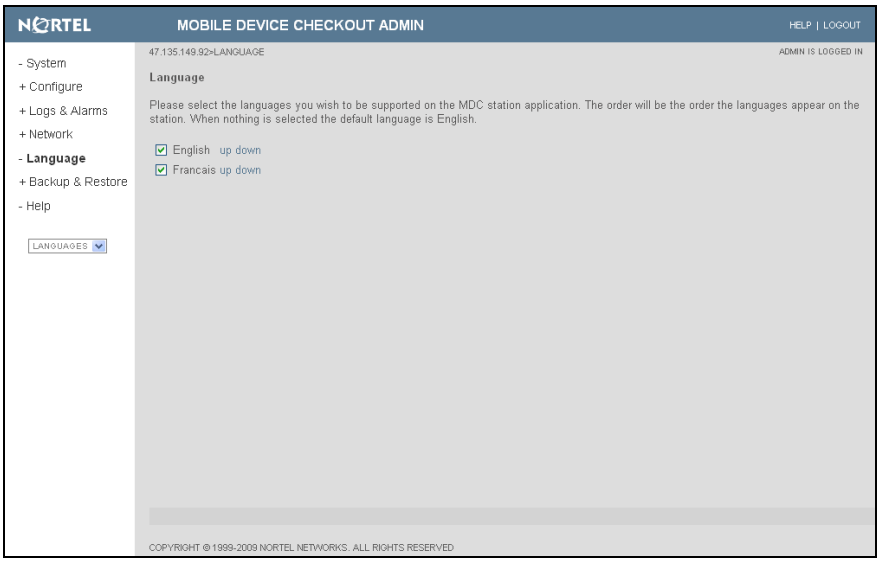


Figure 49: Configuring Languages displayed on MDC Station

4. It is recommended that all MDC Stations be rebooted. The language changes will not take effect on the MDC Station screens until that MDC Station is rebooted. See Section 13.11 *Reboot All MDC Stations* for the detailed procedure.

5.12 Backup & Restore

This section describes procedures and MDC Admin GUI screens for managing the backup and restoration of MDC application data.

The MDC uses secure FTP to transfer backup copies of its data (database and configuration) to a configurable backup server for emergency contingency purposes. If needed, there is a restore procedure to recover the backup MDC data onto MDC Server.

The naming convention of the MDC backup files follows this format: nortel_ebs_mdc.<year>-<month>-<date>-<hour>-<minutes>-<seconds>.sql-tar.gz. An example is nortel_ebs_mdc.2009-05-12-16-50-13.sql.tar.gz.

WARNING: The backup server must be configured before any manual or scheduled backups can be successful. See Section 5.12.1 *Backup Server* for instructions on configuring the backup server information.

WARNING: It is up to the user to manually manage the number of backup images and the file space used on the backup server. The MDC application will continue to make backup images based on the configured backup schedule.

WARNING: Ensure that a copy of the barcode label file is archived, as the ZebraDesigner label files are not included as part of MDC backups.

WARNING: the system ID file /opt/nortel/ebs/cklt/ckltsysid.xml and license file opt/nortel/ebs/cklt/license/ckltlicense.xml are not part of the MDC backup. The system ID file is automatically created when licensing server cklt is started. The licensing file can be retrieved from KRS system. See Section 7 *MDC Licensing and Keycode Retrieval System (KRS)* for more details.

WARNING: It is the responsibility of the user to retain and maintain backups of all the customized MDC Station configuration files used in the commissioning of these devices. These are not included in the backup of MDC server.

The following procedures are described:

- Backup Server
- Backup Schedule
    - Add Backup Schedule
    - Update Backup Schedule
    - Delete Backup Schedule
- Manual Backup
- Restore From Backup Server
- Restore from Alternate Location

5.12.1 Backup Server

Description:

This procedure describes how to configure the backup server.

Required information:

- IP address of backup server
- Port used for SFTP
- Userid and password to log in to SFTP on backup server
- Directory of backup server on which to store MDC backup images

Steps:

1. From the MDC Admin GUI, click the **Backup & Restore** task on the left navigation menu.
2. The main Backup and Restore screen will appear.

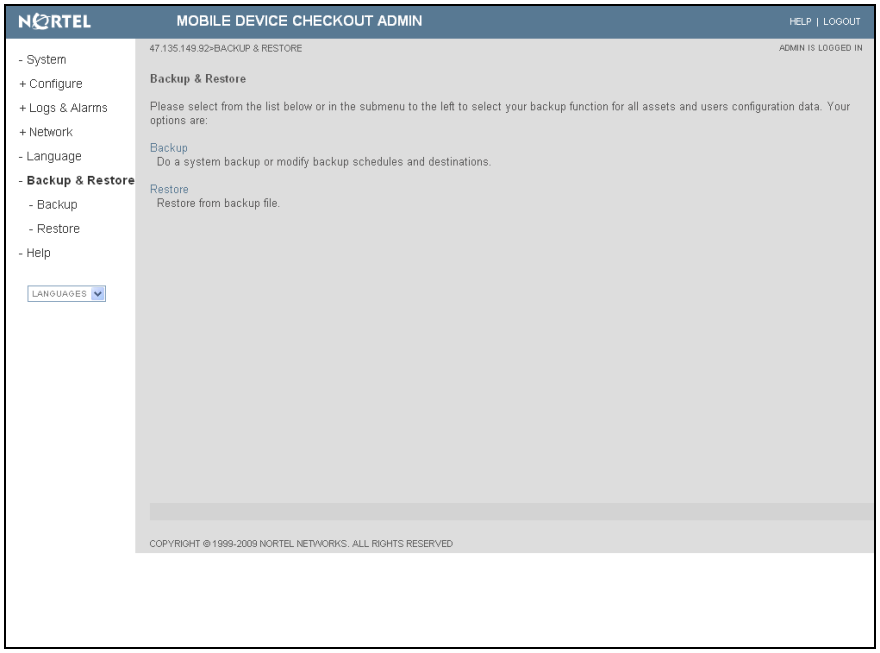


Figure 50: Backup & Restore Screen on MDC Admin GUI

3. Click **Backup** from either the main task area or the Backup & Restore submenu on the left navigation menu.
4. The Backup screen of the Mobile Device Checkout Admin appears. The Backup Schedule is shown in the main task working area.

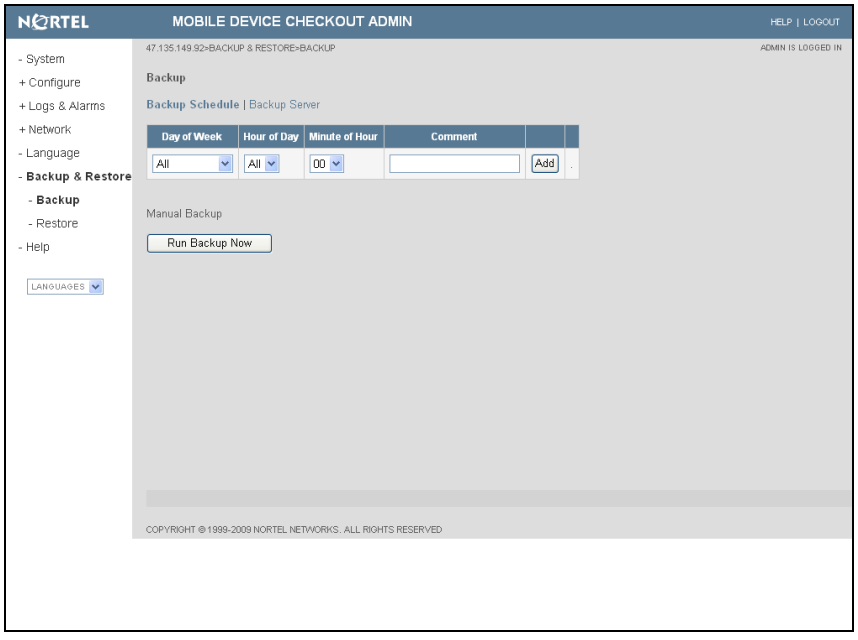


Figure 51: Backup Screen of MDC Admin GUI

5. Click **Backup Server** on the Backup main task working area to configure where the MDC backups will be stored.
6. The Backup Server screen appears.
7. To configure the backup server, type in the following parameters:
    a. **IP address**: IP address of the backup server which will act as repository for MDC backup files.
    b. **Port**: port used for SFTP. By default, this is 22.
    c. **Userid:** used to log in to SFTP utility on the backup server.
    d. **Password**: password for SFTP login in to the backup server.
    e. **Remote Directory Path:** directory on the backup server where backup files will be stored.

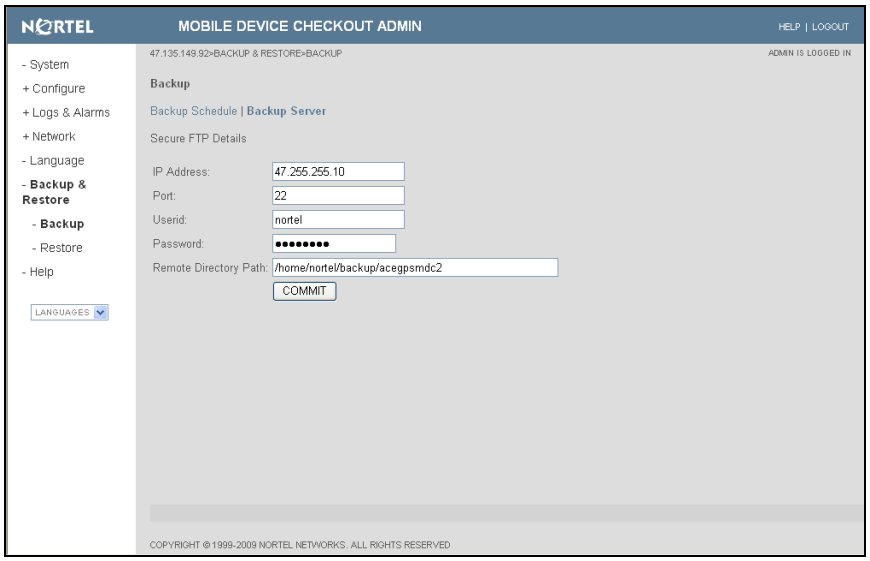


Figure 52: Backup Server Screen of MDC Admin GUI

8. Click the **Commit** button to save the configuration of the backup server. A test connection will automatically be run to verify the backup server configuration.
9. A message indicating the success of the action will be displayed...

5.12.2 Backup Schedule

5.12.2.1 Add Backup Schedule

Description:

This section describes the configuration for automatic backup of MDC application's data.

WARNING: The backup server must be configured before any scheduled backups can be successful. See Section 5.12.1 *Backup Server* for instructions on configuring the backup server information.

Required information:

- Day of Week or All to schedule backups

- Hour of Day and Minute of Hour to initiate backup
- Descriptive text comment

Steps:

1. Click **Backup Schedule** from the backup screen of the Mobile Device Checkout Admin GUI (underneath the Backup title on the main task working area). Or click **Backup** from the Backup & Restore submenu on the left navigation menu.
2. The Backup screen of the Mobile Device Checkout Admin appears. The Backup Schedule is shown in the main task working area.

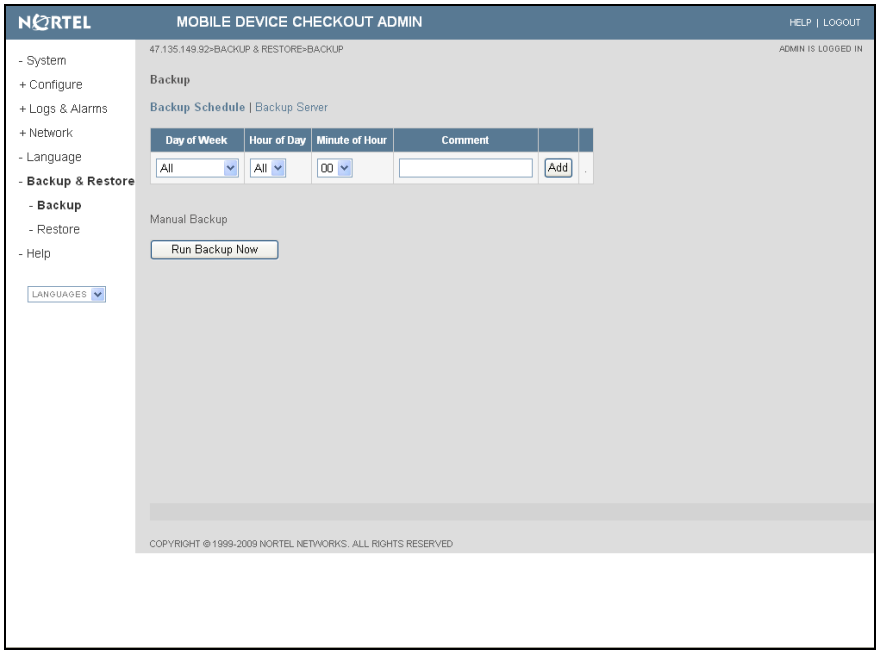


Figure 53: Backup Screen of MDC Admin GUI

3. To configure a time & date for automatic backup of MDC data, input the following parameters from the pulldown menus:
    a. **Day of Week**: Select the day of the week when the backup will be performed from the pulldown menu. Selecting “All” will schedule a backup every day of the week.
    b. **Hour of Day**: Select the hour when the backup will be performed from the pulldown menu. This field is based on a 24-hour clock. Selecting “All” will schedule a backup every hour.
    c. **Minute of Hour:** Select the minute when the backup will be performed from the pulldown menu. The options are 15-minute intervals.
    d. **Comment**: Type in descriptive text.
4. Click the **Add** button to save the schedule entry of backup of MDC data.
5. A message indicating the success of the action will be displayed. If successful, the newly added schedule entry will be displayed in the backup schedule.

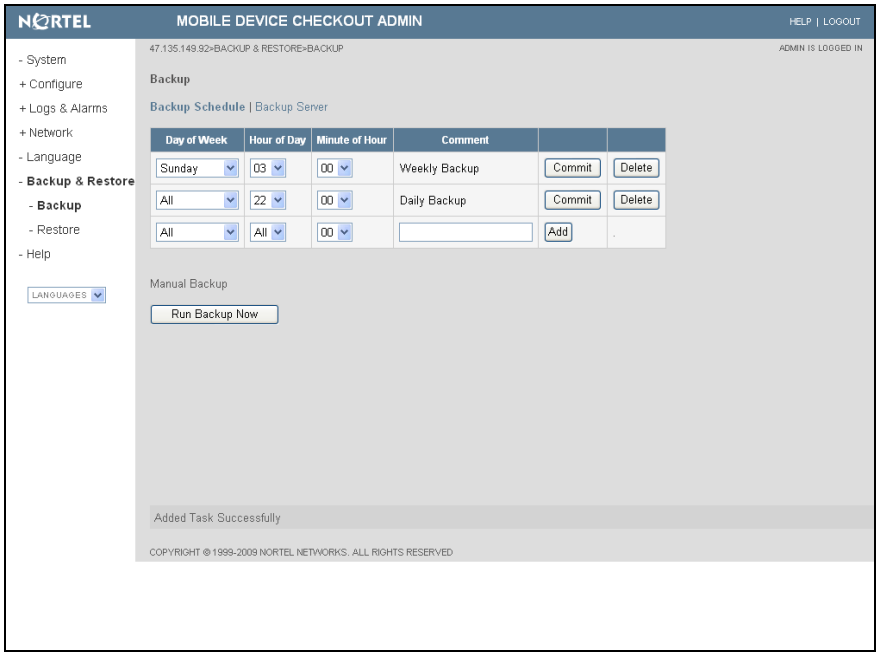


Figure 54: Successful Add to Backup Schedule Message

6. When the scheduled backup runs, you should be able to see the newly created backup image in the Restore screen. See Section 5.12.4 *Restore* From Backup Server for the procedure.

5.12.2.2 Update Backup Schedule

Description:

This section describes modifying the configuration for automatic backup of MDC application's data.

WARNING: It is recommended that only a single entry row be modified at a time, as the Commit will only save changes to a single entry row. Any updates to other entry rows in the Backup Schedule table will be lost when the table is refreshed after the commit.

WARNING: The backup server must be configured before any scheduled backups can be successful. See Section 5.12.1 *Backup Server* for instructions on configuring the backup server information.

Required information:

- Scheduled backup which will be updated
- One or more updated information items:
  - Day of Week or All to schedule backups
  - Hour of Day and./or Minute of Hour to initiate backup
  - Descriptive text comment

Steps:

1. Click **Backup Schedule** from the backup screen of the Mobile Device Checkout Admin GUI (underneath the Backup title on the main task working area). Or click **Backup** from the Backup & Restore submenu on the left navigation menu.

2. The Backup screen of the Mobile Device Checkout Admin appears. The Backup Schedule is shown in the main task working area.
3. Locate the scheduled automatic backup that needs to be updated. The following fields can be updated:
    a. **Day of Week**: Select the updated day of the week when the backup will be performed from the pulldown menu. Selecting “All” will schedule a backup every day of the week.
    b. **Hour of Day**: Select the updated hour when the backup will be performed from the pulldown menu. This field is based on a 24-hour clock. Selecting “All” will schedule a backup every hour.
    c. **Minute of Hour:** Select the updated minute when the backup will be performed from the pulldown menu. The options are 15-minute intervals.
    d. **Comment**: To edit this field, place the cursor in the field and click. The field will become highlighted as a data entry field. Type in updated descriptive text.
4. Click the **Commit** button to save the updated schedule entry of backup of MDC data.
5. A message indicating the success of the action will be displayed. If successful, the Backup Schedule table will be updated with the modified schedule changes entered.

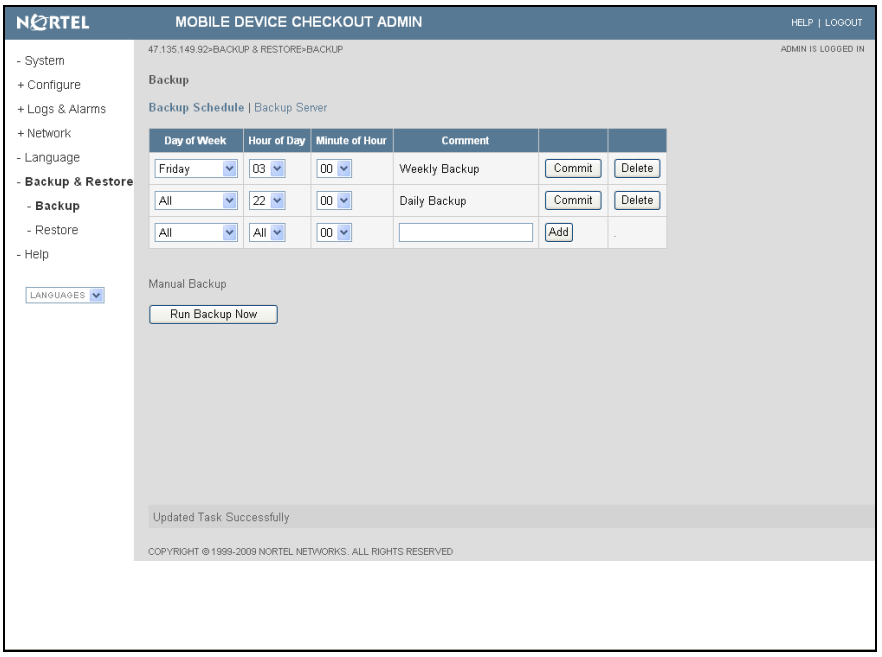


Figure 55: Successful Updated Backup Schedule Message

5.12.2.3 Delete Backup Schedule

Description:

This section describes how to delete a scheduled automatic backup of MDC application’s data.

WARNING: It is recommended to save any changes made to Backup Schedule table prior to deleting a scheduled backup entry. Any unsaved updates to other entry rows in the Backup Schedule table will be lost when the table is refreshed after the delete.

Required information:

- Scheduled backup which will be deleted

Steps:

1. Click **Backup Schedule** from the backup screen of the Mobile Device Checkout Admin GUI (underneath the Backup title on the main task working area). Or click **Backup** from the Backup & Restore submenu on the left navigation menu.
2. The Backup screen of the Mobile Device Checkout Admin appears. The Backup Schedule is shown in the main task working area.
3. Locate the scheduled automatic backup that needs to be deleted. Click the **Delete** button on that table row entry to delete this scheduled automatic backup.
4. A delete confirmation popup dialog will appear. Click **OK** to confirm deleting the scheduled backup.

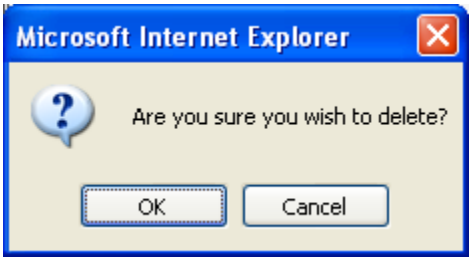


Figure 56: Delete Backup Schedule Confirmation Dialog

5. A message indicating the success of the action will be displayed. If successful, the Backup Schedule table will be updated and the deleted backup will be removed from the list of scheduled backups.

5.12.3 Manual Backup

Description:

This procedure describes how to perform a manual backup of MDC data.

WARNING: The backup server must be configured before initiating a manual backup. See Section 5.12.1 *Backup Server* for instructions on configuring the backup server information.

WARNING: Ensure that a copy of the barcode label file is archived, as the ZebraDesigner label files are not included as part of MDC backups.

WARNING: It is the responsibility of the user to retain and maintain backups of all the customized MDC Station configuration files used during the commissioning of the MDC Stations hardware. These are not included in the backup of MDC server.

WARNING: the system ID file /opt/nortel/ebs/cklt/ckltsysid.xml and license file opt/nortel/ebs/cklt/license/ckltlicense.xml are not part of the MDC backup. The system ID file is automatically created when licensing server cklt is started. The licensing file can be retrieved from KRS system. See Section 7 *MDC Licensing and Keycode Retrieval System (KRS)* for more details.

Required information:

None

Steps:

1. From the MDC Admin GUI, click the **Backup & Restore** task on the left navigation menu.

2. The main Backup and Restore screen will appear.
3. Click **Backup** from either the main task area or the Backup & Restore submenu on the left navigation menu.
4. The Backup screen of the Mobile Device Checkout Admin appears. The Backup Schedule is shown in the main task working area. Beneath the Backup Schedule is the Manual Backup.

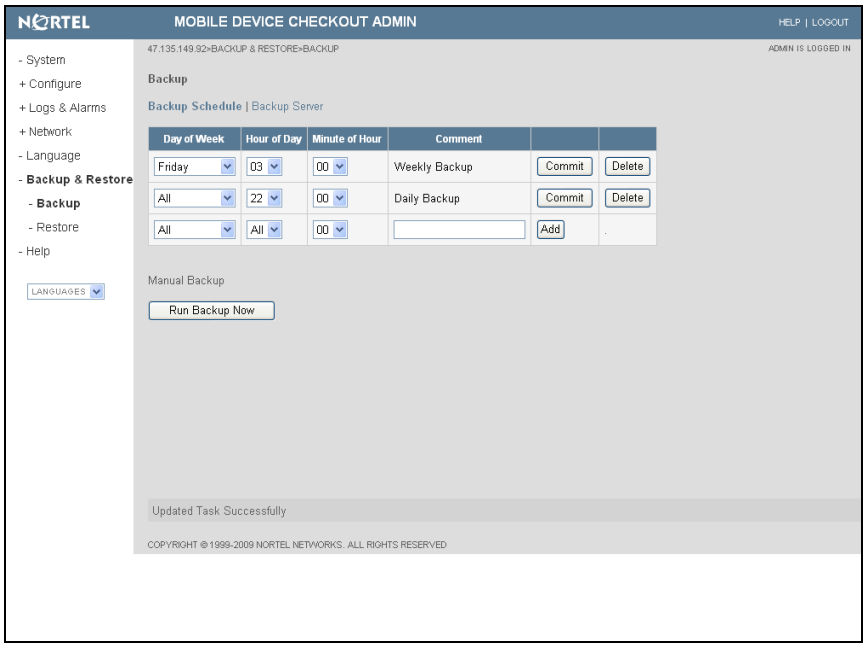


Figure 57: Backup Screen of MDC Admin GUI

5. Under Manual Backup, click the **Run Backup Now** button to initiate a manual backup.
6. A message indicating the success of the action will be displayed. If successful, a progress message will be displayed when the backup is initiated followed by a successfully done info message when the backup has been copied to the backup server.
7. With successful backups, you should be able to see the newly created backup image in the Restore screen. See Section 5.12.4 *Restore* From Backup Server for the procedure.

5.12.4 Restore From Backup Server

Description:

This procedure describes how to restore MDC data from an earlier backed-up image.

TIP: The backup server must be configured and backups (either scheduled or manual) must have been performed earlier before attempting a restore. See Section 5.12.1 *Backup Server* for instructions on configuring the backup server information.

WARNING: Only restore backups made from the same MDC Server running the same MDC software release. (Release 2.0 or Release 2.0.1)

The naming convention of the MDC backup files follows this format: nortel_ebs_mdc.<year>-<month>-<date>-<hour>-<minutes>-<seconds>.sql-tar.gz. For example, this is a typical MDC backup image name: nortel_ebs_mdc.2009-05-12-16-50-13.sql.tar.gz.

WARNING: This procedure is service affecting. This procedure will overwrite the MDC configuration information and the contents of the MDC database. You may wish to perform a manual backup **prior to restoring** if you want to be able to return to the current configuration and database.

Required information:

- MDC backup image to restore (approximate <year>-<month>-<date>-<hour>-<minutes>-<seconds> the backup was created)

Steps:

1. From the MDC Admin GUI, click the **Backup & Restore** task on the left navigation menu.
2. The main Backup and Restore screen will appear.
3. Click **Restore** from either the main task area or the Backup & Restore submenu on the left navigation menu.
4. The Restore screen of the Mobile Device Checkout Admin appears. A list of available backup images on the backup server is shown in the main task working area. A warning message will appear if the backup server credentials are missing or invalid.
5. **Click** the backup image you want to restore from the list. This will highlight the selected backup image in the list.

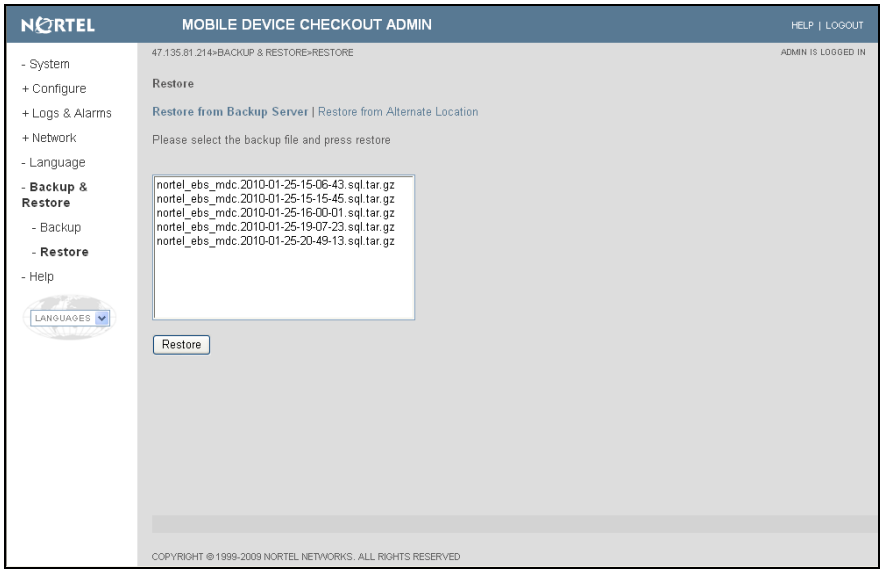


Figure 58: Restore Screen of MDC Admin GUI

6. Click the **Restore** button to initiate overwriting the MDC configuration and MDC database with the contents of the backup image. If it is a large backup image, a progress message will be shown at the bottom of the screen.
7. A message indicating the success of the action will be displayed.
8. The restored data may affect the configuration of the MDC Stations. It is recommended that all MDC Station be rebooted. See Section 13.11 *Reboot All MDC Stations* for the detailed procedure.

5.12.5 Restore from Alternate Location

Description:

This procedure describes how to perform a restore of MDC data using an alternate backup server where an earlier backed-up image is located.

This procedure is used to perform a restore of an MDC backup image when there is no backup server information available in the database. This procedure can be used to restore the MDC configuration and database information if the MDC server software ever has to be reinstalled as part of disaster recovery. This procedure may also be used when the user wants to initiate a restore from a different location other than the provisioned backup server, perhaps due to network issues.

Backups (either scheduled or manual) must have been performed prior to attempting a restore. See Section 5.12.1 *Backup Server* for instructions on configuring the backup server information.

WARNING: Only restore backups made from the same MDC Server running the same MDC software release. (Release 2.0 or Release 2.0.1)

The naming convention of the MDC backup files follows this format: nortel_ebs_mdc.<year>-<month>-<date>-<hour>-<minutes>-<seconds>.sql-tar.gz. For example, this is a typical MDC backup image name: nortel_ebs_mdc.2009-05-12-16-50-13.sql.tar.gz.

WARNING: This procedure is service affecting. This procedure will overwrite the MDC configuration information and the contents of the MDC database. You may wish to perform a manual backup **prior to restoring** if you want to be able to return to the current configuration and database.

Required information:

- IP Address of alternate backup server
- Port used for SFTP
- Userid and Password to log into SFTP on alternate backup server
- Directory of alternate backup server where MDC backup images is stored
- MDC backup image to restore (approximate <year>-<month>-<date>-<hour>-<minutes>-<seconds> the backup was created)

Steps:

1. From the MDC Admin GUI, click the **Backup & Restore** task on the left navigation menu.
2. The main Backup and Restore screen will appear.
3. Click **Restore** from either the main task area or the Backup & Restore submenu on the left navigation menu.
4. The Restore screen of the Mobile Device Checkout Admin appears. A list of available backup images on the backup server is shown in the main task working area if information on the backup server is available in the database.
5. Click **Restore from Alternate Location** on the Restore main task working area.
6. The Restore from Alternate Location screen appears.

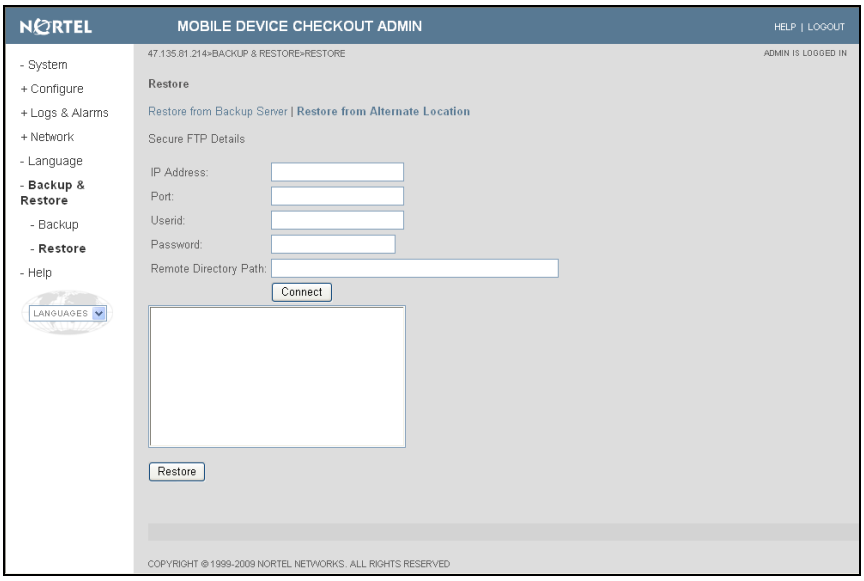


Figure 59: Restore from Alternate Location Screen of MDC Admin GUI

7. To initiate an alternate restore, you will need to configure the server where the alternate restore will locate the backup image. Type in the following parameters:
    a. **IP address**: IP address of server which has the MDC backup image you want to restore.
    b. **Port**: port used for FTP. By default, this is 22.
    c. **Userid:** used to log in to ftp utility on backup server.
    d. **Password**: password for ftp login into backup server
    e. **Remote Directory Path:** directory on the backup server where backup images are located.
8. Click the **Connect** button.
9. A list of available backup images on the server will be displayed. Otherwise, if it was unable to connect, an error message will appear requesting the user validate the credential to the alternate backup server and try again.

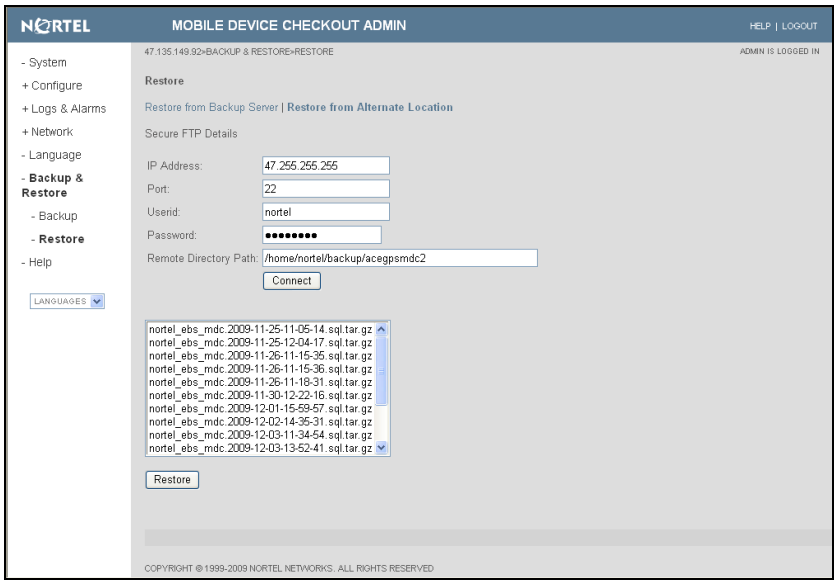


Figure 60: List of backup images available for Restore from Alternate Location

10. **Click** the backup image you want to restore from the list. This will highlight the selected backup image in the list.
11. Click the **Restore** button to initiate overwriting the MDC configuration and MDC database with the contents of the backup image.
12. A message indicating the success of the action will be displayed.
13. The restored data may affect the configuration of the MDC Stations. It is recommended that all MDC Station be rebooted. See Section 13.11 *Reboot All MDC Stations* for the detailed procedure.

6 Status, Starting and Stopping the MDC Application

6.1 Status of the MDC Application

Description:

This procedure displays the status of the MDC application.

Note: Depending on OS hardening procedures, it may not be possible to log into MDC Server directly as root. If this is the case, the user can log in as another user and switch user privileges to root (e.g. **su – root**).

Required information:

- IP address of MDC server
- Linux root user password for MDC server
- Non-root username and password for MDC server

Steps:

1. Open a terminal window connection to the MDC server and log in as root.
2. Type **service mdc status**
3. The following are examples of the output (Note: the pid [process id] will differ).

   The output while the MDC application is running.

```
# service mdc status
EventProcessor.php (pid  22018) is running...
StationMonitor.php (pid  22240) is running...
WatchDog.php (pid  22294) is running...
BackupManager.php (pid  22079) is running...
ProcessingQueue.php (pid  22132) is running...
KeepAliveCS1K.php (pid  22348) is running...
EventNotificationProcessor.php (pid  11913) is running...
```

   The output while the MDC application is stopped.

```
 # service mdc status
EventProcessor.php is stopped
StationMonitor.php is stopped
WatchDog.php is stopped
BackupManager.php is stopped
ProcessingQueue.php is stopped
KeepAliveCS1K.php is stopped
EventNotificationProcessor.php is stopped
```

6.2 Starting the MDC Application

Description:

This procedure describes starting the MDC application. This will normally not be necessary as the MDC application is automatically started following server reboots, MDC installation and MDC upgrades.

Note: Depending on OS hardening procedures, it may not be possible to log into MDC Server directly as root. If this is the case, the user can log in as another user and switch user privileges to root (e.g. **su – root**).

Required information:

- IP address of MDC server
- Linux root user password for MDC server
- Non-root username and password for MDC server

Steps:

1. Open a terminal window connection to the MDC server and log in as root.
2. Type **service mdc start**
3. The following is an example of the output:

```
# service mdc start
Starting MDC EventProcessor.php:                          [  OK  ]
Starting MDC BackupManager.php:                           [  OK  ]
Starting MDC ProcessingQueue.php:                         [  OK  ]
Starting MDC StationMonitor.php:                          [  OK  ]
Starting MDC WatchDog.php:                                [  OK  ]
Starting MDC KeepAliveCS1K.php:                           [  OK  ]
Starting MDC EventNotificationProcessor.php:              [  OK  ]
```

4. Typing **service mdc status** should show all the MDC processes as running.

6.3 Restarting the MDC Application

Description:

This procedure describes restarting the MDC application. This will normally not be necessary except for troubleshooting purposes as the MDC application is automatically started following server reboots, MDC installation and MDC upgrades.

WARNING: The procedure is service affecting.

Note: Depending on OS hardening procedures, it may not be possible to log into MDC Server directly as root. If this is the case, the user can log in as another user and switch user privileges to root (e.g. **su – root**).

Required information:

- IP address of MDC server
- Linux root user password for MDC server
- Non-root username and password for MDC server

Steps:

1. Open a terminal window connection to the MDC server and log in as root.
2. Type **service mdc restart**
3. The following is an example of the output.

```
# service mdc restart
                                                           [  OK  ]
Starting MDC EventProcessor.php:                           [  OK  ]
Starting MDC BackupManager.php:                            [  OK  ]
Starting MDC ProcessingQueue.php:                          [  OK  ]
Starting MDC StationMonitor.php:                           [  OK  ]
Starting MDC WatchDog.php:                                 [  OK  ]
Starting MDC KeepAliveCS1K.php:                            [  OK  ]
Starting MDC EventNotificationProcessor.php:               [  OK  ]
```

5. Typing **service mdc status** should show all the MDC processes as running.

6.4 Stopping the MDC Application

Description:

This procedure describes stopping the MDC application. This will normally not be necessary except for troubleshooting purposes.

WARNING: The procedure is service affecting.

Note: Depending on OS hardening procedures, it may not be possible to log into MDC Server directly as root. If this is the case, the user can log in as another user and switch user privileges to root (e.g. **su – root**).

Required information:

- IP address of MDC server
- Linux root user password for MDC server
- Non-root username and password for MDC server

Steps:

1. Open a terminal window connection to the MDC server and log in as root.
2. Type **service mdc stop**
3. You should see an [OK] response.

   Example output:

```
# service mdc stop
                                                           [  OK  ]
```

4. Typing **service mdc status** should show all the MDC processes are stopped.

7 MDC Licensing and Keycode Retrieval System (KRS)

This section describes the required interactions with the Nortel Keycode Retrieval System (KRS) to obtain and update keycode licenses to enable features on the MDC system. The licensed features of MDC should be purchased beforehand. The licensed features available are quantities of:

- MDC Stations
- assets (phones)
- [optional] location tracked enabled users
- [optional] enable roles on MDC Stations

A keycode license file is generated for a specific MDC system through KRS. This license file must be transferred to the specified MDC Server to enable the licensed features of that MDC system. Subsequently, the number of licenses for a specific MDC Server can be updated through KRS and the updated license file must again be transferred to the specified MDC Server to enable the licensing changes.

KRS supports Try-n-Buy licenses for MDC which allow a 30-day trial of MDC functionality at no cost for a specific MDC Server. The user can create a Try-n-Buy license for each feature only once for a specific MDC Server. Unlike the flexibility of purchased licenses, when an individual feature is trialed the quantities are fixed for Try-n-Buy licenses for MDC at:

- 2 MDC Stations
- 50 assets (phones)
- 100 location-tracked-enabled users
- enable roles on all MDC Stations

The user is encouraged to purchase and transfer permanent licenses for MDC prior to the end of the trial period. When applied on an MDC Server, the permanent license for a feature will override any Try-n-Buy license for the same feature. If the Try-n-Buy licenses expire at the end of the 30-day period without being replaced by permanent licenses, the MDC data will be maintained but the MDC functionality will stop working.

The MDC Admin GUI will indicate the total number of licenses available and in use on their Assets, Users and Station screens. The MDC screen will also indicate when there are no licenses, or Try-n-Buy licenses have expired.

The role selection is accessed via the MDC Stations. To enable the roles functionality on an MDC Server, the number of role licenses must match (or be greater than) the number of MDC Station licenses. The MDC Admin GUI Role administration screens are not accessible if there are no role licenses. If there is insufficient number of role licenses or the role Try-n-Buy licenses have expired, the Role administration screens will no longer be accessible and the role selection screens will no longer appear on any MDC Stations. However, any existing data is retained in the database and can be reactivated when the role licensing problem is corrected.

The MDC application will automatically resynchronize licensing information every 5 hours with the license server on the MDC Server. When the keycode license file is updated, new license information may not appear for up to 5 hours on existing MDC Admin GUI sessions. However, the user can take manual action to update the licensing information on the MDC Admin GUI sessions and MDC stations as described in Section 7.7 *Update Licensing Information in the MDC Application.*

TIP: The KRS User Guide for MDC is available from KRS. See Section 7.3 *Login into KRS* for how to access KRS. Within KRS, select **Product Control > Documentation, Forms & USER GUIDES.**

7.1 Required Information for KRS

Required Information:

- Username and password to access KRS. See Section 7.8.1 *Register for KRS Access* for how to register for KRS access.
- Site name for this specific MDC system. Blanks spaces are not allowed within the site name.
- A copy of the System ID file for the MDC Server. This file is automatically generated during MDC installation. The location of the system ID file is **/opt/nortel/ebs/cklt/ckltsysid.xml**
- Electronic authorization codes for purchased MDC licenses features. This can be one of the following:
    - SAP Sale Order Number/ Nortel Order Number (COEO)
    - Customer PO Number
    - SAP Non Stock PO Number
    - Numeric Authorization Code
- How many licensed features are to be allocated for this specific MDC :
    - Number of MDC Stations (kiosks)
    - Number of assets (phones)
    - [Optional]Number of location-tracked-enabled users when location tracking is being used
    - [Optional] Number of roles licenses. Note: the total number of role licenses on the MDC Server must match (or be greater than) the number of MDC Stations licenses otherwise the role functionality is not enabled.
- Folder on local computer in which to place copy of the MDC keycode license file.
- IP address for this specific MDC Server.
- Root password for this specific MDC Server
- Non-root username and password for this specific MDC Server

7.2 High-Level Overview of Process to Obtain Keycode from KRS

Here is a high-level overview of the process to obtain the keycode license file for MDC from KRS:

- Log in to KRS with Product Family of **Enterprise Business Solution.** See Section 7.3 *Login into KRS* for details.
- Register MDC product as site (if this has not already been done). See Section 7.4 *Register MDC* for details.
- [Optional] Select **eAuthCode Management** from KRS navigation menu to review PO. Refer to the KRS product documentation for more information on this feature.
- Select **Product Control > Generate Keycode** from KRS navigation menu to generate a keycode for a specific site based on allocation from electronic authorization codes. The allocations can be from multiple electronic authorization codes if necessary. See Section 7.5 *Generate and Retrieve Keycode for MDC* for details.

- You will automatically be re-directed to **Product Control > Retrieve Keycode** to **Download Keycode** file for the keycode which was created in the previous step. See Section 7.5 *Generate and Retrieve Keycode for MDC* for details.
- Copy keycode license file onto the MDC Server and apply the licenses to the licensing server. See Section 7.6 *Copy Keycode File onto MDC Server and Apply Licenses* for details.
- Update licensing information for MDC Admin GUI sessions and MDC stations as needed. See Section 7.7 *Update Licensing Information in the* MDC for details.

In addition, the following procedures are described:

- Section 7.8.3 *Generate Try-n-Buy Licenses for MDC* explains how to create 30-day no-cost trial license for MDC features.
- Section 7.8.2 *Retrieve Keycode for MDC System* explains how to retrieve an existing license for the MDC system.
- Section 7.8.4 *Adding More Licenses to MDC System* explains how to increase the number of licenses for an MDC system.

7.3 Login into KRS

1. Open a web browser window.
2. Go to www.nortel.com/krs
3. Select Product Family of **Enterprise Business Solutions**
4. Enter **username** and **password** on login page.

7.4 Register MDC System

You must register the MDC system before being able to generate keycodes. Product registration only needs to be done once per MDC system.

1. The default screen after login is the **Product Registration** screen. Otherwise, select **Product Control > Product Registration** from the navigation menu.
2. Select **Create.**
3. Enter the **Site Name** for the MDC. Note: Blanks spaces are not allowed within the site name. Click **Continue.**
4. Upload the unique system ID file for this MDC. Click **Browse** to locate the file on your computer and **Open** after you have selected the file in the popup dialog. (Note: The unique system ID file is originally retrieved from **/opt/nortel/ebs/cklt/ckltsysid.xml** on the MDC.) Click **Continue**.
5. Enter the location information to complete the registration. Click **Continue**.
6. After reviewing the product registration summary, click **Save**.

7.5 Generate and Retrieve Keycode for MDC System

Use this procedure to generate a keycode for a specific site based on allocation from electronic authorization codes. The allocations can be from multiple electronic authorization codes if necessary.

TIP: A functioning MDC system must have at a minimum phone and kiosk (station) licenses.

1. Select **Product Control > Generate Keycode** from the navigation menu.

2. Enter the site name used during product registration as the **System ID** to identify the system for which you wish to generate licenses. Click **Continue**.
3. To generate your keycode you must either have a numeric authorization code which you would enter in the box opposite **Auth Code**. Or you can search for a Purchase Order by entering a PO and clicking **Go to PO**.
    a. If you use a numeric authorization code, you will need to use the full entitlement associated with the numeric authorization code for the license creation.
    b. If you use a purchase order, you can select the quantity of each line item to include in the license. After clicking **Continue**, you can either specify another PO to take additional features from, or enter Auth Code or click **Go to Summary** to review and produce the keycode license.

    A functioning MDC system must have, at a minimum, phone (asset) and kiosk (station) licenses.
4. Review the summary of your Auth code or PO selections and click **Generate Keycode** to produce a keycode license. This may take 10-20 seconds. You will automatically be taken to the Retrieve Keycode screen.
5. The most current keycode is displayed with a green bar. The summary shows the order/authcode specifics that were last used to create the keycode license. Click **Download Keycode**.
6. Click **Save** on the File Download dialog box.
7. In the **Save As** dialog box, a default filename will be given to the keycode license file. Specify the location where you wish to save the file in the **Save As** dialog box and click **Save**.
8. Click the **Close** button to close the File Download dialog box.

7.6 Copy Keycode File onto MDC Server and Apply Licenses

The following steps will load the keycode licenses onto the MDC Server and make the quantity of features available for use in the licensing server.

1. Log on to the MDC Server as root with a UNIX terminal session. Due to OS security hardening, you may need to login with a non-root username and then switch user privileges to root (e.g. **su – root**).
2. Copy the keycode license file onto the MDC Server using a file transfer utility (such as sftp or winscp). Note: use a userid other than root to transfer the file due to OS hardening security restrictions.
3. As root, copy the keycode license file into the directory **/opt/nortel/ebs/cklt/license**
4. Rename file as **/opt/nortel/ebs/cklt/license/ckltlicense.xml**
5. Execute **service cklt restart** to restart the licensing server. All processes started should have an OK response.
6. Execute **service cklt status** to verify that the licensing server is running. All processes displayed should have a running status.
7. Further steps are needed to update licensing information in MDC application. See Section 7.7 *Update Licensing Information in the* MDC for details.

7.7 Update Licensing Information in the MDC Application

The MDC application will automatically resynchronize licensing information every 5 hours with the license server on the MDC Server. When the keycode license file is updated, the new license information may not appear for up to 5 hours on existing MDC Admin GUI sessions. The following procedures will expedite the resynchronization of the licensing information on the MDC Admin GUI sessions and/or MDC Stations and make the quantity of features available for immediate use.

To expedite the update of the licensing information on MDC Admin GUI:

1. Log completely out of the MDC Admin GUI session and then re-log back in. This will refresh the licensing information and the updated licensing will be displayed in the Assets, Users, Roles and Stations screens.

To expedite the update of the licensing information on the MDC Station:

1. Reboot the MDC Station(s). This will refresh the snapshot of MDC Station licenses and registration will proceed if there are sufficient licenses in the updated licensing information. See Section 13.10 *Reboot MDC Station* or Section 13.11 *Reboot All MDC Stations* for the detailed procedure.

7.8 Other KRS Activities

The following procedures describe other KRS-related activities which may be needed for future administrative tasks.

7.8.1 Register for KRS Access

It may take up to 5 business days to validate registration and provide access to KRS.

1. Open a web browser window.
2. Go to www.nortel.com
3. Under **SUPPORT & TRAINING > ONLINE SELF-SERVICE,** select **Keycode Retrieval**.
4. Click **CUSTOMER REGISTRATION** and follow the instructions.

7.8.2 Retrieve Keycode for MDC System

You can retrieve an existing keycode of an MDC system at any time.

1. Select **Product Control > Retrieve Keycode** from the navigation menu.
2. Enter the site name or part of the site name in the Host Id/Product Id field and click **Search.**
3. The most current keycode is displayed with a green bar. The summary shows the order/authcode specifics that were last used to create the keycode license. Click **Download Keycode**.
4. Click **Save** on the File Download dialog box.
5. In the **Save As** dialog box, a default filename will be given to the keycode license file. Specify the location where you wish to save the file in the **Save As** dialog box and click **Save**.
6. You must copy the keycode license file onto the MDC Server and apply it before the licenses can take effect. Follow the instructions in Section 7.6 *Copy Keycode File onto MDC Server and Apply Licenses* and Section 7.7 *Update Licensing Information in the* MDC.

7.8.3 Generate Try-n-Buy Licenses for MDC System

KRS supports Try-n-Buy licenses for MDC, which allow a 30-day trial of MDC functionality at no cost for a specific MDC Server. The user can create a Try-n-Buy license for each feature only once for a specific MDC server. Unlike the flexibility of purchased licenses, the quantities are fixed for Try-n-Buy licenses for MDC at:

- 2 MDC Stations
- 50 assets (phones)
- 100 location-tracked-enabled users

- Enable roles on all MDC Stations

The user is encouraged to purchase and transfer permanent licenses for MDC prior to the end of the trial period. When applied on an MDC Server, the permanent licenses for a feature will override any Try-n-Buy license for the same feature. If the Try-n-Buy licenses expire at the end of the 30-day period without being replaced by permanent licenses, the MDC data will be maintained but the MDC functionality will stop working.

TIP: A functioning MDC system must have at a minimum phone and kiosk (station) licenses.

1. Select **Product Control > Gen Try N Buy Keycode** from the navigation menu.
2. Enter the site name in the **Site Name** field.
3. From the **Try 'N Buy Feature Package List**, select the Try-n-Buy license you want to add by clicking the line. Multiple licenses can be selected if you hold the Ctrl button while selecting. Click the **Add** button, under the list, to move these licenses into the **Try 'N Buy Feature Package Selected.**
4. Type in the name in the **End User Contact** field.
5. Fill in the **Email Address** field for the End User Contact.
6. Click the **Continue** button.
7. The summary screen will appear. Review the summary and click the **Generate Keycode** button to generate the keycode license. This may take 10-20 seconds.
8. The Retrieve Keycode screen will appear.
9. The most current keycode is displayed with a green bar. The summary shows the quantities of each feature used to create the keycode license. Click **Download Keycode**.
10. A new browser window will appear, displaying the content of the keycode license file in xml. Select **File > Save As** to save the keycode license file on the local computer.
11. In the **Save As** dialog box, a default filename will be given to the keycode license file. Specify the location where you wish to save the file in the **Save As** dialog box and click **Save**.
12. Close the browser window with the keycode license file.
13. Copy the keycode license file onto the MDC Server and apply the licenses to the license server. Follow the instructions in Section 7.6 *Copy Keycode File onto MDC Server and Apply Licenses* for details.
14. Update licensing information for the MDC Admin GUI sessions and MDC Stations for the new licensing information can take effect. See Section 7.7 *Update Licensing Information in the* MDC for details.

7.8.4 Adding More Licenses to MDC System

The process to add more licenses is the same as the process to obtain the initial keycode license file for MDC from KRS described in Section 7.2 *High-Level Overview of Process to Obtain Keycode from KRS*. The differences are:

- In the summary (prior to generating the keycode), the system profile will show how many units are already installed in this system. This information is in the **INSTALLED** column. The sum total of the already installed licenses plus those additional licenses being allocated will be shown in the **NEW TOTAL** column.

  Review the summary to verify that this is the total number of licenses you want to allocate.

- In the retrieve keycode license screen, the current keycode will be displayed in green and the sequence number will have incremented.

  Once this keycode license file has been copied onto the MDC server, all other keycode license files with earlier sequence numbers will be obsolete.

Refer to Section 7.2 *High-Level Overview of Process to Obtain Keycode from KRS* for the steps to add more licenses to the MDC System.

8 Integrate MDC and Location Service

This section provides the steps to enable communications between the MDC Server and a location service. Use this procedure only if location tracking service is being used with MDC.

Integration with two types of location services is supported by MDC:

- SynTrack: The integration permits MDC to inform the SynTrack product as location-tracking-enabled user checkout or return location-trackable assets. The default port for communication with SynTrack is port 443.
- Ekahau: The integration permits MDC to inform the Ekahau product of the name associated with a location-trackable asset as users check out or return assets. The default port for communication with Ekahau is TCP port 8550. The same port is used by the Ekahau Positioning Engine administration web interface.

Note: MDC can only be actively integrated with one location service at a time.

Location tracking is an optional feature on MDC. Location tracking enabled is an attribute of the phone asset and an attribute of the user. Location Tracking can only take effect if the location service has been configured and a location enabled user checks out a location enabled asset. There is a clickable visual indicator on the View Users screen to show when a user is actively being location tracked with a location service. This is also a clickable visual indicator on the View Asset screen to show when a phone is actively being location tracked with a location service.

For further information related to integrating MDC with location services:

- The following sections describe the different options for enabling/disabling location tracking on assets:
  - Section 10.7 *Enable Location Tracking for All Assets*
  - Section 10.8 *Disable Location Tracking for All Assets*
  - Section 10.5 *Update Asset from View Screen*
  - Section 10.6 *Update Asset from Insert/Update Screen*
  - Section 10.2 *Insert New Asset*
- The following sections describe the different options for enabling/disabling location tracking on users:
  - Section 11.6 *Enable Location Tracking for All Users*
  - Section 11.7 *Disable Location Tracking for All*
  - Section 11.4 *Update Users from View Screen*
  - Section 11.5 *Update Users from Insert/Update Screen*
  - Section 11.1 *Insert New Users*
- The following sections describe the visual indicators when location tracking is actively in effect on users and assets:
  - Section 10.3 View Assets
  - Section 11.2 View Users
- A description of licensing related to location services is described in Section 7 *MDC Licensing and Keycode Retrieval System (KRS)*

These are the pre-requisites for enabling location tracking service on MDC:

- The applicable components of Nortel Healthcare Solutions Asset Tracking and Management (ATM) solution are assumed to be installed, configured, and operational per the ATM documentation. The administrator must synchronize SynTrack with EPE to update the zones and tag information. The tag id of the phone assets is its MAC address.
- Each phone asset (handset) must be provisioned to enable Location Service with Ekahau EPE.
- Sufficient EPE licenses must be available to enable tracking of the phone assets (handsets).
- If SynTrack is being used:
    - Each location tracked users in MDC must correspond to a user in SynTrack whose 'SynTrack Alternate IDs' matches the user's 'MDC Barcodes (tag) value'.

8.1 Required Information for Integrating MDC Server and Location Server

The following information is needed to configure connection between the MDC Server and the location service:

- Location service product
- IP address of the Location Server
- Port to communicate with the Location Server
- User name and password to communicate with the Location Server

If using SynTrack for Healthcare for location tracking, the following additional information is needed for the procedure in Section 8.3 *Configuration Required on SynTrack for Healthcare*:

- IP address of SynTrack Admin GUI
- User name and password for SynTrack Admin GUI

8.2 Integrating MDC Server and Location Service

Description:

This procedure describes how to configure connection between the MDC Server and the location service.

TIP: If using SynTrack for Healthcare for location tracking, an additional procedure, Section 8.3 *Configuration Required on SynTrack for Healthcare*, is needed.

Required information:

- Location service product
- IP address of the Location Server
- Port to communicate with the Location Server
- User name and password to communicate with the Location Server

Steps:

1. From the MDC Admin GUI, click the **Network** task on the left navigation menu.
2. The main Network screen will appear.

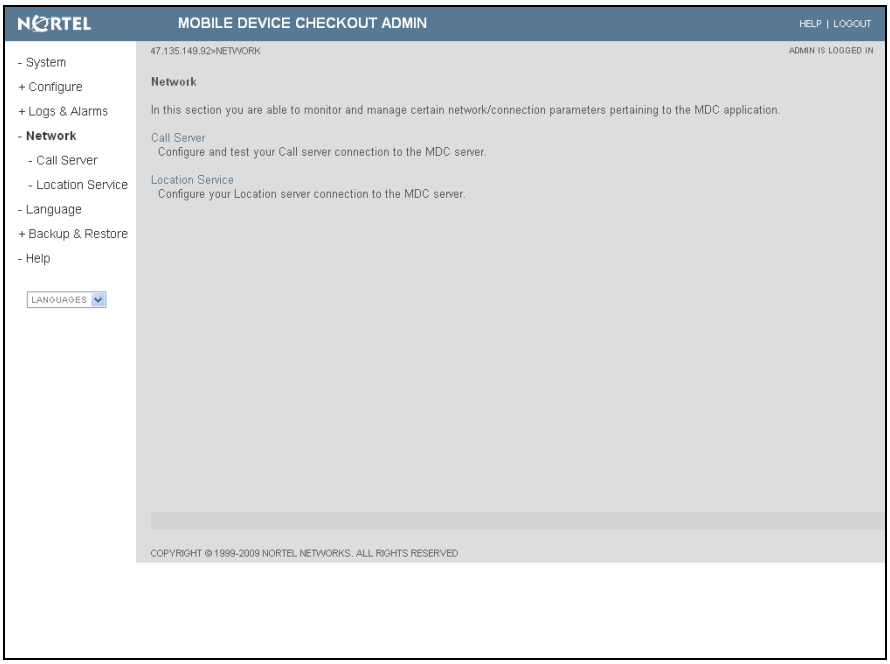


Figure 61: Network Screen on MDC Admin GUI

3. Click **Location Service** from either the main task area or the Network submenu on the left navigation menu.
4. The Location Service configuration screen appears.

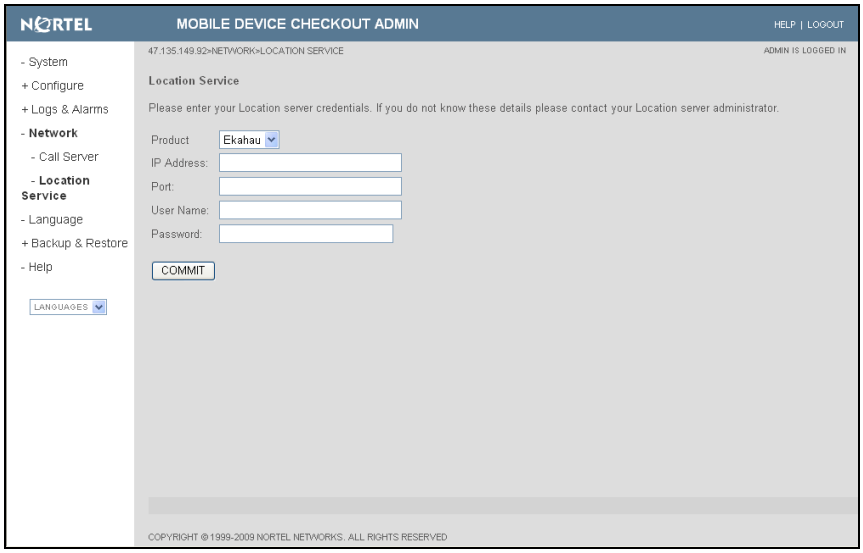


Figure 62: Location Service on MDC Admin GUI

5. To configure communications between the MDC Server and the Location Server, type in the following parameters:

a. **Product**: Select the location service product from the pulldown menu

b. **IP Address**: IP address of the Location Server

c. **Port:** Port number for communication with the Location Server

d. **User Name:** for the MDC application to communicate with the Location Server

e. **Password**: password for the MDC application to communicate with the Location Server

6. Click the **Commit** button to save the location service configuration. As part of saving the configuration, a test of the credential to the location service will be run to ensure that the connection is working. If the test was successful, a successful updated location services properties message should appear.

   If the connection test failed, an error message will be displayed indicating a problem with connecting to the location service. Check the value for the Location Server credentials to make sure they are correct.

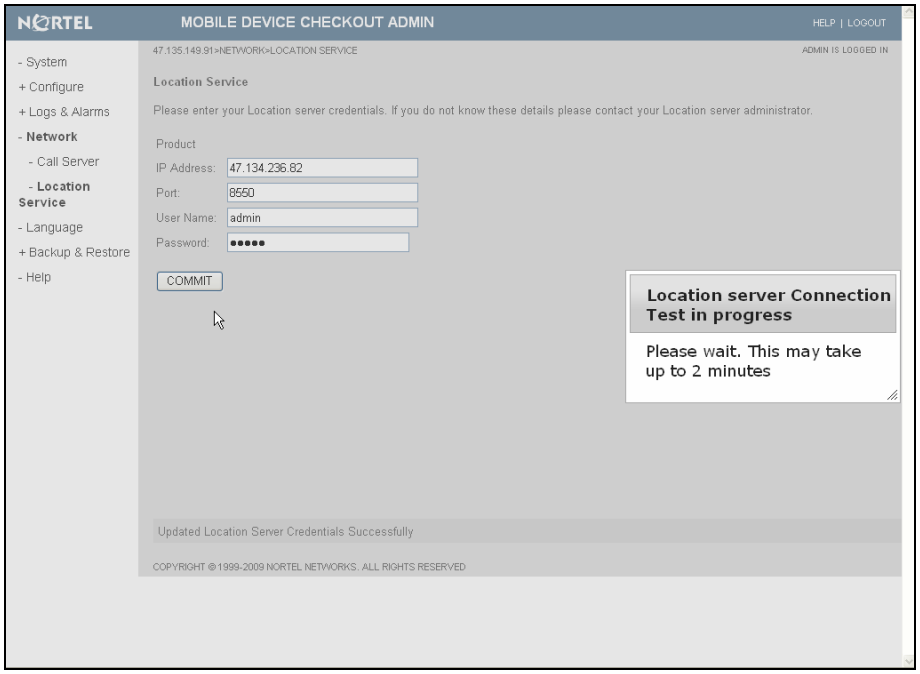


Figure 63: Location Server Connection Test in Progress

8.3 Configuration Required on SynTrack for Healthcare

Description:

The procedure describes the configuration required for MDC on the SynTrack for Healthcare location for MDC location tracking. Use this procedure ONLY when the location service being supported by MDC is SynTrack for Healthcare.

Required information:

- IP address of SynTrack Admin GUI
- User name and password for SynTrack Admin GUI

Steps:

1. Log in to the SynTrack for Healthcare Administration GUI from the MDC Management Station by opening a web browser window and typing in **https://<IP Address of SynTrack Admin GUI>/SynTrack.** A Synapse login window will appear.
    a. Enter the user name.
    b. Enter the password.
    c. Click the **OK** button to log in.

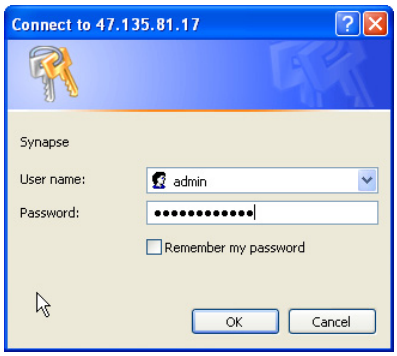


Figure 64: SynTrack for Healthcare Synapse Login Window

2. The SynTrack for Healthcare GUI will appear.
3. For ATM Release 2.1: From the task area, click the **Administration.**

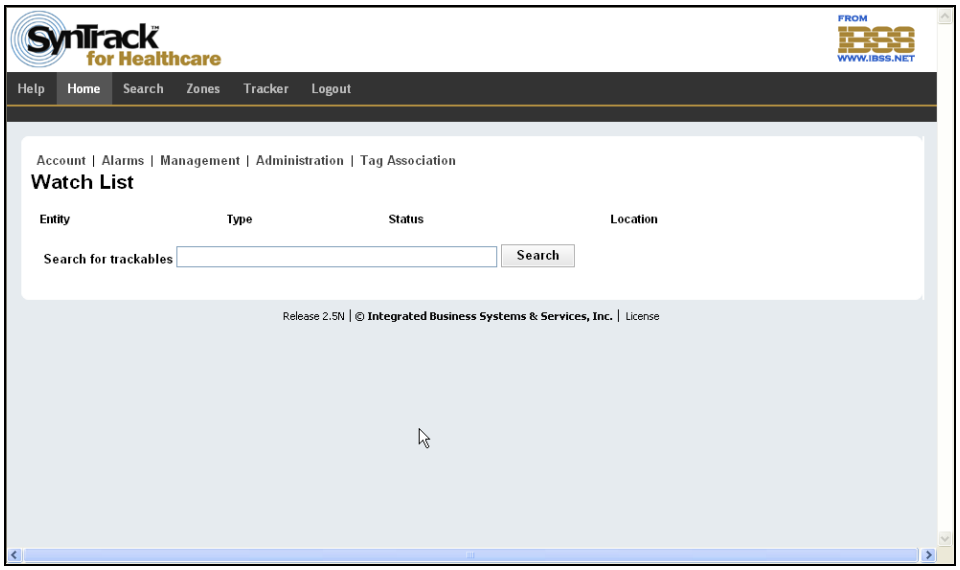


Figure 65: Selecting SynTrack RFID Administration from SynTrack for Healthcare GUI

For earlier releases of ATM: From the title menu Login option, select the **SynTrack RFID Administration** module from the pulldown menu.

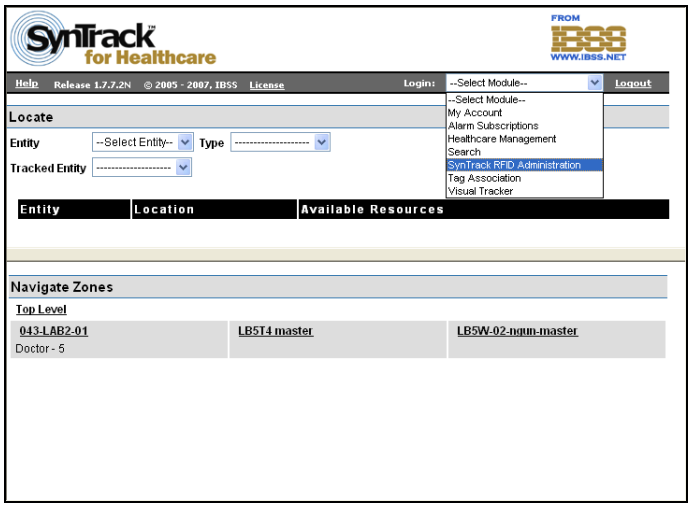


Figure 66: Selecting SynTrack RFID Administration from SynTrack for Healthcare GUI

4. The SynTrack RFID Administration GUI will appear in a new window.

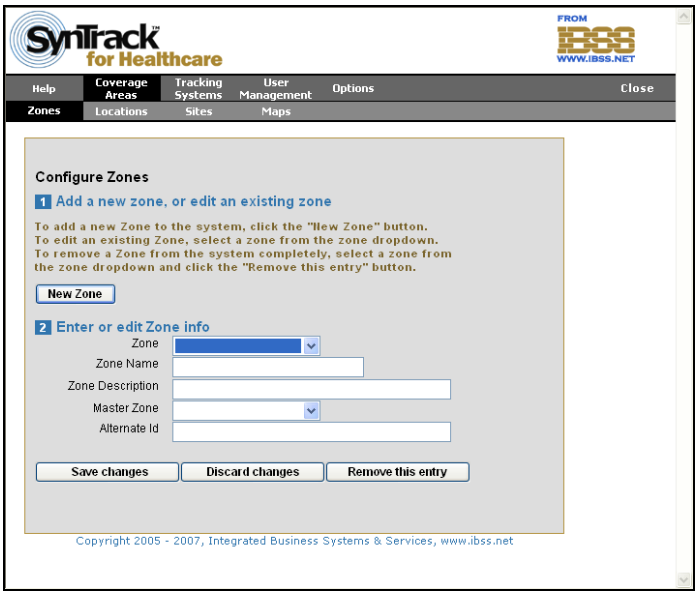


Figure 67: SynTrack RFID Administration GUI

5. From the SynTrack RFID Administration GUI window, click **Tracking Systems** from the title menu.
6. The Tracking Systems will appear in the working area.

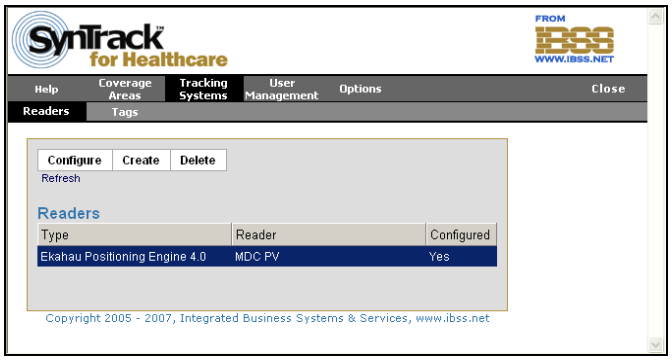


Figure 68: SynTrack RFID Administration GUI

7. Click **Tags** from the working area title menu. A list of configured tags will be displayed.
8. Search for a tag with ID of **NOTAG** in the list. If this tag does not exist, continue with the next step.

   If the NOTAG tag exists, the tag used by MDC to enable the SynTrack location tracking using username has already been configured. You do not have to continue with this procedure. Close the SynTrack RFID Administration Window by clicking **Close** on the title menu bar. Click **Logout** on the SynTrack for Healthcare GUI title menu bar or close this browser window.
9. Click **Create** from the working area.

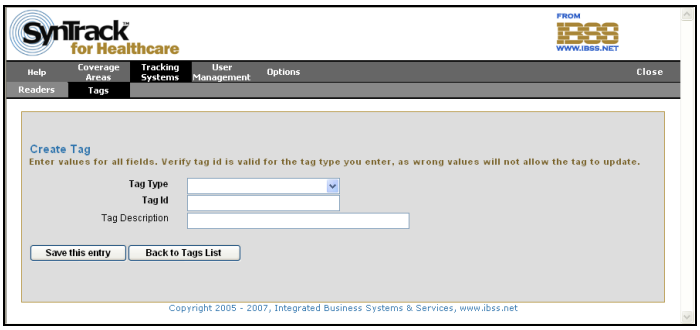


Figure 69: Create Tag on SynTrack RFID Administration GUI

10. Create a tag for use by MDC for location tracking by entering:
    a. Tag Type: Select **Ekahau 301 tag** from the pulldown menu.
    b. Tag Id: Type **NOTAG** in the text field.
    c. Tag Description: Type **Tag for Mobile Device Checkout**.
    d. Click the **Save this entry** button.
11. The Tags screen will appear. Confirm that the NOTAG tag appears in the list of tags configured.

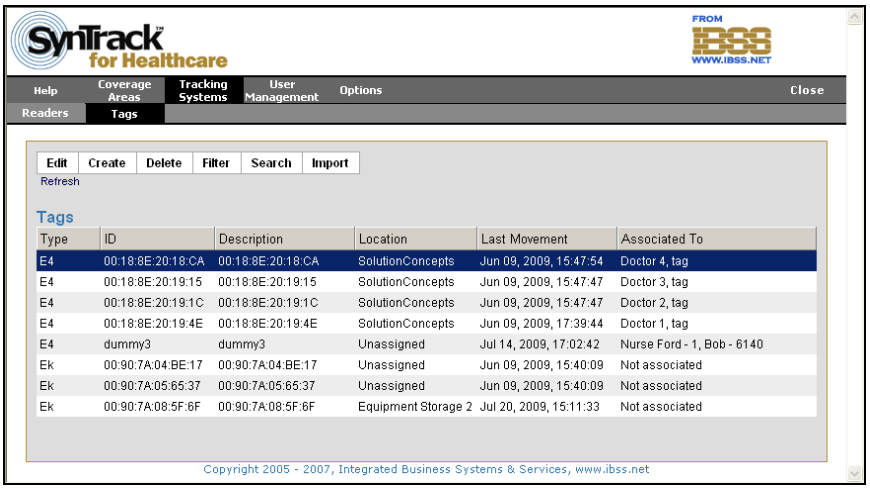


Figure 70: Tags screen on SynTrack RFID Administration GUI

12. Close the SynTrack RFID Administration Window by clicking **Close** on the title menu bar.
13. Close the web browser window for the SynTrack Healthcare GUI. If you click **Logout** on the SynTrack for Healthcare GUI title menu bar, a dialog will appear instructing you to close the SynTrack window and all other open web browser windows in order to log out.

9 Integrating MDC Server and Call Server

This section provides the required integration steps to enable communications between the MDC Server and the call server. This communication is used by the MDC application to configure phone information on the call server when a phone is checked out by a user or when a phone is returned by a user.

There are two types of call server supported: Communication Server 1000 (CS 1000) and Communication Server 2100 (CS 2100). A MDC Server can only be connected to one call server. Use the procedure appropriate for the call server being integrated:

- Configure and Test Connection to CS 1000 from MDC Server
- Configure and Test Connection to CS 2100 from MDC Server

Information on the configuration steps on the call server is contained in the document NN49010-102 Nortel Healthcare Solutions MDC Customer Preparation Guide.

9.1 Configure and Test Connection to CS 1000 from MDC Server

Description:

This procedure describes the steps to enable communications between the MDC Server and the CS 1000 via the E-LAN. This communication is used by the MDC application to configure phone information on CS 1000 when a phone is checked out by a user or when a phone is returned by a user.

For information on the configuration steps on the CS 1000 for MDC is contained in the document NN49010-102 Nortel Healthcare Solutions MDC Customer Preparation Guide.

WARNING: The procedure requires a restart of the MDC application. This action is service affecting.

WARNING: The line number selection for personal phone number and role phone number assignments will only take effect if the role feature is licensed on the MDC Server and there are two numbers are being assigned to the phone during checkout. Otherwise if only a single phone number is being assigned to the phone during checkout (i.e. either the role phone number or the personal phone number) it will always be assigned to the primary key on the phone. For more information on roles and role templates, refer to Section 12 *Managing Roles*.

Required information:

- Release version of CS 1000
- IP address of CS 1000 Call Server on E-LAN
- Username and password for limited access user account for MDC to use
- Customer number for phones and users
- Rlogin Session Timeout (the inactivity timeout for passwords on CS 1000)
- Line number on phone for user personal phone number assignment. Only required if roles are licensed.
- Line number on phone for role phone number assignment. Only required if roles are licensed.
- Line Mode (MCR or SCR) for all the phones, users (and roles if applicable) on this call server
- Whether phones should be disabled (from making calls) when they are returned
- IP address of MDC Server
- Root password for MDC Server (Due to OS security hardening, you may need to login with a non-root username and then switch user privileges to root (e.g. **su – root**))
- Non-root username and password for MDC Server

The fields for configuring line number for user personal phone number assignment and role phone number assignments are related to roles and these fields are only displayed if roles are licensed on the MDC Server.

Steps:

1. From the MDC Admin GUI, click the **Network** task on the left navigation menu.
2. The main Network screen will appear.



Figure 71: Network Screen on MDC Admin GUI

3. Click **Call Server** from either the main task area or the Network submenu on the left navigation menu.
4. The Call Server configuration screen appears. If there has been a committed call server configuration, it will be shown on the screen.

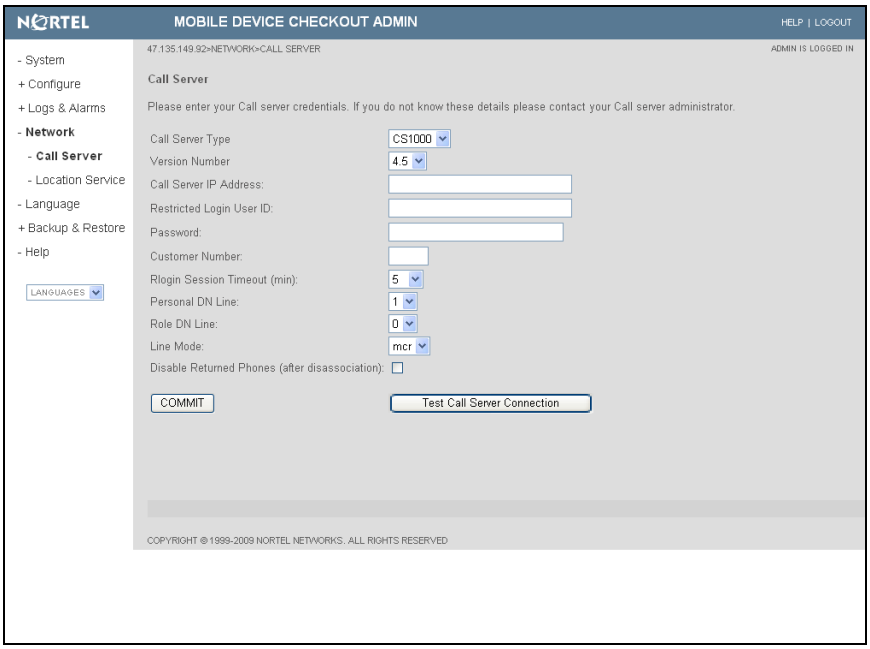


Figure 72: Default Call Server Screen (with Roles) on MDC Admin GUI

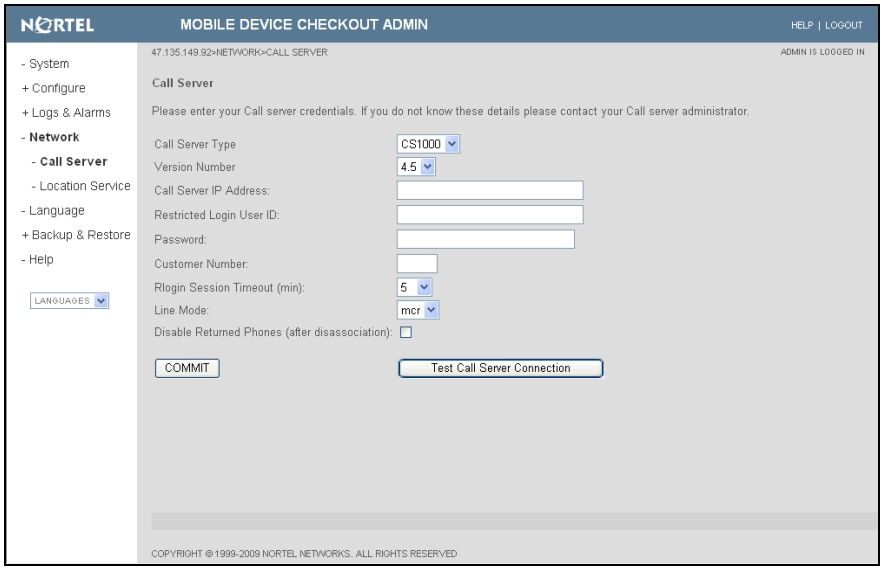


Figure 73: Default Call Server Screen (without Roles) on MDC Admin GUI

5. To configure remote login communications between the MDC Server and CS 1000 Server, select **CS1000** from the pulldown menu for the Call Server Type field.
6. Type in the following parameters:
    a. **Version Number**: Select the software release version of CS 1000 from the pulldown menu. Releases 4.5, 5.0, 5.5 and 6.0 are supported options.
    b. **Call Server IP Address**: IP address of the CS 1000 Call Server on E-LAN.
    c. **Restricted Login User ID:** for the MDC application to remotely log in to CS 1000 Call Server.

d. **Password**: password MDC application to remotely log in to CS 1000 Call Server.

e. **Customer Number:** the customer number in CS 1000 for the users and assets on the MDC.

f. **Rlogin Session Timeout (min):** this value has to be equal to the Inactivity Timeout for passwords in CS 1000.

g. **Personal DN Line**: Select from the pulldown menu which line number on the phone will be assigned the user's phone number when both Role DN and Personal DN are being assigned to a phone during checkout. Selecting a line number for the Personal DN Line will toggle the value of the Role DN Line as these two fields cannot be the same value.

   Note: If only one phone number is being assigned during checkout (either Personal DN or Role DN), this phone number will always be assigned to the primary line on the phone.

   This field only appears when roles are licensed on the MDC.

h. **Role DN Line**: Select from the pulldown menu which line number on the phone will be assigned the role phone number when both Role DN and Personal DN are being assigned to a phone during checkout. Roles are an optional MDC feature which is controlled by licensing. Selecting a line number for the Role DN Line will toggle the value of the Personal DN Line as these two fields cannot be the same value.

   Note: If only one phone number is being assigned during checkout (either Personal DN or Role DN), this phone number will always be assigned to the primary line on the phone.

   This field only appears when roles are licensed on the MDC.

i. **Line Mode**: Select either Multiple Call Ringing (MCR) or Single Call Ringing (SCR) to indicate the call arrangement type for all the phones, users (and roles) used on this call server. This setting must match how these items are provisioned on the call server.

   SCR permits only a single active call on a phone number. MCR permits additional calls on a phone number even when there is already an active call on that phone number. In the case of MCR, if a second call is made to the phone number, the other unused phones will ring. The line mode is important when there are multiple phones with the same phone number. Multiple phones may be assigned the same phone number when the user has permanent phone in addition to their mobile phone. Multiple phones may be assigned the same phone number when roles are being used.

j. **Disable Return Phones** (after disassociation): Check this box if you want the telephony features (i.e. ability to make phone calls) of the phone to be disabled while the phone is not assigned to a user.

7. Click the **Test Call Server Connection** button to test the credentials and connectivity to CS 1000. You will see a warning message of call server connection test in progress.

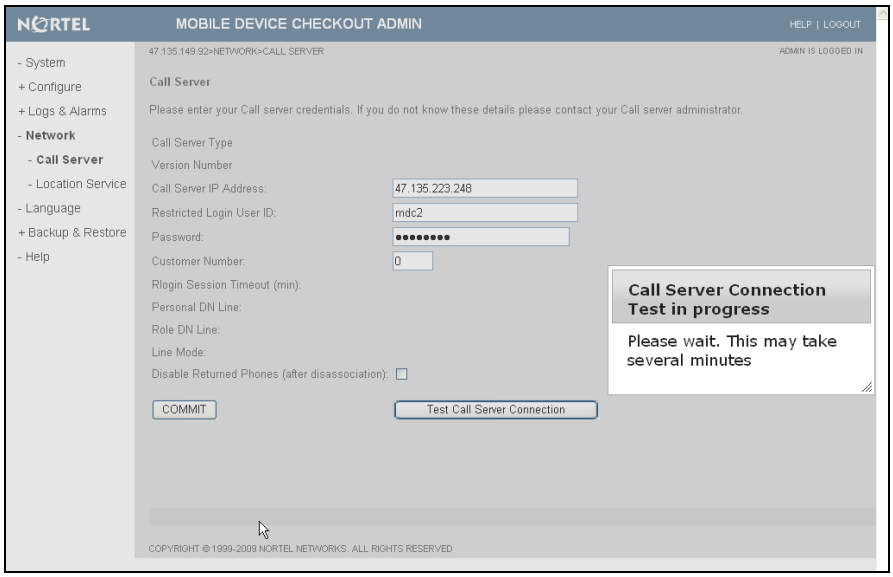


Figure 74: CS 1000 Connection Test in Progress on MDC Admin GUI

8. A successful connection test result message should appear.

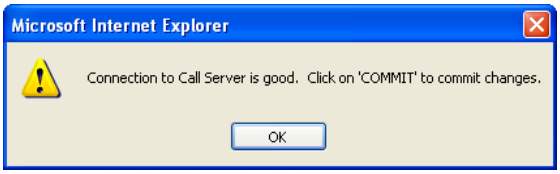


Figure 75: Successful Call Server Connection Test on MDC Admin GUI

9. Click the **Commit** button to save the CS 1000 configuration. This will automatically initiate another call Server connection test.
10. A successful connection test result message should appear.

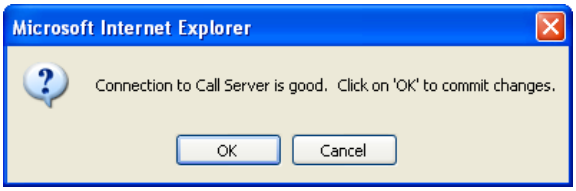


Figure 76: Confirm Call Server Commit on MDC Admin GUI

11. Click the **OK** button to commit changes.
12. A dialog will appear requesting the user to restart the MDC application by executing **service mdc restart** in a UNIX terminal session on the MDC Server. This is necessary to activate the new CS 1000 configuration changes. Click the **OK** button to acknowledge the dialog.

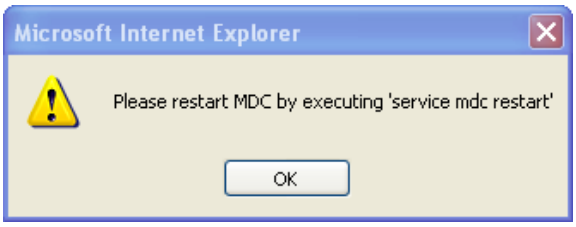


Figure 77: Dialog requesting restarting MDC application to activate CS 1000 Configuration changes

13. A successful response message should appear in the task area.
14. Log on to the MDC Server as root with a UNIX terminal session. (Due to OS security hardening, you may need to login with a non-root username and then switch user privileges to root (e.g. **su – root**))
15. Type **service mdc restart**
16. The MDC processes will be restarted. Type **service mdc status** to verify that all the MDC processes are running.

You have completed configuring and testing the CS 1000 network connection.

9.2 Configure and Test Connection to CS 2100 from MDC Server

Description:

This procedure describes the steps to enable communications between the MDC Server and the CS 2100 Call Server. MDC will interface with CS 2100 Call Server using SERVORD via the OSS Gateway on the Packet Telephony Manager (PTM) Server. This communication is used by the MDC application to configure phone information on CS 2100 when a phone is checked out by a user or when a phone is returned by a user.

For information on the configuration steps on the CS 2100 for MDC is contained in the document NN49010-102 Nortel Healthcare Solutions MDC Customer Preparation Guide.

IMPORTANT NOTE: With CS 2100, the mobile phones deployed for MDC must be in RSUS state (Request for service suspension) for their default DN. The **Disable Return Phones** must be selected when configuring the connection between MDC and CS 2100 call server on the MDC Admin GUI. After successfully checking out a phone, the users must check for dial tone by pressing their off hook key. For situations when both role and user phone numbers are assigned, the user should press the Line button (and select appropriate line 1 or 2) and verify that dial tone is available on both lines. It can take up to 3.5 minutes after checkout before the dial tone is available. If dial tone is not audible after 3.5 minutes, try to check out the phone again.

WARNING: The procedure requires a restart of the MDC application. This action is service affecting.

WARNING: The line number selection for personal phone number and role phone number assignments will only take effect if the role feature is licensed on the MDC Server and there are two numbers are being assigned to the phone during checkout. Otherwise if only a single phone number is being assigned to the phone during checkout (i.e. either the role phone number or the personal phone number) it will always assign to the primary key on the phone. For more information on roles and role templates, refer to Section 12 *Managing Roles*.

Required information:

- IP address of CS 2100 Packet Telephony Manager (PTM) Server to access OSS Gateway
- Port number of CS 2100 OSS Gateway on PTM Server
- Username and password for restricted login user account for MDC to access CS 2100 OSS Gateway

- LATA (Local Access and Transport Area)
- Network Class of Service
- Customer Group
- Customer Sub Group
- Line number on phone for user personal phone number assignment. Only required if roles are licensed.
- Line number on phone for role phone number assignment. Only required if roles are licensed.
- Line Mode (MCA or SCA) for all the users (and roles if applicable) on this call server. For CS 2100, the default DN on phone must always be a single DN (i.e. not multiple-appearance DNs).
- Whether phones should be disabled (from making calls) when they are returned. For CS 2100 call server disabling returned phone must always be selected.
- IP address of MDC Server
- Root password for MDC Server. (Due to OS security hardening, you may need to login with a non-root username and then switch user privileges to root (e.g. **su – root**))
- Non-root username and password for MDC Server

The fields for configuring line number for user personal phone number assignment and role phone number assignments are related to roles and these fields are only displayed if roles are licensed on the MDC Server.

Steps:

1. From the MDC Admin GUI, click the **Network** task on the left navigation menu.
2. The main Network screen will appear.



Figure 78: Network Screen on MDC Admin GUI

3. Click **Call Server** from either the main task area or the Network submenu on the left navigation menu.

4. The Call Server configuration screen appears. If there has been a committed call server configuration, it will be shown on the screen.
5. To configure remote login communications between the MDC Server and CS 2100 Server, select **CS2100** from the pulldown menu for the Call Server Type field.

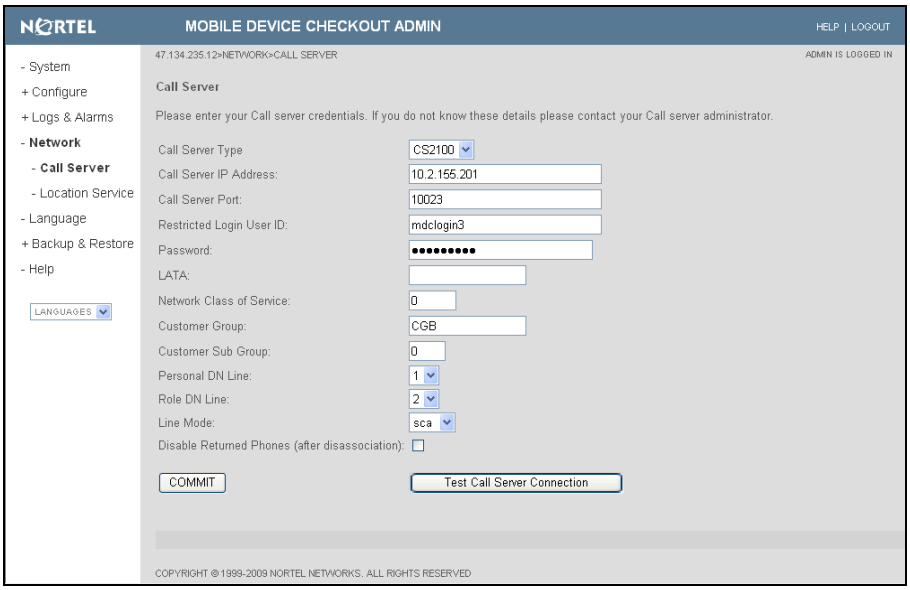


Figure 79: CS 2100 Call Server Screen (with Roles) on MDC Admin GUI

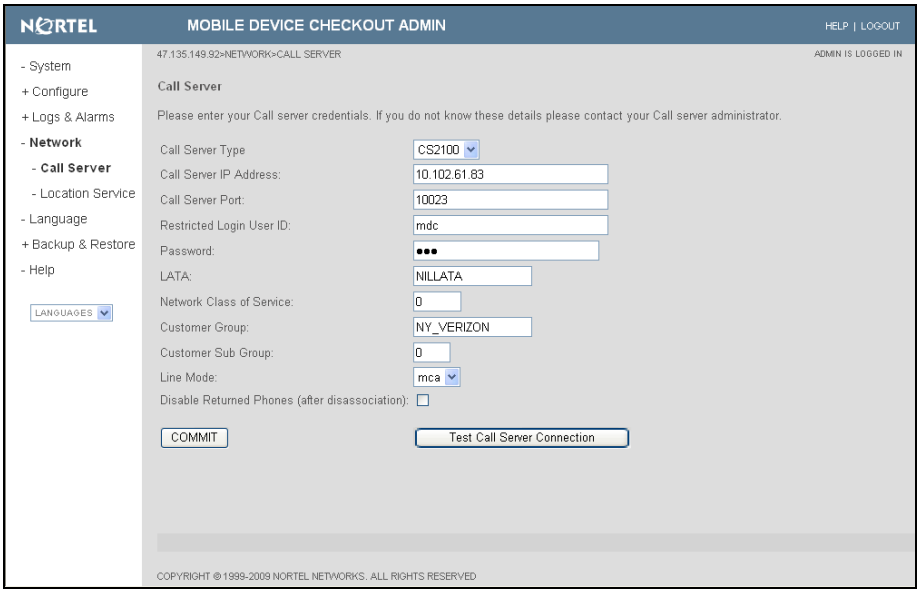


Figure 80: CS 2100 Call Server Screen (without Roles) on MDC Admin GUI

6. Type in the following parameters:
    a. **Call Server IP Address**: IP address of CS 2100 Packet Telephony Manager (PTM) Server to access OSS Gateway

b. **Call Server Port**: Port number of CS 2100 OSS Gateway on PTM Server

c. **Restricted Login User ID: Username** for the MDC application to log in to CS 2100 OSS Gateway.

d. **Password**: Password MDC application to log in to CS 2100 OSS Gateway.

e. **LATA:** Local Access and Transport Area. Leave this field blank if the CS 2100 has been not been configured to use LATA in SERVORD (i.e. EA_LATANAME_IN_SERVORD set to N). Otherwise if CS 2100 has been configured to use LATA in SERVORD (i.e. EA_LATANAME_IN_SERVORD is set to Y), enter the LATA name or use NILLATA if it does not apply. The EA_LATANAME_IN SERVORD parameter can be found in table OFCOPT.

f. **Network Class of Service**: numeric value representing Network Class of Service

g. **Customer Group:** Customer group for the phones and users on the MDC.

h. **Customer Sub Group**: Customer subgroup for the phones and users on the MDC.

i. **Personal DN Line**: Select from the pulldown menu which line number on the phone will be assigned the user's phone number when both Role DN and Personal DN are being assigned to a phone during checkout. Selecting a line number for the Personal DN Line will toggle the value of the Role DN Line as these two fields cannot be the same value.

   Note: If only one phone number is being assigned during checkout (either Personal DN or Role DN), this phone number will always be assigned to the primary line on the phone.

   This field only appears when roles are licensed on the MDC.

j. **Role DN Line**: Select from the pulldown menu which line number on the phone will be assigned the role phone number when both Role DN and Personal DN are being assigned to a phone during checkout. Roles are an optional MDC feature which is controlled by licensing. Selecting a line number for the Role DN Line will toggle the value of the Personal DN Line as these two fields cannot be the same value.

   Note: If only one phone number is being assigned during checkout (either Personal DN or Role DN), this phone number will always be assigned to the primary line on the phone.

   This field only appears when roles are licensed on the MDC.

k. **Line Mode**: Select either Multiple Call Arrangement (MCA) or Single Call Arrangement (SCA) to indicate the call arrangement type for all users (and roles if applicable) used on this call server. This setting must match how these items are provisioned on the call server.

   SCA permits only a single active call on a phone number. MCA permits additional calls on a phone number even when there is already an active call on that phone number. In the case of MCA, if a second call is made to the phone number, the other unused phones will ring. The line mode is important when there are multiple phones with the same phone number. Multiple phones may be assigned the same phone number when the user has permanent phone in addition to their mobile phone. Multiple phones may be assigned the same phone number when roles are being used.

   Note: On CS 2100, the default DN of an asset phone used by MDC must always be a single DN (i.e. not multiple-appearance DNs).

l. **Disable Return Phones** (after disassociation): Check this box. For CS 2100, the telephony features (i.e. ability to make phone calls) of the phone must be disabled while the phone is not assigned to a user.

7. Click the **Test Call Server Connection** button to test the credentials and connectivity to CS 2100. You will see a warning message of call server connection test in progress.

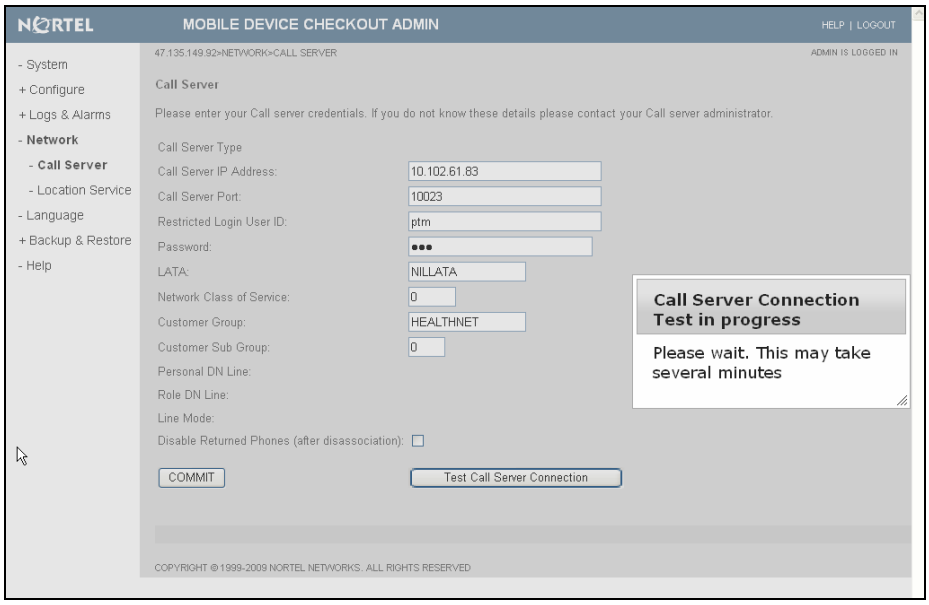


Figure 81: CS 2100 Connection Test in Progress (with Roles) on MDC Admin GUI

8. A successful connection test result message should appear.

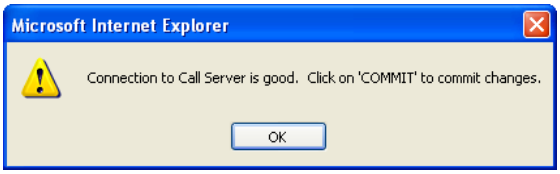


Figure 82: Successful Call Server Connection Test on MDC Admin GUI

9. Click the **Commit** button to save the CS 2100 configuration. This will automatically initiate another call Server connection test.
10. A successful connection test result message should appear.

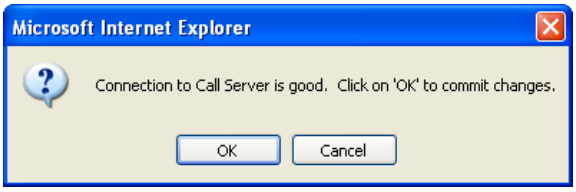


Figure 83: Confirm Call Server Commit on MDC Admin GUI

11. Click the **OK** button to commit changes.
12. A dialog will appear requesting the user to restart the MDC application by executing **service mdc restart** in a UNIX terminal session on the MDC Server. This is necessary to activate the new CS 2100 configuration changes. Click the **OK** button to acknowledge the dialog.

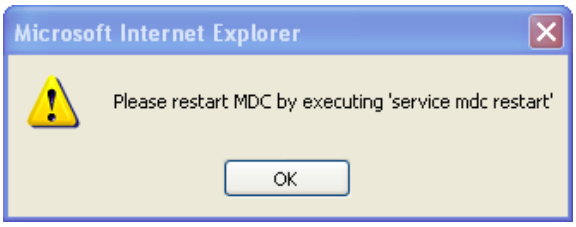


Figure 84: Dialog requesting restarting MDC application to activate CS 2100 Configuration changes

13. A successful response message should appear in the task area.
14. Log on to the MDC Server as root with a UNIX terminal session. (Due to OS security hardening, you may need to login with a non-root username and then switch user privileges to root (e.g. **su – root**))
15. Type **service mdc restart**
16. The MDC processes will be restarted. Type **service mdc status** to verify that all the MDC processes are running.

You have completed configuring and testing the CS 2100 network connection.

10 Managing Assets (Phones)

The number of assets permitted on an MDC is controlled by license. At the bottom of the assets screens, a running tally of the total number of licensed assets permitted, along with the number of licensed assets in use, is displayed. It is possible for an error message to appear indicating that there is no license file OR a warning message that all licenses for assets have been used. When the license file is updated, new license information may not appear for up to 5 hours on existing MDC Admin GUI sessions. However, the user may choose to manually refresh the licensing information. Refer to Section 7 *MDC Licensing and Keycode Retrieval System (KRS)* for more information on MDC licensing.

The phone asset should have a barcode label attached physically on the back of the phone or inside the battery compartment if using protective silicon covers (e.g. zCovers) on the WLAN handsets. Refer to *Figure 14: Barcode Placed in Battery Compartment when Protective Cover used on WLAN Handset* 6140 for a diagram. The barcode is used to identify the phone asset. If needed, refer to the document NN49010-501 Nortel Healthcare Solutions MDC Deployment Guide for more information on creating barcode labels.

When roles are not licensed:

- If a phone asset is checked out, a clickable icon will appear in the owner field to provide details of the user who has checked out the phone.
- If the phone asset is used while checked out (i.e. assigned) to a user, the calling phone number associated with the phone will be the phone number of that user, as displayed in the Current DN field. Any phone calls to the default DN of this phone asset will not connect.
- When the asset is returned by the user, the owner icon field will be blanked, and the Current DN field will be blanked. When the phone is used while not assigned to a user, the calling phone number associated with the asset will be the default DN.

See Section 12 *Managing Roles* for a description of roles and how roles can change the phone numbers assigned to the phone when it is checked out.

The MDC interface to the call server should be provisioned prior to provisioning assets. See Section 9 Integrating MDC Server and Call Server for further details.

The following information about the pool of phones must be specified:

- Role DN and Personal DN line assignment: Allows the administrator to specify the phone line used for Role DN and Personal DN when two DNs are assigned during phone checkout. Note: If only one phone number is being assigned during checkout (either Personal DN or Role DN), this phone number will always be assigned to the primary line on the phone.
- Line mode: Specified whether multiple active calls can be made to a DN which may be assigned to multiple phones. This setting must match how the call server has been provisioned.
- Disable Return Phones (after disassociation): Whether the telephony features (i.e. ability to make phone calls) of the phone are disabled while the phone is not assigned to a user.

See Section 9 *Integrating MDC Server and Call Server* for instructions on how to specify the above information.

Location tracking enabled is an attribute of the asset and an attribute of the user. The owner icon is colored green with a T for location tracked only when both the asset and the user have location tracking enabled **at the assignment time** when the user checks out the asset.

There are three scenarios when a location-tracking-enabled user may have an asset checked out but the phone icon does not indicate location tracking:

1. The user has checked out an asset which is not configured to support location tracking.
2. The user had their location-tracking-enabled status changed while they already had an asset checked out. The location tracking will not take effect until the next time the user checks out an asset. The phone icon associated with the user will remain a gray non-tracked phone icon to indicate the user is not currently being location tracked.

3. Both the user and the asset had location tracking enabled when the user checked out the asset. Normally, the phone icon will be a green tracked (T) phone icon. However, if there was a communication error with the Location Server at the time the user checked out the asset, MDC will be unable to confirm that the user is being location tracked. The user will be informed at the MDC Station that they are not being tracked. The asset will be checked out but the phone icon associated with the user will be a gray non-tracked phone icon to indicate that the user is not currently being location tracked.

Note: When location tracking is enabled on assets, there must also be sufficient licenses available on the Ekahau location service to enable location tracking of these assets. Also, the location tracking feature must also be manually enabled on the physical phones. See Section 8 *Integrate MDC and Location Service* for more information on enabling location services.

WARNING: Asset information on the MDC Admin GUI must exactly match the phone configuration on the call server and must remain synchronized. Any mismatch of information will impair service. If changes have been made to the call server, update the associated phones in MDC.

The procedures in this section are:

- Terminal Number Format based on Call Server
- Insert New Asset
- View Assets
- View Owner of Assets
- Update Asset from View Screen
- Update Asset from Insert/Update Screen
- Enable Location Tracking for All Assets
- Disable Location Tracking for All Assets
- Delete Asset
- Bulk loading of Assets

10.1 Terminal Number Format based on Call Server

A terminal number (TN) for a phone must have a specific format which is dependent on the call server being used. See Section 9 *Integrating MDC Server and Call Server* for more information on determining the call server being used with MDC.

10.1.1 Terminal Number Format for CS 1000

For phone on CS 1000 call server, the TN format is **<loop> <shelf> <card> <unit>** where:

- **<loop>** is the loop number with a value from 0 to 252 in increments of 4 (i.e. 0, 4, 8, 12 … 248, 252) and represented by up to three digits. A single or double digit number may have leading zeros. For example, the number eight may be shown as 8, 08 or 008.
- **<shelf>** is the shelf number and is either 0 or 1.
- **<card>** is the card number with a value from 1-4 or 7-10 and is represented by up to two digits number. A single digit number may have a leading zero. For example, the number eight may be shown as 8 or 08.
- **<unit>** is the unit number with a value from 0 to 31 and is represented by up to two digit number. A single digit number may have a leading zero. For example, the number eight may be shown as 8 or 08.

These are some examples of correctly formatted CS 1000 TNs: 156 0 05 20, 104 1 00 00 and 120 0 1 1.

10.1.2 Terminal Number Format for CS 2100

For phones on CS 2100 call server, the TN is the line equipment number (LEN). The format is **<site> <frame> <group> <upper circuit> <lower circuit>** where:

- **<site>** is a string defined in table SITE (typically **CICM** but can be any string of up to 16 characters)
- **<frame>** is a number with a value from 0 to 511 and represented by up to three digits. Leading zeros may be used for single or double digit numbers. For example, the number eight may be shown as 8, 08, or 008.
- **<group>** is a number from 0 to 2.
- **<upper circuit>** is a number with a value from 0 to 10 and represented by up to two digits. A single digit number may have a leading zero. For example, the number eight may be shown as 8 or 08.
- **<lower circuit>** is a number with value from 0 to 99 (or 0 to 22 if upper circuit is 10 since a CICM node can only have up to 1023 terminals) and represented by up to two digits. A single digit number may have a leading zero. For example, the number eight may be shown as 8 or 08

Note: The site, frame and group represent the node and must be provisioned in table LGRPINV to be valid.

These are some examples of correctly formatted CS 2100 LENs: CICM 001 2 08 81, CICM 1 2 8 81 or CICM 2 2 10 21.

10.2 Insert New Asset

Description:

This procedure describes adding a new asset to MDC.

WARNING: The phone must already be provisioned AND functional (i.e. working) on the call server.

WARNING: With CS 1000 call servers, when adding a phone asset, the phone MUST be powered on, and, able to make and receive calls. This allows the MDC to retrieve the phone asset information from the call server to ensure synchronization of data. The phone can be powered off once it has been added through the MDC Admin GUI.

Note: For CS 2100 call servers, the specified Default DN must be the full 10 digit DN, even if extension dialing is supported.

The number of assets permitted on MDC is controlled by license. Ensure that you have sufficient licenses for assets. If the licensing information has changed within the last 5 hours, you may need to manually refresh the licensing information using the procedure described in Section 7.7 *Update Licensing Information in the* MDC

If enabling location tracking on the phone assets, you must ensure that:

- MAC address for the phone asset is configured
- The location tracking feature is also manually enabled on the physical phones and configured for the Ekahau location service.
- There are sufficient licenses on the Ekahau location service to support location tracking for these phones.

Note: This procedure is for adding individual handsets. For a large number of handsets, Nortel provides a bulk-load capability, described in Section 10.10 *Bulk loading of Assets*.

WARNING: Asset information on the MDC Admin GUI must exactly match the phone configuration on the call server and must remain synchronized. Any mismatch of information will impair service.

Required information:

For each asset added to MDC:

- Barcode labels of phones
- Tag type
- Default DN
- Phone type
- Terminal number
- MAC address
- Whether the asset is tracking enabled
- [Optional] Brief text description of the asset

If a phone asset is hosted on a CS 1000 call server, the phone asset MUST be powered on and able to make and receive calls while it is being added to the MDC.

A terminal number (TN) has a specific format which is dependent on the call server being used:

- For phone on CS 1000 call server, the TN format is **aaa b cc dd** where aaa = loop number, b = shelf number, cc = card number, and, dd = unit number. These are some examples of correctly formatted CS 1000 TNs: 156 0 05 20, 104 1 00 00 and 120 0 1 1.
- For phone on CS 2100 call server, the TN format is **<site> aaa b cc dd** where <site> = site, aaa = frame number, b = group number, cc = upper circuit number, and, dd = lower circuit number. These are some examples of correctly formatted CS 2100 LENs: CICM 001 2 08 81, CICM 1 2 8 81 or CICM 2 2 10 21.

See Section 10.1 *Terminal Number Format based on Call Server* for a more detailed description of the TN formats.

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Assets** from either the main task area or the Configure submenu on the left navigation menu.
4. The Assets screen appears. The main Assets screen is the View screen, which displays a list of assets in a table format. On a newly installed MDC, there will initially be no assets to display.



Figure 85: View Assets Screen with No Assets

5. Ensure that there is a barcode label stuck physically on the back of the asset being added. Ensure the phone is powered on and able to make and receive calls.

   Note: When using a protective silicon cover on WLAN handsets (e.g. zCovers):

   - The barcode label should be placed inside the battery compartment.
   - If you plan to use a hand held scanner to input the barcode value, wait until after the phone barcode label has been scanned before powering on the phone.

6. Click **Insert/Update Asset** from the Assets main task working area to add an asset to MDC.
7. The Insert/Update Asset screen appears. The Insert/Update Asset screen will look different depending on which call server is integrated with MDC:

   - If the call server is CS 1000, the Insert/Update Asset screen has a Get Phone Information button.
   - If the call server is CS 2100, the Insert/Update Asset screen does not have a Get Phone Information button.

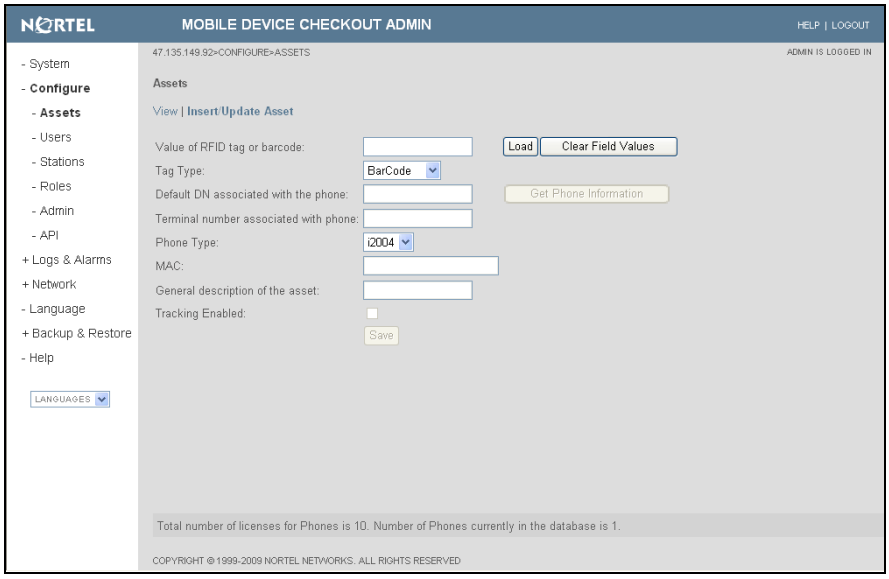


Figure 86: Insert/Update Asset Screen (with Get Phone Information button)

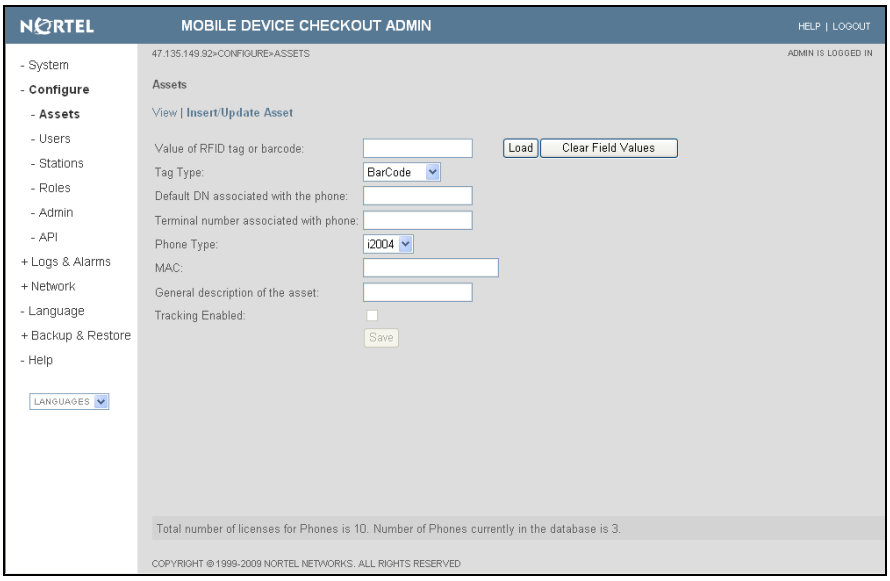


Figure 87: Insert/Update Asset Screen (without Get Phone Information button)

The number of assets permitted on an MDC is controlled by license. It is possible for an error message to appear indicating that there is no license file, OR a warning message that all licenses for phones have been used. Refer to Section 7 *MDC Licensing and Keycode Retrieval System (KRS)* for more information on MDC licensing.

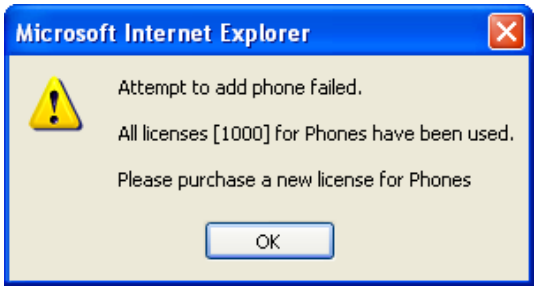


Figure 88: No available license for Asset message

8. To insert a new asset, use the information which should match the information physically on the asset. Enter in the following parameters:
    a. **Value of RFID tag or barcode**: This is the RFID or barcode label associated with the asset. Verify that the information on the asset matches the information for the screen. Choose one of the following two possible methods to enter this information into the MDC:
        - Using the barcode reader:
            - Place the cursor in the text box for Value of RFID tag or barcode.
            - Use the barcode reader to scan the barcode/RFID on the asset. This will read and type the barcode/RFID digits into the text box automatically.
        - Manually read and type barcode/RFID digits into the text box.
    b. **Tag Type**: Select the type of tag from the Tag Type pulldown menu.
    c. Click the **Load** button.
        - For barcodes/tags already provisioned as an asset, this will retrieve the information from the MDC database about this asset and display it on the screen. This is not the expected behavior if a new phone is being added. If this occurs, make sure the barcode of the asset has been entered correctly and all assets have unique barcodes.
        - For barcodes/tags which are not known (i.e. new), a message will appear on the message banner indicating that no phone has been found with the given tag value. This is the expected behavior when a new phone asset is being added. The text fields will become editable to permit the input of the asset information.
        - If this barcode/tag has been assigned to a user, an error message will popup,
9. Execute this step if the phones are on a CS 1000 call server (i.e. the Insert/Update Asset screen has a Get Phone Information button):

    Information should match the information physically on the asset and the configuration on the call server. Note: Manually entering information these MDC Admin GUI fields does not change the call server configuration.

    Ensure the phone is powered on and able to make and receive calls.

    Type in the **Default DN associated with the phone.** This is the directory phone number associated with the asset. Click the **Get Phone Information** button. This will trigger the MDC to retrieve the asset information from the call server.

    - After a few moments, the following retrieved information should be displayed on the screen:
        - Terminal number associated with phone,
        - Phone Type
        - MAC

- Confirm that the Phone Type displayed is the phone type of the phone. Note: The phone type will show as 2210 even if the set is a 6140
- If the MAC address is shown as NON-REGISTERED:
    - For CS 1000 call server, this indicates the handset is either not powered on or it has not been able to complete registration with the call server. The MAC address must be configured for RF location tracked phones. Ensure the handset is powered on and has the ability to make and receive phone calls. Click the **Get Phone Information** button again.

If you have entered an unknown DN or if there was a communication problem, a popup message dialog will appear. Check and correct the **Default DN associated with the phone** if needed. Click **Get Phone Information** again.

If you have the correct DN but communication problems persist between the call server and the MDC, you can manually enter the phone asset information. The information must match the phone configuration on the call server for this DN. Note: Manually entering information into these fields will not change the call server configuration:

- **Terminal number associated with phone**: Terminal Number for the asset on the call server. A terminal number (TN) has a specific format which is dependent on the call server being used.
    - For phone on CS 1000 call server, the TN format is aaa b cc dd where aaa = loop number, b = shelf number, cc = card number, and, dd = unit number.

  See Section 10.1 *Terminal Number Format based on Call Server* for a more detailed description of the TN formats.
- **Phone Type**: select the phone type from the pulldown menu.
- **MAC**: Media Access Control number for asset. The MAC format must be XX:XX:XX:XX:XX:XX where X is a hexadecimal number (0 to 8 and A to F). The MAC address must be configured for RF location tracked phones.

10. Execute this step if the phones are on a CS 2100 call server (i.e. the Insert/Update Asset screen does not have a Get Phone Information button):

    Information should match the information physically on the asset and the configuration on the call server. Note: Manually entering information these MDC Admin GUI fields does not change the call server configuration.

    a. Type in the **Default DN associated with the phone.** This is the directory phone number associated with the asset. For CS 2100, the full 10 digit DN must be specified, even if extension dialing is supported.

    b. Type in the **Terminal number associated with phone** i.e. the Terminal Number for the asset on the call server. A terminal number (TN) has a specific format which is dependent on the call server being used.
        - For phone on CS 2100 call server, the LEN is used for the Terminal Number, The TN format is <site> aaa b cc dd where <site> = site, aaa = frame number, b = group number, cc = upper circuit number, and, dd = lower circuit number.

      See Section 10.1 *Terminal Number Format based on Call Server* for a more detailed description of the TN formats.

    c. Select the **Phone Type** from the pulldown menu.

    d. Type in the **MAC**: Media Access Control number for asset. The MAC format must be XX:XX:XX:XX:XX:XX where X is a hexadecimal number (0 to 8 and A to F). The MAC address must be configured for RF location tracked phones.

11. Type in the **General Description of the asset**. This is a brief text description of the asset.

12. Click the **Tracking Enabled** box if this asset can be RF location tracked. Note: The location tracking feature must also be manually enabled on the physical phones.



Figure 89: Data filled Insert/Update Asset Screen (with Get Phone Information button)

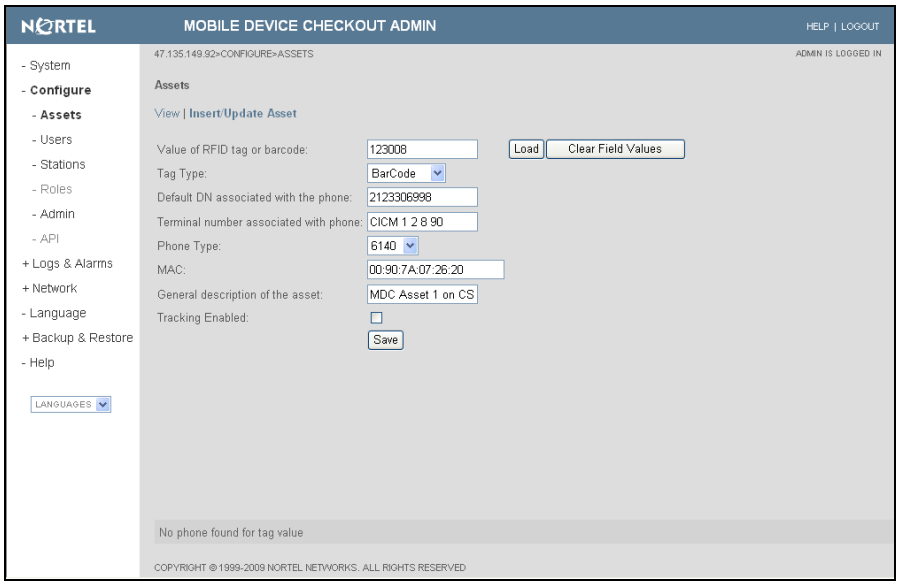


Figure 90: Data filled Insert/Update Asset Screen (without Get Phone Information button)

13. Click **Save** to insert the displayed asset into the MDC database.
14. Ensure that a successfully inserted message is displayed to confirm that the asset was added. The data fields will be blanked to facilitate inserting the next asset. If desired, you can now power off the phone.
15. When you have completed adding all the assets, click **View** from the main task area menu. The main Assets screen is the View screen, which displays a list of assets in a table format. You should see all the assets you have just added to MDC displayed.

16. If the terminal number, phone type or MAC address information had to be manually entered in Step 9, it is recommended to test the newly added phone asset by performing a check out and a return of this phone at an MDC Station. See Section 14.1 *Check out a phone to a user at an MDC Station* and 14.2 *Return a phone at an MDC Station* for the detailed description of these tests. (If this is a location tracked phone, you may wish to use the tests in Section 14.4 *Check out a phone to a location-tracked user* and Section 14.5 *Return a phone assigned to a location tracked user*.) In particular, it is important to confirm the phone number on the handset changes to the user's phone number within 3.5 minutes after a successful phone assignment.

    Once these tests have passed, the phone can be added to the phone pool and made available for general use.

    If the phone number does not change to the user's phone number within 3.5 minutes of a successful phone assignment, perform the check out again. If the problem persists:

    - Return the phone at an MDC Station
    - Confirm that the phone number, terminal number and the MAC address are configured correctly in the MDC Admin GUI for this phone.

    If necessary, correct the phone information in the MDC Admin GUI using the procedure in Section 10.6 *Update Asset from Insert/Update Screen*.

10.3 View Assets

Description:

This procedure describes how to view the list of assets from the MDC Admin GUI.

Required information:

- None

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Assets** from either the main task area or the Configure submenu on the left navigation menu.
4. The Assets screen appears. The main Assets screen is the View screen, which displays a list of assets in a table format. On a newly installed MDC, there will initially be no assets to display.

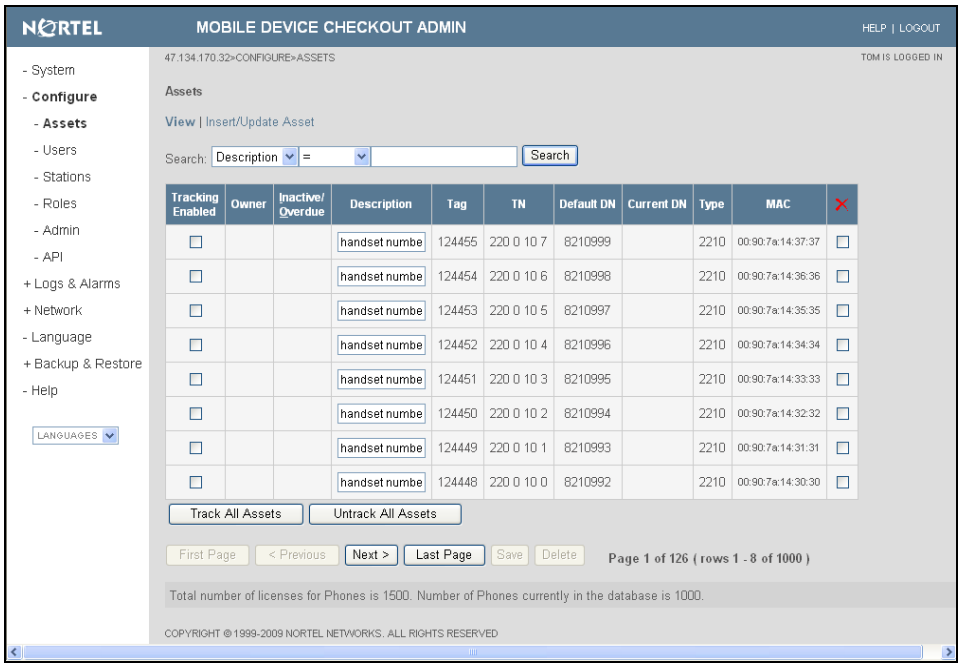


Figure 91: View Assets on MDC Admin GUI

The columns in the asset table are:

- Tracking Enabled: Indicates whether an asset has RF location tracking enabled.
- Owner: Displays a clickable icon when the asset is assigned to a user or is blank if the asset is not assigned.
    - The icon may have an **R** if a role has been assigned to the phone.
    - The icon may be colored green with a **T** if the user is being RF location tracked.
    - The icon may be colored green with a **T** and **R** if the user is being RF location tracked and in addition a role has been assigned to the phone.

  For more information on the owner field, refer to Section 10.4 *View Owner of Assets.*
- Inactive/Overdue: Displays an icon if the asset is either overdue/inactive or is blank if neither situation applies.
    - The icon may be colored red with an **I** if the asset has been inactive (i.e. checked in and unused) too long.
    - The icon may be colored yellow with an **O** if the asset has been overdue (i.e. checked out) too long

  See Section 5.9.6 *Configure Alarms* for more information on configuring the inactive and overdue asset monitoring.
- Description: A text description of the asset.
- Tag: Tag number attached to the asset.
- TN: Terminal Number for the asset on the call server.
- Default DN: Directory number associated with the asset
- Current DN: Directory number of the user who has checked out this asset. If roles are not licensed on the MDC, this is the directory number associated with the asset while it is assigned to

a user. If roles are in use, it is recommended to click the Owner icon to view the directory numbers assigned to the asset. See Section 10.4 *View Owner of Assets* for further details.

- Type: Type of asset. For phones, this will be the phone type.
- MAC: Media Access Control number for asset.
- Delete: This field is checked to delete the asset from MDC.

When there are a large number of assets in the list, only some of the assets will be displayed on the screen at a time. This is considered a "page." The page number is shown on the screen along with the total number of available pages at the bottom of the table to help orient the user within the view asset table. The equivalent row information for these entries in the asset table is also given in parentheses.

There are a number of options to view other assets not displayed on the screen:

- Paging
- Sort
- Search

See Section 5.2.4 *MDC Admin GUI Paging, Sort, and Search* for a description of paging, sorting and searching and an explanation of how to use these features.

10.4 View Owner of Assets

Description:

This procedure describes how to view the owner of an asset on the MDC Admin GUI.

Refer to Section 12 *Managing Roles* for more information on roles. See Section 8.2 *Integrating MDC Server and Location Service* for more information on location tracking.

Required information:

- None

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Assets** from either the main task area or the Configure submenu on the left navigation menu.
4. The Assets screen appears. The main Assets screen is the View screen, which displays a list of assets in a table format. On a newly installed MDC, there will initially be no assets to display.
    a. If this asset has been checked out by a user, a person icon will appear in the Owner field.
        - The person icon may have an **R** if a role has been assigned to the phone.
        - The person icon may be colored green with a **T** to indicate that the user is being RF location tracked.
        - The person icon may be colored green with a **T** and **R** if the user is being RF location tracked and in addition a role has been assigned to the phone.
        - The phone number associated with the user will appear in the Current DN field. If roles are not licensed on the MDC, this is the directory number associated with the asset while it is assigned to a user. If roles are in use, it is recommended to proceed to click the Owner icon to view the directory numbers assigned to the asset.

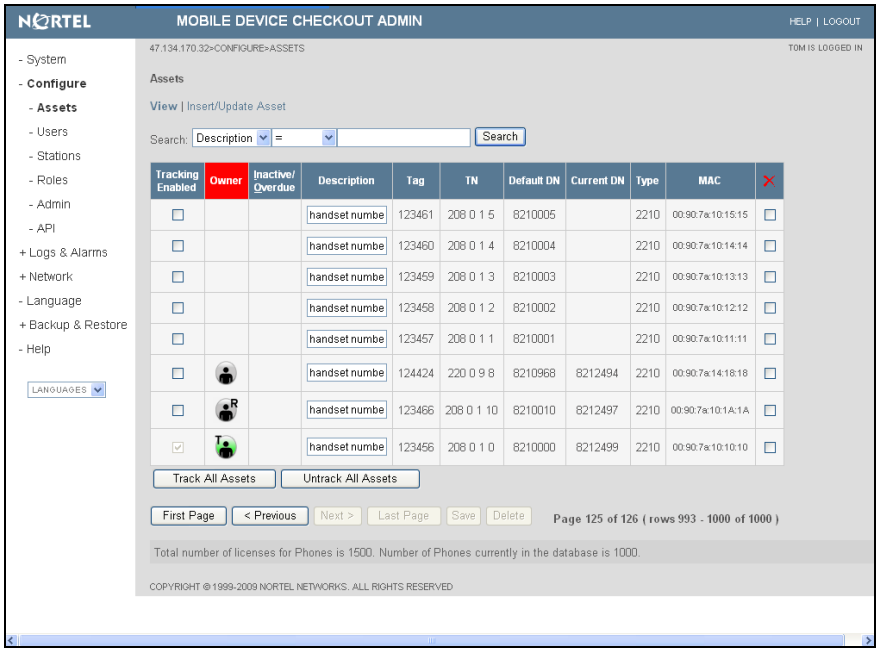


Figure 92: View Asset with Owner Associated

b. Click the **icon** in the Owner field and a popup screen will appear with the details of the user who has checked out this asset.

- Tag Value is the tag number for the asset.
- First Name and Last Name are the name of the user.
- Display Name is the display configured in the call server for the user.
- Personal Number is the phone number associated with the user.
- Personal Number Provisioned on Phone will indicate whether the personal number of the user has been assigned to the asset.
- Role Provisioned on Phone is the name of the role assigned to the phone. This field may be blank if no role has been assigned.
- Role Phone Number is the phone number of the role assigned to the phone. This field may be blank if no role has been assigned.
- Role Phone Number Provisioned on Line will give the phone line number which has been assigned the role phone number.
- Assignment Time shows the time when the user checked out this asset.

If there is only one phone number assigned (either personal phone number or role phone number), this number will always be assigned to the primary key on the phone.

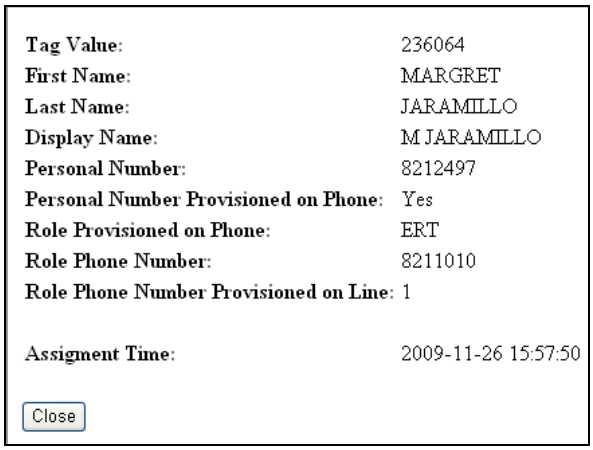


Figure 93: Asset Owner Details with Roles

10.5 Update Asset from View Screen

Description:

This applies to making changes to previously provisioned assets on MDC.

Note: There are limited fields that can be updated from the Asset View screen.

Required information:

- Asset which needs to be updated identified by one of these fields: tag, terminal number, default DN, or MAC address
- Updated information for asset: Description, or Tracking Enabled Status

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Assets** from either the main task area or the Configure submenu on the left navigation menu.
4. The Assets screen appears. The main Assets screen is the View screen, which displays a list of assets in a table format. On a newly installed MDC, there will initially be no assets to display.

   Note: The **Save** button, below the asset table, does not become enabled until there are changes made to entries in the asset table.

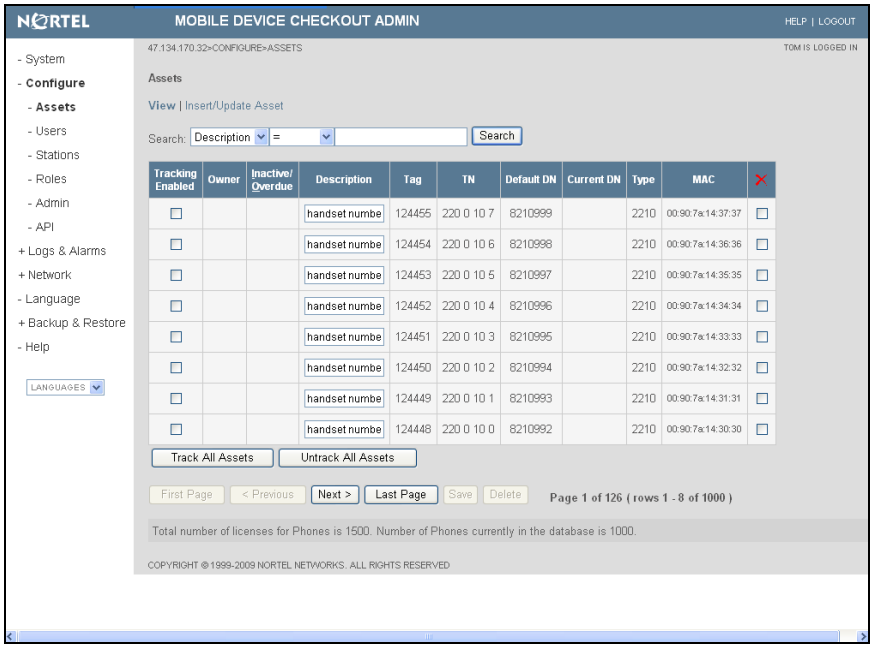


Figure 94: View Assets in MDC Admin GUI

5. Locate the table entry of the asset you want to modify. See the procedures on View Assets for options to sort and search the asset table. The following fields can be updated from the View screen:

    a. **Tracking Enabled**: This field is a check box that indicates whether the asset can be RF location tracked or not.

    - This field cannot be edited when the asset is assigned to a location-tracked user.
    - For convenience, this field can be enabled when an asset is assigned to a non-location-tracked user; however, location tracking does not take effect until the next time a user checks out this asset. The owner icon associated with the asset will remain a gray non-tracked user icon to indicate that the user is not currently being location tracked (even though the asset may have tracking enabled).

    b. **Description:** This is a general description text for the asset.

    Once changes have been made to fields in the View Assets table, the **Save** button, below the table, becomes enabled to indicate that there are asset entries which have been modified. You can modify multiple entries in the View Assets table. If you use the page control buttons, the entries you have modified may not be displayed on the screen.

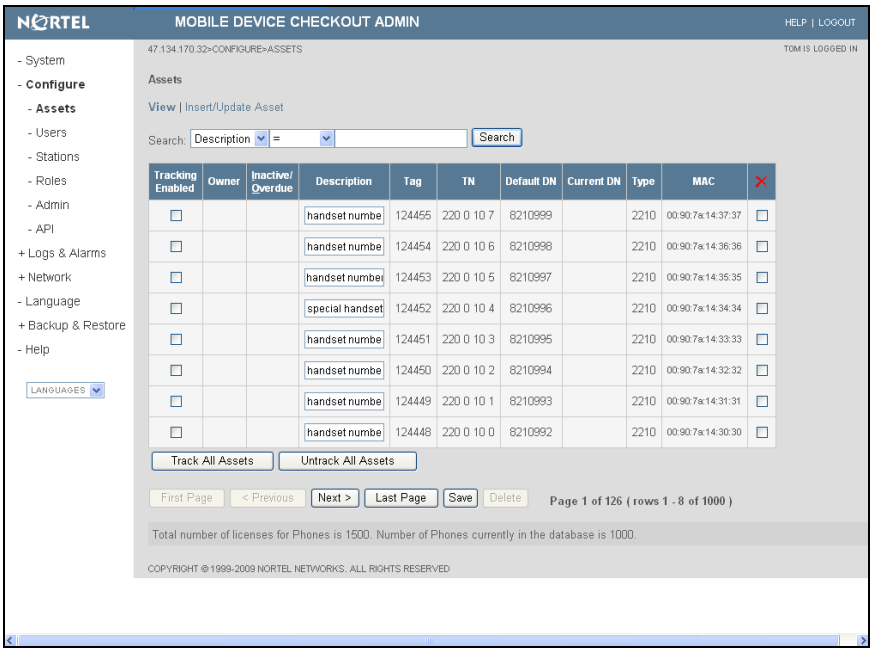


Figure 95: Updating Assets from View Assets Screen

If you attempt to navigate away from the View Assets screen while there are unsaved changes, a warning dialog will pop up.

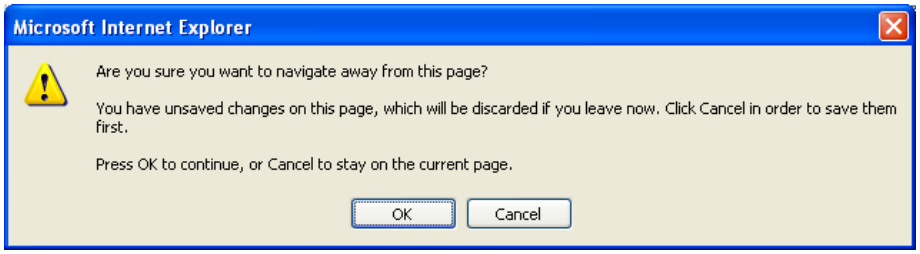


Figure 96: Warning of Unsaved Modifications to Assets

6. Click the **Save** button at the button of the table to save all the updates to the Asset table.

   The View screen will be refreshed and the latest Asset data will be displayed. A successful update message will be displayed. You may verify that the changes were made to the assets. If you use the page control buttons, the entries you have modified may not be displayed on the screen.

10.6 Update Asset from Insert/Update Screen

Description:

This applies to making changes to previously provisioned assets on MDC.

Note: Barcode and Tag Type cannot be updated from the Insert/Update screen.

WARNING: Asset information on the MDC Admin GUI must exactly match the phone configuration on the call server and must remain synchronized, especially for Default DN, Terminal Number, Phone Type and MAC. Any mismatch of information will impair service.

Required information:

- Tag value of asset which needs to be updated
- Updated information for asset: Default DN, Terminal Number, Phone Type, MAC, Description, or Tracking Enabled Status.

  Note: A terminal number (TN) has a specific format which is dependent on the call server being used:

  - For phone on CS 1000 call server, the TN format is **aaa b cc dd** where aaa = loop number, b = shelf number, cc = card number, and, dd = unit number. These are some examples of correctly formatted TNs are: 156 0 05 20, 104 1 00 00, and, 120 0 1 1.
  - For phone on CS 2100 call server, the TN format is **<site> aaa b cc dd** where <site> = site, aaa = frame number, b = group number, cc = upper circuit number, and, dd = lower circuit number. These are some examples of correctly formatted CS 2100 LENs: CICM 001 2 08 81, CICM 1 2 8 81 or CICM 2 2 10 21.

  See Section 10.1 *Terminal Number Format based on Call Server* for a more detailed description of the TN formats.

  Note: For CS 2100, the specified Default DN must be the full 10 digit DN, even if extension dialing is supported.

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Assets** from either the main task area or the Configure submenu on the left navigation menu.
4. The Assets screen appears. The main Assets screen is the View screen, which displays a list of assets in a table format. On a newly installed MDC, there will initially be no assets to display.
5. Click **Insert/Update Asset** from the Assets main task working area to update an asset on the MDC.
6. The Insert/Update Asset screen appears. The Insert/Update Asset screen will look different depending on which call server is integrated with MDC:
   - If the call server is CS 1000, the Insert/Update Asset screen has a Get Phone Information button.
   - If the call server is CS 2100, the Insert/Update Asset screen does not have a Get Phone Information button.

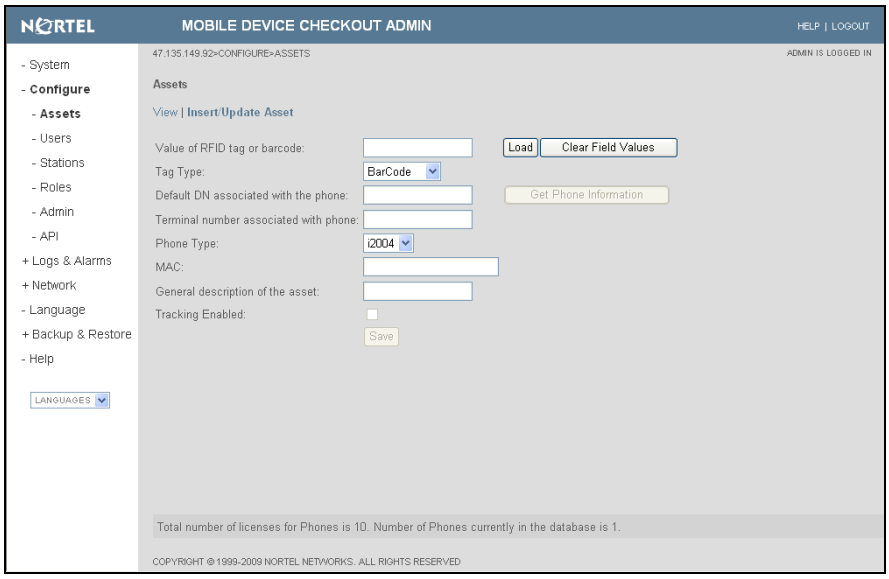


Figure 97: Insert/Update Asset Screen of MDC Admin GUI (with Get Phone Information button)

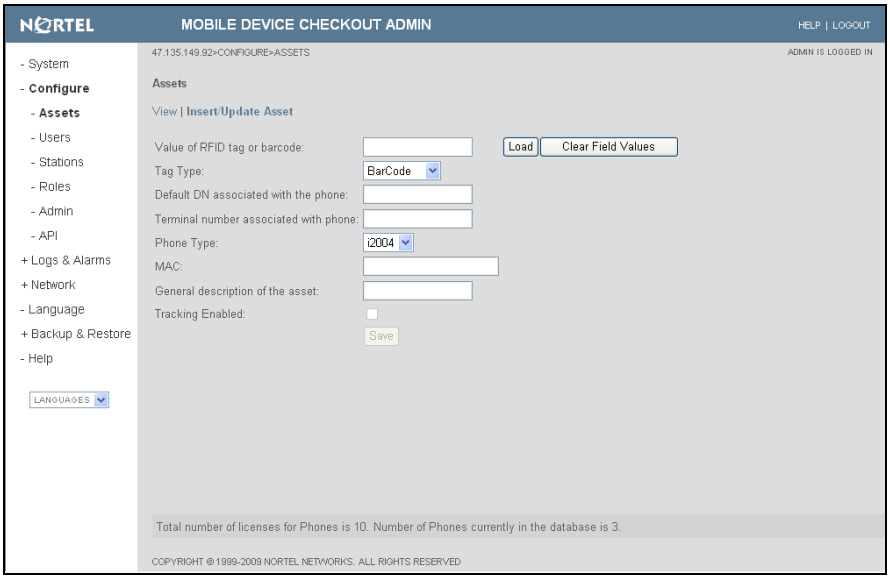


Figure 98: Insert/Update Asset Screen of MDC Admin GUI (without Get Phone Information button)

7. Enter the **Value of RFID tag or barcode** associated with the asset for which you want to make changes. Choose one of the following two methods to enter this information into MDC:
    - Using the barcode reader:
        - Place the cursor in the text box for Value of RFID tag or barcode.
        - Use the barcode reader to scan the barcode/RFID on the asset. This will read and type the barcode/RFID digits into the text box automatically.

- Manually read and type barcode/RFID digits into the text box.

8. Click the **Load** button.

   - For barcodes/tags already provisioned as an asset, this will retrieve the information from the MDC database about this asset and display it on the screen. This is the expected behavior if an existing asset is being modified.

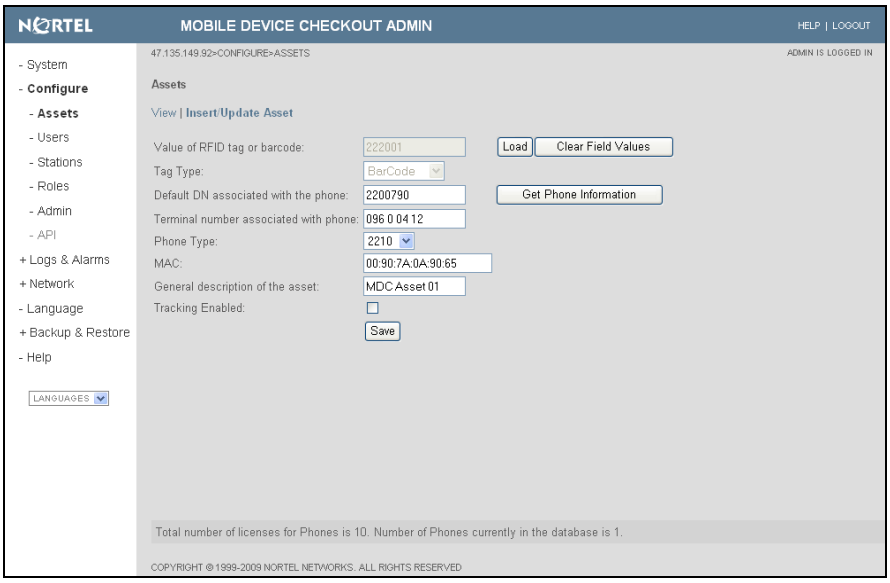


Figure 99: Loaded data on Insert/Update Asset (with Get Phone Information button)

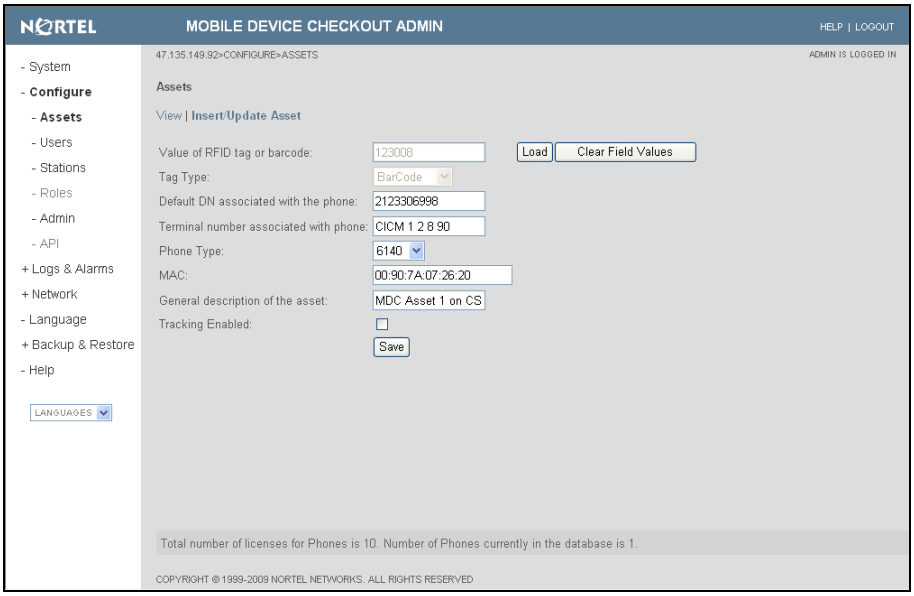


Figure 100: Loaded data on Insert/Update Asset (without Get Phone Information button)

   - For barcodes/tags which are not known, a message will appear on the message banner indicating that no phone has been found with the given tag value. This is not the expected behavior if an existing phone is being modified. If this occurs, make sure the barcode of the asset has been entered correctly and press **Load** again.

- If this barcode/tag has been assigned to a user, an error message will popup.

9. Execute this step if the assets is on a CS 1000 call server (i.e. the Insert/Update Asset screen has a Get Phone Information button):

   The following fields can be updated from the Insert/Update screen. The Default DN, Terminal Number, Phone Type and MAC must match what has been configured on the call server. This can be facilitated by entering the default DN and using the Get Phone Information button as described in step a below:

   a. **Default DN associated with this phone**: This is the directory number associated with the asset.

      - If applicable, type in the new default DN for the asset
      - Ensure the phone is powered on and able to make and receive calls.
      - Click the **Get Phone Information** button. This will trigger the MDC to retrieve the phone information from the call server. Retrieving information from the call server will help to ensure the MDC data matches the call server configuration.
      - After a few moments, the following retrieved information should be displayed on the screen:
        - Terminal number associated with phone
        - Phone Type
        - MAC

        Verify that this is the phone information which should be associated with the asset tag number entered. The phone type will show as 2210 even if the set is a 6140.

        If the MAC address is shown as NON-REGISTERED:

        - For CS 1000 call server, this indicates the handset is either not powered on or it has not been able to complete registration with the call server. The MAC address must be configured for RF location tracked phones. Ensure the handset is powered on and has the ability to make and receive phone calls. Click the **Get Phone Information** button again.
      - If you get a pop message indicating the MDC was unable to retrieve the data, this indicates you have either entered an unknown DN (phone number) OR there was a communication problem. Ensure the phone number is correct and click the **Get Phone Information** button again. If you are unable to retrieve the data from the call server automatically, you can manually enter the phone asset information using the formats specified below.
      - If desired, you can now power off the phone.

   b. **Terminal number associated with phone**: Terminal Number for the asset on the call server. The Terminal Number can be automatically retrieved from the call server using the procedure described in step a above. A terminal number (TN) has a specific format which is dependent on the call server being used:

      - For phone on CS 1000 call server, the TN format is **aaa b cc dd** where aaa = loop number, b = shelf number, cc = card number, and, dd = unit number.

      See Section 10.1 *Terminal Number Format based on Call Server* for a more detailed description of the TN formats.

   c. **Phone Type**: select the phone type from the pulldown menu. The phone type can be automatically retrieved from the call server using the procedure described in step a above.

   d. **MAC**: Media Access Control number for asset. The MAC format must be XX:XX:XX:XX:XX:XX where X is a hexadecimal number (0 to 8 and A to F). The MAC address must be configured for RF location tracked phones.

The MAC can be automatically retrieved from the CS1000 call server using the procedure described in step a above:

- If the MAC address is shown as NON-REGISTERED for CS 1000 call server, this indicates the handset is either not powered on or it has not been able to complete registration with the call server. The MAC address must be configured for RF location tracked phones. Ensure the handset is powered on and has the ability to make and receive phone calls. Click the **Get Phone Information** button again.

10. Execute this step if the assets is on a CS 2100 call server (i.e. the Insert/Update Asset screen does not have a Get Phone Information button):

    The following fields can be updated from the Insert/Update screen. The Default DN, Terminal Number, Phone Type and MAC must match what has been configured on the call server. Note: Manually entering information these MDC Admin GUI fields does not change the call server configuration.

    a. **Default DN associated with this phone**: This is the directory number associated with the asset.

    b. **Terminal number associated with phone**: Terminal Number for the asset on the call server. A terminal number (TN) has a specific format which is dependent on the call server being used:

       - For phone on CS 2100 call server, the TN format is **<site> aaa b cc dd** where <site> = site, aaa = frame number, b = group number, cc = upper circuit number, and, dd = lower circuit number.

       See Section 10.1 *Terminal Number Format based on Call Server* for a more detailed description of the TN formats.

    c. **Phone Type**: select the phone type from the pulldown menu.

    d. **MAC**: Media Access Control number for asset. The MAC format must be XX:XX:XX:XX:XX:XX where X is a hexadecimal number (0 to 8 and A to F). The MAC address must be configured for RF location tracked phones.

11. **General Description of the asset:** This is a general description text for the asset. Click the cursor in the data field and make the changes needed.
12. **Tracking Enabled**: This field is a check box that indicates whether the asset can be RF location tracked or not. This field cannot be edited when the asset is assigned to a location-tracked user.
13. Click **Save** to save the modifications for the asset into the MDC database.
14. Ensure that a successfully updated message is displayed to confirm that the changes were saved. The data fields will be blanked to facilitate inserting or updating another asset.
15. Click **View** to return to the main Asset screen. The View screen will be refreshed and the latest Asset data will be displayed. Verify the changes you made against the specific asset.
16. If the terminal number, phone type, or MAC address of the phone asset has been manually entered in Step 9 (for CS 1000 call server) or Step 10 (for CS 2100 call server) above, it is recommended to test this phone asset by performing a check out and a return of this phone at an MDC Station. See Section 14.1 *Check out a phone to a user at an MDC Station* and 14.2 *Return a phone at an MDC Station* for the detailed description of these tests. (If this is a location tracked phone, you may wish to use the tests in Section 14.4 *Check out a phone to a location-tracked user* and Section 14.5 *Return a phone assigned to a location tracked user*.) In particular, it is important to confirm the phone number on the handset changes to the user's phone number within 3.5 minutes after a successful phone assignment.

    Once these tests have passed, the phone can be added to the phone pool and made available for general use.

    If the phone number does not change to the user's phone number within 3.5 minutes of a successful phone assignment, perform the check out again. If the problem persists:

- Return the phone at an MDC Station
- Confirm that the phone number, terminal number and the MAC address are configured correctly in the MDC Admin GUI for this phone.

If necessary, correct the phone information in the MDC Admin GUI by using this procedure again (Section 10.6 *Update Asset from Insert/Update Screen*.)

10.7 Enable Location Tracking for All Assets

Description:

Use this procedure to enable location tracking for all assets. This function is disabled (grayed out) when all assets are already enabled for location tracking.

Note: When location tracking is enabled on assets, there must also be sufficient licenses available on the Ekahau location service to enable location tracking of these assets. Also, the location tracking feature must also be manually enabled on the physical phones.

WARNING: It is recommended to save any changes made to assets in the View screen prior to enabling location tracking for all assets. You will be warned if there are unsaved changes.

Required information:

None

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Assets** from either the main task area or the Configure submenu on the left navigation menu.
4. The Assets screen appears. The main Assets screen is the View screen, which displays a list of assets in a table format. On a newly installed MDC, there will initially be no assets to display.

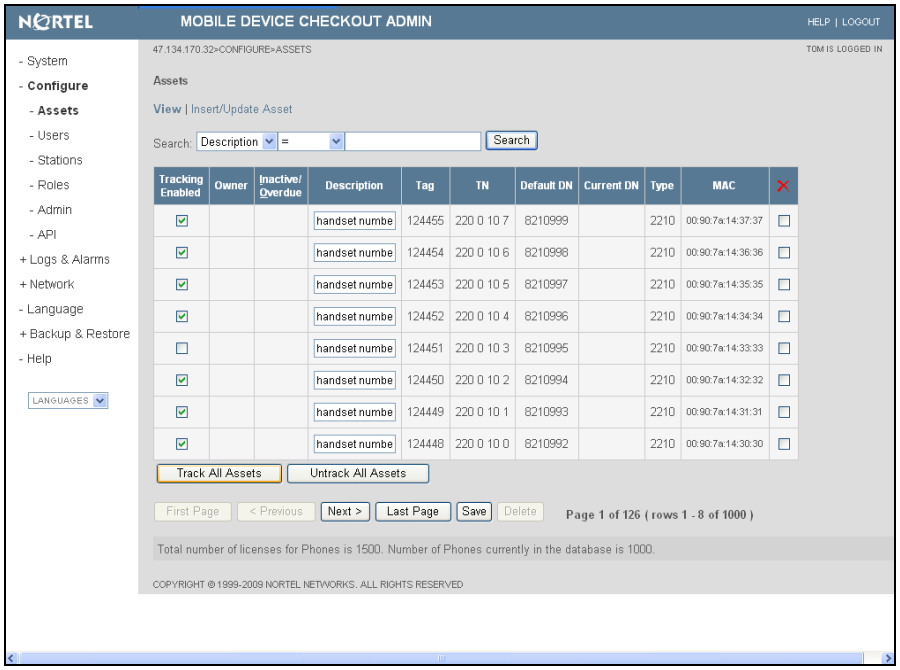


Figure 101: View Assets on MDC Admin GUI

5. Click the **Track All Assets** button to enable location tracking for all assets. This button is disabled (grayed out) when all assets are already enabled for location tracking.
6. The View screen will be refreshed and the latest Asset data will be displayed. The Tracking Enabled box is enabled for all assets not assigned to users.

10.8 Disable Location Tracking for All Assets

Description:

Use this procedure to disable location tracking for all assets. Note: This will apply only to assets which are not currently assigned to a location-tracked user.

This function is disabled (grayed out) when all assets are already disabled for location tracking.

WARNING: It is recommended to save any changes made to assets in the View screen prior to disabling location tracking for all assets. You will be warned if there are unsaved changes.

Required information:

- None

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Assets** from either the main task area or the Configure submenu on the left navigation menu.
4. The Assets screen appears. The main Assets screen is the View screen, which displays a list of assets in a table format. On a newly installed MDC, there will initially be no assets to display.

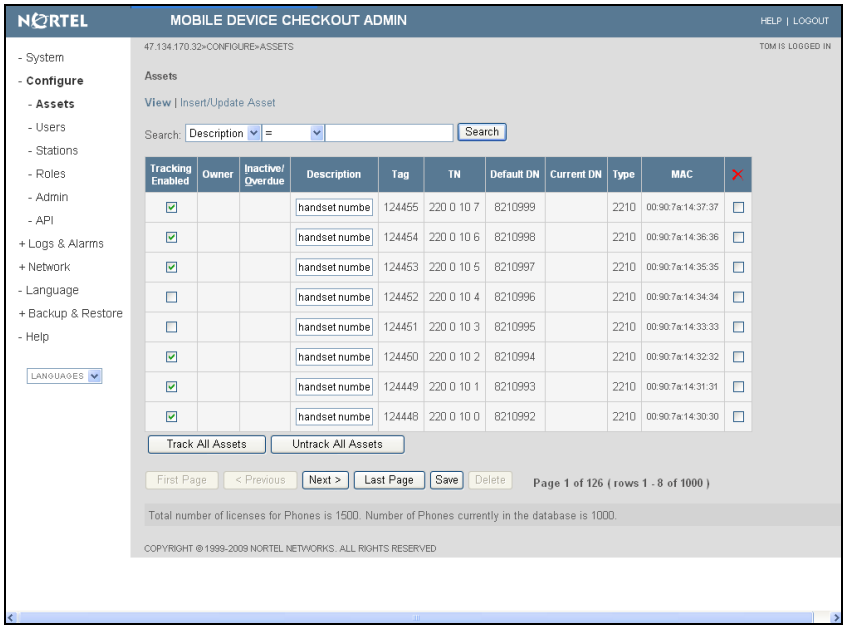


Figure 102: View Assets on MDC Admin GUI

5. Click the **Untrack All Assets** button to disable location tracking for all assets. Note: This will only apply to assets which are not currently assigned to a location-tracked user. This button is disabled (grayed out) when all assets are already disabled for location tracking.

   With a large number of assets, it may take up to one minute to untrack all assets. A popup dialog will appear to inform the administrator the action is in progress.

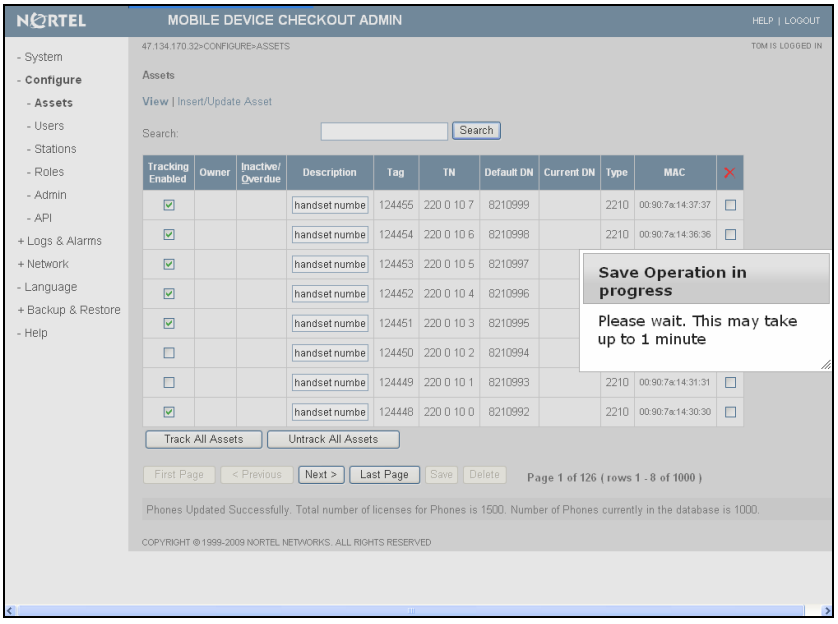


Figure 103: Tracking Disabled on all Assets

6. The View screen will be refreshed and the latest Asset data will be displayed. Confirm that the Tracking Enabled box is updated for all assets not assigned to users.

10.9 Delete Asset

Description:

Use this procedure to delete assets. Assets cannot be deleted while they are checked out to users.

WARNING: It is recommended to save any changes made to assets in the View screen prior to deleting assets. The Save button is enabled when there is an unsaved change.

Required information:

- Asset which needs to be deleted identified by one of these fields: tag, terminal number, default DN, or MAC address.

Steps:

From the MDC Admin GUI, click the **Configure** task on the left navigation menu.

1. The Configure screen of the Mobile Device Checkout Admin appears.
2. Click **Assets** from either the main task area or the Configure submenu on the left navigation menu.
3. The Assets screen appears. The main Assets screen is the View screen, which displays a list of assets in a table format. On a newly installed MDC, there will initially be no assets to display.

   Note: The **Delete** button, below the asset table, does not become enabled until there are entries marked for deletion from the asset table.

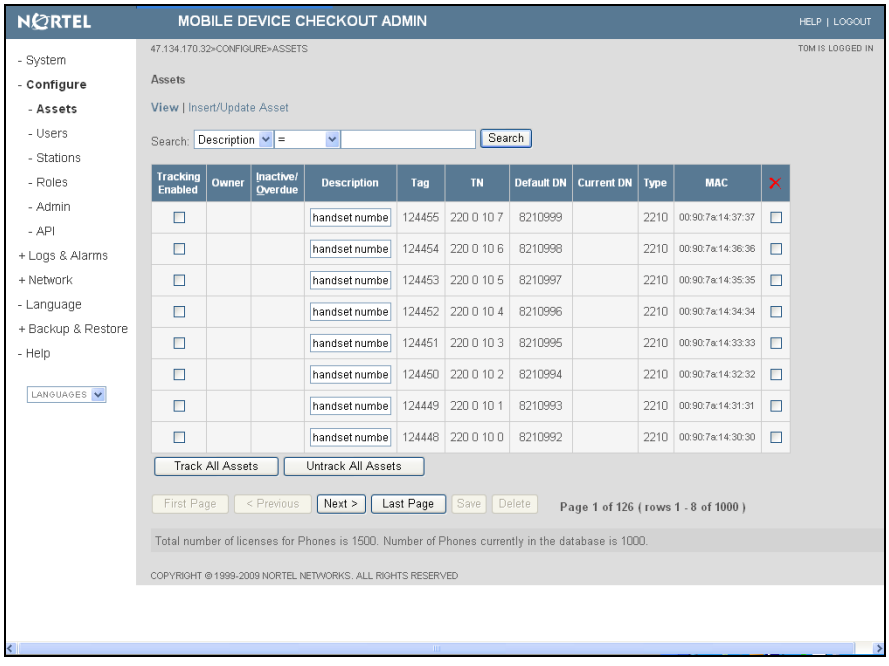


Figure 104: View Assets in MDC Admin GUI

4. Locate the table entry of the asset you want to remove. See the procedures on View Assets for options to sort and search the asset table. Check the box in the **Delete** column (rightmost column in the table) to delete a particular asset. Once any assets have been marked for deletion from the View Assets table, the **Delete** button, below the table, becomes enabled to indicate that there are pending deletions. You may

mark multiple assets for deletion. If you use the page control buttons, the entries you have marked for deletion may no longer be displayed on the screen.

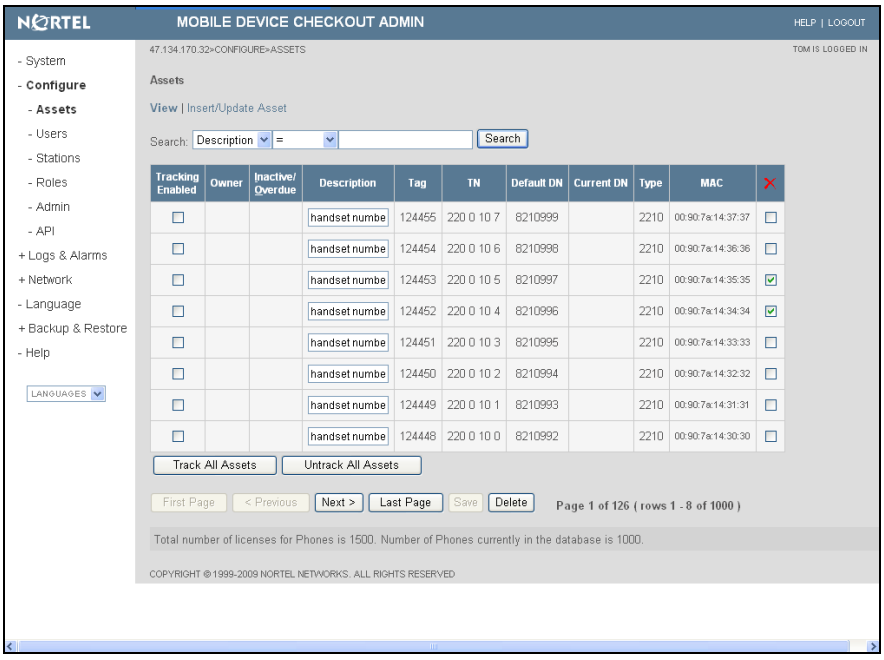


Figure 105: Deleting Assets from View Assets

If you attempt to navigate away from the View Assets screen while there are assets marked for deletion, a warning dialog will pop up.

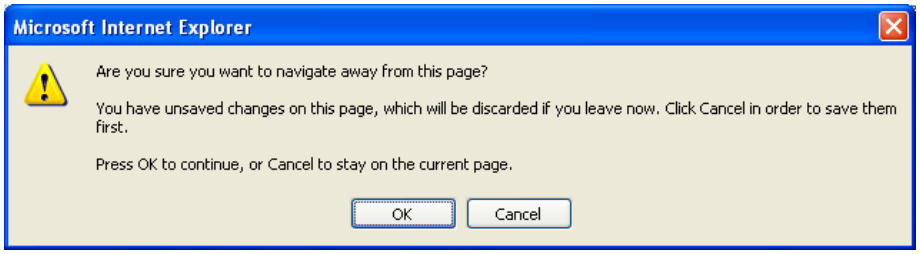


Figure 106: Warning of assets marked for Deletion

Note: Assets cannot be deleted while they are checked out to users.

5. Click the **Delete** button, below the asset table, to delete the marked asset(s).
6. A delete confirmation popup dialog will appear. Click **OK** to confirm deleting the asset(s).

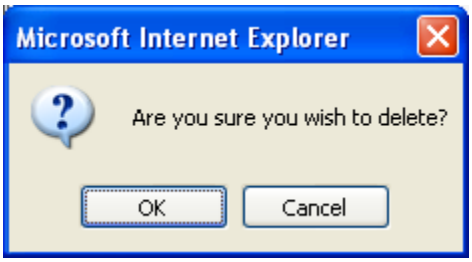


Figure 107: Delete Asset Confirmation Dialog

7. The View screen will be refreshed and the latest Asset data will be displayed. The deleted asset(s) are removed from the list of assets.

10.10 Bulk loading of Assets

Description:

To assist with the coordination of large numbers of assets and users, scripts have been created to take specific formatted files as their input for the purpose of creating, deleting, and updating of assets and users on the MDC Server. These scripts were designed to synchronize MDC with the information contained in other administrative directories or databases.

This script must be executed on the MDC Server.

WARNING: Asset information on the MDC must exactly match the phone configuration on the call server and must remain synchronized. Any mismatch of information will impair service. The input files used with the bulk loading scripts should be derived from a primary data source used to drive the call server configuration, such as LDAP.

WARNING: The number of location-tracked users and the number of assets permitted on an MDC is controlled by license. Ensure that you have sufficient licenses when using bulk loading scripts.

WARNING: It is strongly recommended that a manual MDC backup be performed prior to bulk loading assets and users. In the event of errors or the use of out-of-date input, a backup will permit the user to restore the current view of users and assets into the MDC database.

WARNING: A bulk loading script cannot operate at the same time as any backup or restore activities or another bulk loading script.

Note:

- Unlike adding individual phones through the MDC Admin GUI, the phones do not have to be powered on while they are being bulk loaded.
- The bulk loading is intended to be used to coordinate large numbers of assets and users for the purposes of adding, deleting and synchronizing information. The input files are expected to specify all assets/users needed by MDC server, thus:
  - Users and assets are designated either as manually added through the MDC Administration GUI or added via bulk loading scripts. The bulk loading scripts will update or delete only those users and assets which were originally added through bulk loaded scripts. They will not update nor modify users or assets which were originally manually added through the MDC Administration GUI.
  - If a user/asset is present in the bulk loading input file but not present in the MDC database, this will be interpreted as an addition of user/asset by the scripts. There must be available licenses on the MDC server for the addition of any new tracking-enabled users and new assets.
  - If an existing user/asset in the MDC database is not present in the bulk loading input file, this will be interpreted as a deletion of user/asset by the scripts.

- If a user/asset is present in both the input file and MDC database, any field associated with the user/asset will be updated, if needed, based on the information in the input file.

- The input files are delimited. The default delimiter is a comma. However, optionally, the user can specify another delimiter character. If the delimiter is a tab, then type (CTRL_V CTRL_I) to put in the delimiter on the command line in UNIX.
- The scripts will go through the following steps:
  - Validate the format of the input file. The scripts automatically check the input file for correct format and will inform the user if formatting errors are discovered. Unfortunately, the scripts cannot determine whether the data is correct.
  - Verify that there are sufficient licenses for the changes (taking into account the additions and deletions).
  - Apply the changes to the MDC database: additions, updates and deletions.
- Data validation is performed by the MDC database and invalid input will be skipped.
- Upon completion, the script will summarize what actions were taken:
  - how may new assets/users were added
  - how many assets/users were deleted
  - how many assets/users were updated
  - how many records were rejected from the input file
- The scripts will issue a start and end log with severity INFO. Failure logs with severity CRITICAL will be generated as needed.
- The fields of the asset input file are fixed. However, the values permitted for some data fields in the asset input file are dependent on which call server is integrated with MDC
  - For CS 1000:
    - For phone on CS 1000 call server, the TN format is **aaa b cc dd** where aaa = loop number, b = shelf number, cc = card number, and, dd = unit number. See Section 10.1 *Terminal Number Format based on Call Server* for a more detailed description of the TN formats.
    - A sample asset input file shown below for a CS 1000 call server. The General Description field is optional:

Barcode	Tag Type	Terminal Number	Default DN	Phone Type	Tracking Enabled	MAC	General Description
12345	Barcode	061 0 00 01	4101	I2004	1	00:90:7A:05:65:37	MDC Phone 1
23456	Barcode	061 0 00 05	4105	I2004	1	00:90:7A:04:BE:17	MDC Phone 2

  - For CS 2100:
    - For phone on CS 2100 call server, the TN format is **<site> aaa b cc dd** where <site> = site, aaa = frame number, b = group number, cc = upper circuit number, and, dd = lower circuit number. See Section 10.1 *Terminal Number Format based on Call Server* for a more detailed description of the TN formats.
    - For CS 2100, the default DN specified must be the full 10 digit DN, even if extension dialing is supported.
    - A sample asset input file shown below for a CS 2100 call server. The General Description field is optional:

Barcode	Tag Type	Terminal Number	Default DN	Phone Type	Tracking Enabled	MAC	General Description
12345	Barcode	CICM 1 2 8 81	8198524101	I2004	1	00:90:7A:05:65:37	MDC Phone 1
23456	Barcode	CICM 1 2 8 82	8198524105	I2004	1	00:90:7A:04:BE:17	MDC Phone 2

- The script is **LoadPhoneScript.php** located in **/opt/nortel/ebs/mdc/backup**

Required information:

- IP address of the MDC Server
- Unix username and password for MDC server
- Asset input file formatted as described above

Steps:

- Example invocation:

  php -f LoadPhoneScript.php -- -fPhoneAssetView.txt -d' '

  where -f parameter is the input file (PhoneAssetView.txt).

  where -d parameter is the delimiter. When the delimiter is a tab (CTRL_V CTRL_I) will specify the tab delimiter on the UNIX command line.

- Sample output from another invocation:

  php -f LoadPhoneScript.php -- -f/tmp/sandra/phones.csv -d','

  where -f parameter is the input file (/tmp/sandra/phones.csv).

  where -d parameter is the delimiter, (comma). This parameter is optional as comma is the default delimiter.

  Example:

  ```
  [root@sc-mdc-2 backup]# php -f LoadPhoneScript.php -- -f/tmp/sandra/phones.csv -d','
  Validating Data...
  Validating Licenses...
  Applying Data File...
  |XXXXXXX_____________________________________________| 12%

  [root@sc-mdc-2 backup]# php -f LoadPhoneScript.php -- -f/tmp/sandra/phones.csv -d','
  Validating Data...
  Validating Licenses...
  Applying Data File...
  |XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX| 100%
  Done
  1000 record(s) added
  0 record(s) updated
  0 record(s) rejected
  ```

0 old record(s) deleted

Done.

- Sample output from bulk updating phones:

  [root@sc-mdc-2 backup]# php -f LoadPhoneScript.php -- -f/tmp/sandra/phones.csv

  Validating Data...

  Validating Licenses...

  Applying Data File...

  |XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX| 100%

  Done

  0 record(s) added

  1000 record(s) updated

  0 record(s) rejected

  0 old record(s) deleted

  Done.

11 Managing Users

The user should have a barcode on his employee badge. The barcode is used to identify the user. If needed, refer to the document NN49010-501 Nortel Healthcare Solutions MDC Deployment Guide for more information on creating barcode labels.

The MDC interface to the call server should be provisioned prior to provisioning users. See Section 9 Integrating MDC Server and Call Server for further details.

WARNING: User information on the MDC Admin GUI must exactly match the user configuration on the call server and must remain synchronized. Any mismatch of information will impair service. If changes have been made to the call server, update the associated users in MDC.

When roles are not licensed:

- If a user has checked out a phone, a clickable icon will appear in the phone field to provide details about the phone.
- If a phone (asset) is used while checked out (i.e. assigned) to a user, the calling phone number associated with the phone will be the phone number of this user as displayed in the Phone Number field.
- When the phone (asset) is returned by the user, the phone icon field will be blanked. The phone asset will no longer be associated with the user's phone number. When the phone is used while not assigned to a user, the calling phone number associated with the phone asset will be the default DN.

See Section 12 *Managing Roles* for a description of roles and how roles can change the phone numbers assigned to the phone when it is checked out by a user.

The number of location-tracked users permitted on an MDC is controlled by license. The number of non-location-tracked users is unrestricted. At the bottom of the Users screens, a running tally of the total number of licensed location-trackable users permitted, along with the number of licensed location-tracked users in use, is displayed. It is possible for an error message to appear indicating that there is no license file OR a warning message indicating that all licenses for location-tracked users have been used. When the license file is updated, new license information may not appear for up to 5 hours on existing MDC Admin GUI sessions. However, the user may choose to manually refresh their licensing information. Refer to Section 7 *MDC Licensing and Keycode Retrieval System (KRS)* for more information on MDC licensing.

Ensure that you have sufficient licenses for location-tracked users when enabling location tracking. A popup dialog will appear to warn the user if they try to enable location tracking when there are no available location-tracked user licenses.

Location tracking enabled is an attribute of the asset and an attribute of the user. The phone icon is colored green with a T for location tracked only when both the asset and the user have location tracking enabled when the user checked out the asset.

There are three scenarios when a location-tracking-enabled user may have an asset checked out but the phone icon does not indicate location tracking:

1. The user has checked out an asset which is not configured to support location tracking.
2. The user has their location-tracking-enabled status changed while they already had an asset checked out. The location tracking will not take effect until the next time the user checks out an asset. The phone icon associated with the user will remain a gray non-tracked phone icon to indicate that the user is not currently being location tracked.
3. Both the user and the asset had location tracking enabled when the user checked out the asset. Normally, the phone icon will be a green tracked (T) phone icon. However, if there was a communication error with the Location Server at the time the user checked out the asset, MDC will be unable to confirm that the user is being location tracked. The user will be informed at the MDC Station that they are not being tracked. The asset will be checked out but the phone icon associated with the user will be a gray non-tracked phone icon to indicate that the user is not currently being location tracked.

Note: When location tracking is enabled on assets, there must also be sufficient licenses available on the Ekahau location service to enable location tracking of these assets. Also, the location tracking feature must also be manually enabled on the physical phones. See Section 8 *Integrate MDC and Location Service* for more information on enabling location services.

The procedures in this section are:

- Insert New Users
- View Users
- View Assets Assigned to User
- Update Users from View Screen
- Update Users from Insert/Update Screen
- Enable Location Tracking for All Users
- Disable Location Tracking for All
- Delete Users
- Bulk loading of Users

11.1 Insert New Users

Description:

This procedure creates a user in MDC who is associated with both his employee badge barcode/tag and his phone information.

The user's information MUST already be provisioned on the call server.

The number of location-tracked users permitted on an MDC is controlled by license. Ensure that you have sufficient licenses for location-tracked users when enabling location tracking. If licensing information has changed within the last 5 hours, you may need to manually refresh the licensing information using the procedure in Section 7.7 *Update Licensing Information in the* MDC.

Note: This procedure is for adding individual users. For a large number of users, Nortel provides a bulk-load capability, described in Section 11.9 *Bulk loading of Users*.

WARNING: User information on the MDC Admin GUI must exactly match the user configuration on the call server and must remain synchronized. Any mismatch of information will impair service. If changes have been made to the call server, update the associated users in MDC.

WARNING: With CS 1000 call servers, the Get Display Name button will not be able to retrieve user data from the call server if there are any the call server administrators or applications (including MDC) using backup or similar activities at the same time. If this condition cannot be avoided, the MDC administrator has the option to manually enter the user data when the Get Display Name button is unable to retrieve this data. The Get Display Name button is not available when the user is on a CS 2100 call server.

Required information:

For each user added to MDC:

- Barcode labels of user
- Tag type

- Phone number/ DN
- Display name
- First name
- Last name
- Whether the user is tracking enabled
- [Optional] Brief text description of the user

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Users** from either the main task area or the Configure submenu on the left navigation menu.
4. The Users screen appears. It displays a list of users in a table format. On a newly installed MDC, there will initially be no users to display.

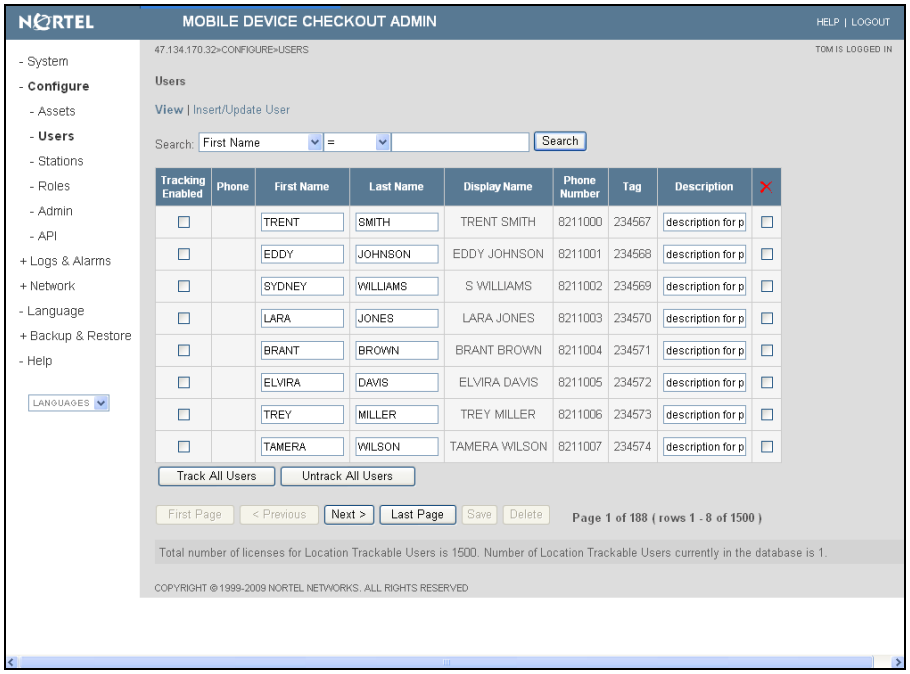


Figure 108: View Users screen of MDC Admin GUI

5. Ensure that there is a barcode label physically stuck on the employee badge.
6. Click **Insert/Update User** from the Users main task working area to add a user to MDC.
7. The Insert/Update User screen appears. The Insert/Update User screen will look different depending on which call server is integrated with MDC:
    - If the call server is CS 1000, the Insert/Update User screen has a Get Display Name button.
    - If the call server is CS 2100, the Insert/Update User screen does not have a Get Display Name button.

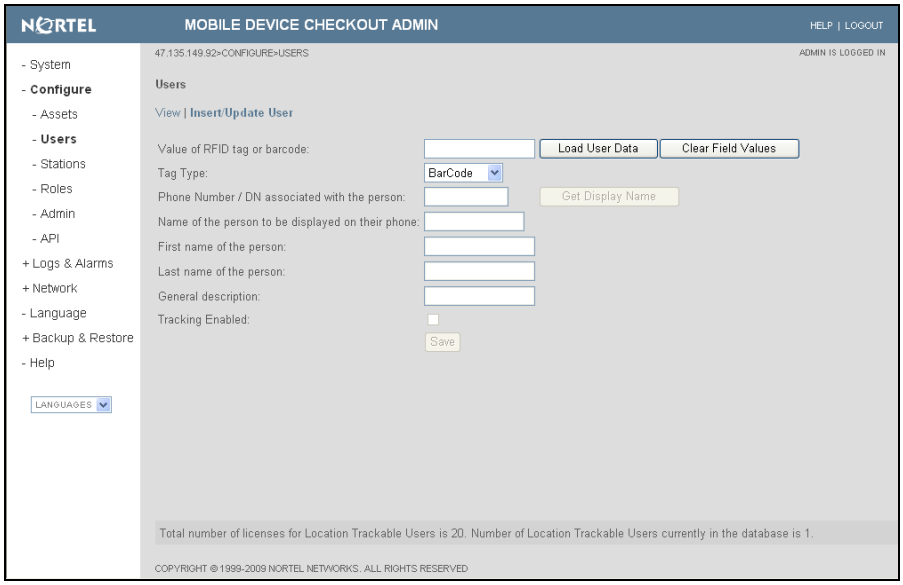


Figure 109: Insert/Update User Screen of MDC Admin GUI (with Get Display Name button)

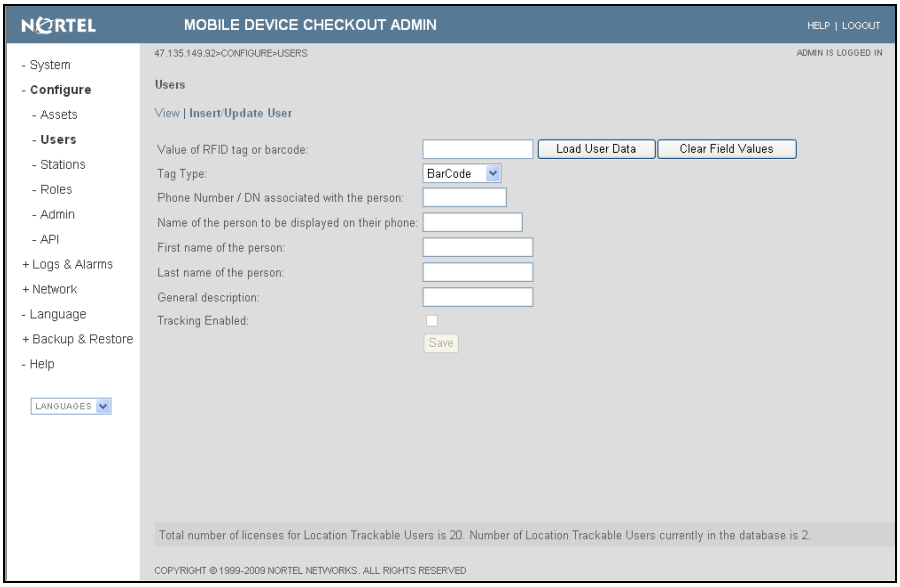


Figure 110: Insert/Update User Screen of MDC Admin GUI (without Get Display Name button)

8. To insert a new user, use the information physically on the user's employee badge and the data which has been provisioned in the call server. Enter in the following parameters:
    a. **Value of RFID tag or barcode**: This is the RFID or barcode label associated with the user's employee badge. Verify that the information on the user's employee badge matches the information on the screen. Choose one of the following two possible methods to enter this information into MDC:
        - Using the barcode reader:

- Place the cursor in the text box for Value of RFID tag or barcode.
- Use the barcode reader to scan the barcode/RFID on the user's employee badge. This will read and type the barcode/RFID digits into the text box automatically.

- Manually read and type barcode/RFID digits into the text box.

b. **Tag Type**: Select the type of tag from the Tag Type pulldown menu.

c. Click the **Load User Data** button.

- For barcodes/tags which are not known (i.e. new), a message will be displayed indicating no user found for tag value. This is the expected behavior when a new user is being added. The Tag Type and Value of RFID tag or barcode text fields become non-editable and the remaining text fields will become editable to permit the input of the user information.
- For barcodes/tags already provisioned to a user, this will retrieve the information from the MDC database about this user and display it on the screen. This is not the expected behavior if a new user is being added. If this occurs, make sure the barcode of the user's employee badge has been entered correctly and all users have unique barcodes.
- If this barcode/tag has been assigned to an asset, an error message will popup.

9. Type in the **Phone Number/ DN associated with the person.** For CS 2100, the phone number specified must be the full 10 digit DN, even if extension dialing is supported.
10. If the call server is a CS 1000 (i.e. the Insert/Update User screen has a Get Display Name button), do the following steps:

a. Click the **Get Display Name** button. This will trigger MDC to retrieve this user's phone information from the call server.

a. After a few moments, the following retrieved information should be displayed on the screen:

- Name of the person to be displayed on their phone
- First name of person
- Last name of person

b. Confirm that this is the name of the user being added.

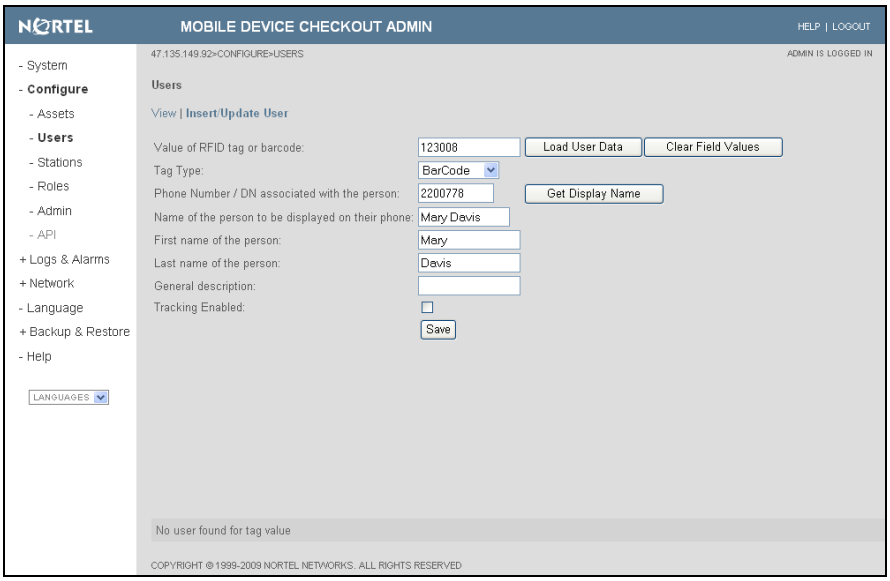


Figure 111: Get Display Name for Insert/Update User

If you have entered an unknown Phone number/DN or there are communication problems, a popup message dialog will appear. Check and correct the **Phone number/DN associated with the person** if needed. Click the **Get Display Name** again.



Figure 112: Unable to retrieve data for Requested DN.

If you have the correct phone number, this message may indicate there is no display name configured against the phone number on the call server or communication problems persist. You can manually enter the user name information. Note: Manually entering information into these fields will not change the call server configuration:

- **Name of the person to be displayed on their phone:** Display name assigned to the user in the call server
- **First name of the person**
- **Last name of the person**

11. If the call server is a CS 2100 (i.e. Update User screen does not have a Get Display Name button), do the following steps:

    a. Type in the **Name of the person to be displayed on their phone**. This is the Display name assigned to the user in the call server. Information should match the configuration on the call server. Note: Manually entering information into this field does not change the call server configuration

    b. Type in the **First name of the person.**

    c. Type in the **Last name of the person**

12. Type in the **General Description of the user**. This is a brief text description of the user.
13. Click the **Tracking Enabled** box if this user should be RF location tracked when they checkout an asset (which supports RF location tracking). The number of location-tracked users permitted on an MDC is controlled by license. If there are no available location-tracked user licenses, a popup dialog will appear to warn the user if they try to check the Tracking Enabled box.

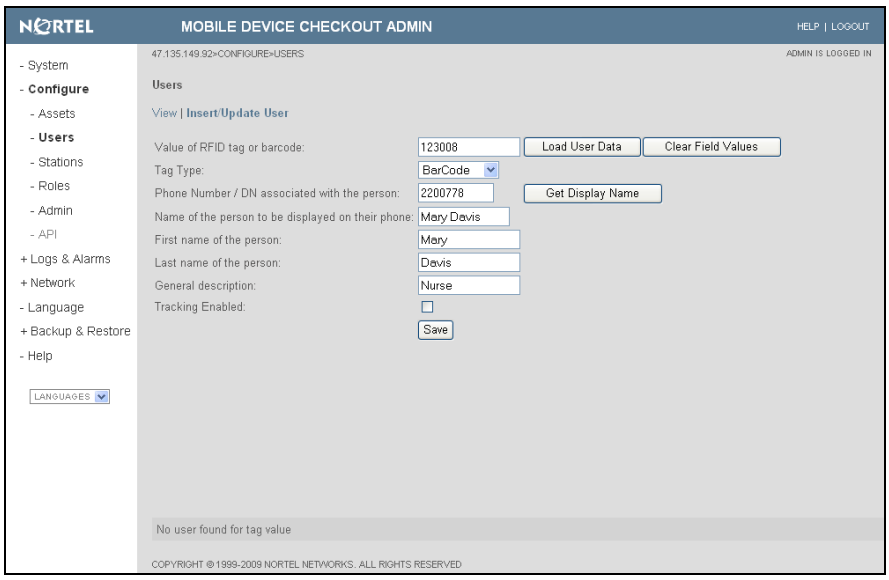


Figure 113: Filled Insert/Update User Screen (with Get Display Name button)

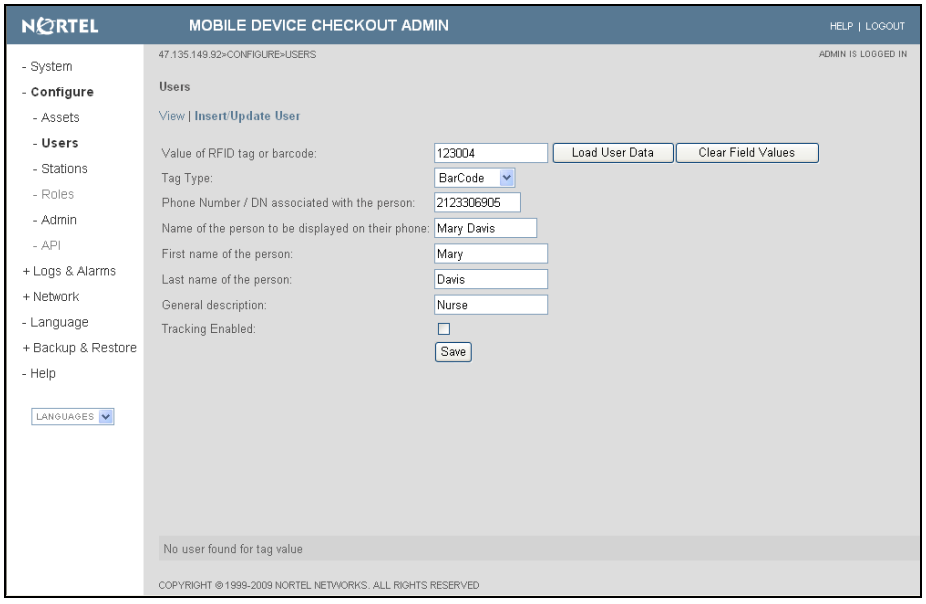


Figure 114: Filled Insert/Update User Screen (without Get Display Name button)

14. Click **Save** to insert the displayed user into the MDC database.
15. Ensure that a successfully inserted message is displayed to confirm the user was added. The data fields will be blanked to facilitate inserting the next user.

16. When you have completed adding all the users, click **View** from the main task area menu. The main Users screen is the View screen, which displays a list of users in a table format. You should see all the users you have just added to MDC displayed.

11.2 View Users

Description:

This procedure describes how to view the list of users from the MDC Admin GUI.

Required information:

- None

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Users** from either the main task area or the Configure submenu on the left navigation menu.
4. The Users screen appears. The main Users screen is the View screen, which displays a list of users in a table format. On a newly installed MDC, there will initially be no users to display.

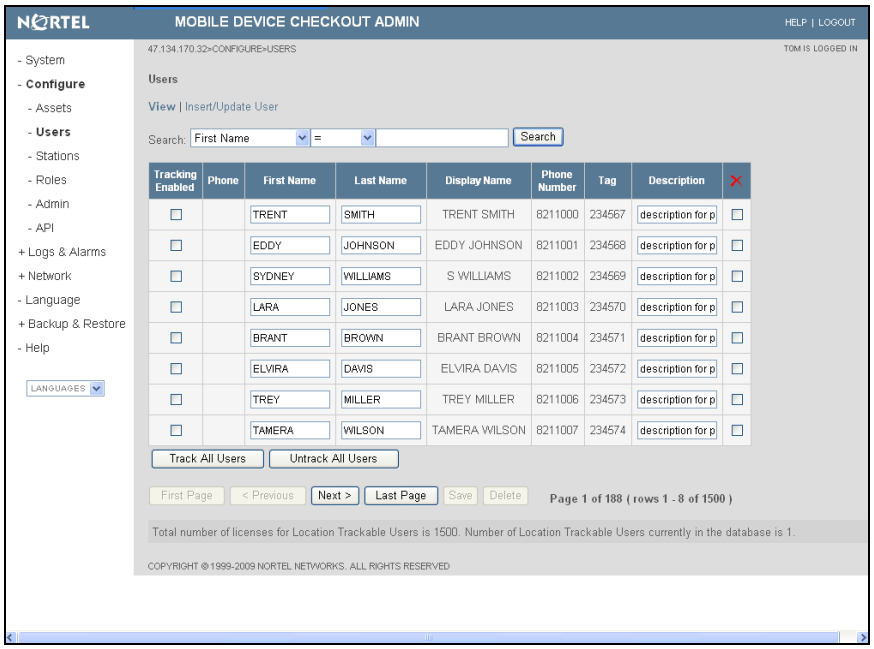


Figure 115: View Users on MDC Admin GUI

The columns in the users table are:

- Tracking Enabled: Indicates whether the user requires RF location tracking.
- Phone: This field will display an icon when the user has checked out an asset or be blank if the user does not have an asset assigned.
    - The icon may have an **R** if a role has been assigned to the phone.

- The icon may also be colored green with a **T** to indicate that RF location tracking is enabled.
- The icon may also be colored green with a **T** and **R** if the user is being RF location tracked and in addition a role has been assigned to the phone.

See Section 11.3 *View Assets Assigned to User* for further details on this field.

- First Name: Text field with the first name of the user.
- Last Name: Text field with the last name of the user.
- Display Name: Display name assigned to the user in the call server.
- Phone Number: Directory number assigned to the user in the call server.
- Tag: Tag Number for the user, which is typically the employee badge number.
- Description: A text description of the user.
- Delete: This field is checked to delete the user from MDC.

When there are a large number of users in the list, only some of the users will be displayed on the screen at a time. This is considered a "page." The page number is shown along with the total number of available pages at the bottom of the table to help orient the user within the view users table. The equivalent row information for these entries in the users table is also given in parentheses.

There are a number of options to view other users not displayed on the screen:

- Paging
- Sort
- Search

See Section 5.2.4 *MDC Admin GUI Paging, Sort, and Search* for a description of paging, sorting and searching and an explanation of how to use these features.

11.3 View Assets Assigned to User

Description:

This procedure describes how to view the asset assigned to a user in the MDC Admin GUI.

Refer to Section 12 *Managing Roles* for more information on roles. See Section 8.2 *Integrating MDC Server and Location Service* for more information on location tracking.

Required information:

- None

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Users** from either the main task area or the Configure submenu on the left navigation menu.
4. The Users screen appears. The main Users screen is the View screen, which displays a list of users in a table format. On a newly installed MDC, there will initially be no users to display.
    a. When a user has checked out an asset, a phone icon will appear in the Phone field.

- The phone icon may have an **R** if a role has been assigned to the phone.
- The phone icon may be colored green and have a **T** to indicate that the user is being RF location tracked.
- The phone icon may be colored green with a **T** and **R** if the user is being RF location tracked and in addition a role has been assigned to the phone.

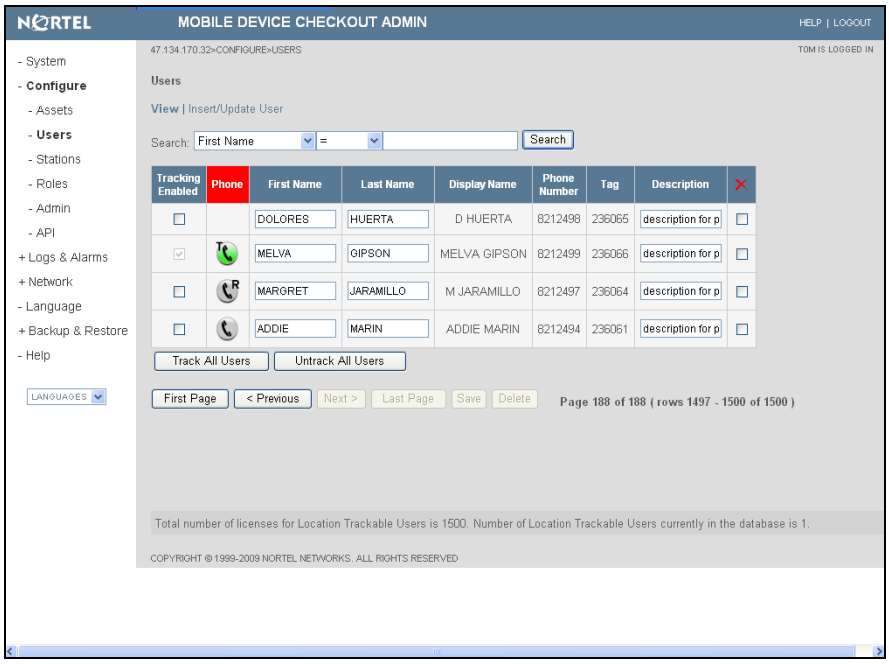


Figure 116: View Users with Phone Associated

b. Click the **icon** in the Phone field and a popup screen will appear with the details of the asset which this user has checked out.

- Tag Value is the tag number for the asset.
- Terminal Number is the terminal number for the asset on the call server.
- Default DN is directory number associated with the asset.
- Personal Number Provisioned on Phone will indicate whether the personal number of the user has been assigned to the asset.
- Role Provisioned on Phone is the name of the role assigned to the phone. This field may be blank if no role has been assigned.
- Role Phone Number is the phone number of the role assigned to the phone. This field may be blank if no role has been assigned.
- Role Phone Number Provisioned on Line will give the phone line number which has been assigned the role phone number.
- Phone Type is the phone type configured for the asset in the call server.
- MAC Address is the Media Access Control number for the asset.
- Assignment Time shows the time when the user checked out this asset.

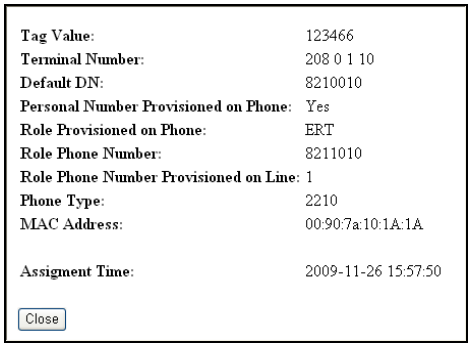


Figure 117: Phone Icon details with Roles

11.4 Update Users from View Screen

Description:

This applies to making changes to previously provisioned users on MDC.

Note: There are limited fields which can be updated from the View Users screen.

The number of location-tracked users permitted on an MDC is controlled by license. Ensure that you have sufficient licenses for location-tracked users when enabling location tracking. If the licensing information has changed within the last 5 hours, you may need to manually refresh the licensing information using the procedure in Section 7.7 *Update Licensing Information in the* MDC.

Required information:

- Users which need to be updated identified by one of these fields: First Name & Last Name, Display Name, Phone Number, Tag Number, or Description
- Updated information for asset: First Name, Last Name, Description, or Tracking Enabled Status

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Users** from either the main task area or the Configure submenu on the left navigation menu.
4. The Users screen appears. The main Users screen is the View screen, which displays a list of users in a table format. On a newly installed MDC, there will initially be no users to display.

   Note: The **Save** button, below the users table, does not become enabled until there are changes made to entries in the users table.

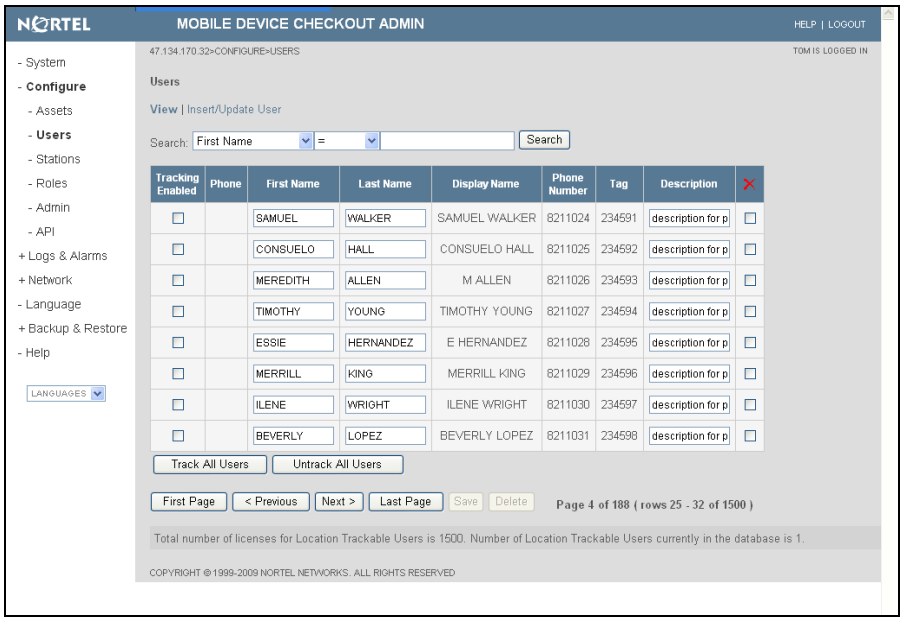


Figure 118: View Users in MDC Admin GUI

5. Locate the table entry of the users you want to modify. See the procedures on View Users for options to sort and search the user table. The following fields can be updated from the View screen:

    a. **Tracking Enabled**: This field is a check box that indicates whether the user is RF location tracked or not.

        - The number of location-tracked users permitted on an MDC is controlled by license. If there are no available location-tracked user licenses, a popup dialog will appear to warn the user if they try to check the Tracking Enabled box.
        - Tracking enabled cannot be disabled while a location-tracked user has an asset checked out.
        - For convenience, this field can be enabled when a non-location-tracked user has an asset assigned; however, location tracking does not take effect until the next time the user checks out an asset. The phone icon associated with the user will remain a gray non-tracked phone icon to indicate that the user is not currently being location tracked (even though they have tracking enabled).

    b. **First Name**: This is a text field containing the first name of the user.

    c. **Last Name**: This is a text field containing the last name of the user..

    d. **Description:** This is a general description text for the user.

    Once changes have been made to fields in the View Users table, the **Save** button, below the table, becomes enabled to indicate that there are user entries which have been modified. You can modify multiple entries in the View Users table. If you use the page control buttons, the entries you have modified may not be displayed on the screen.

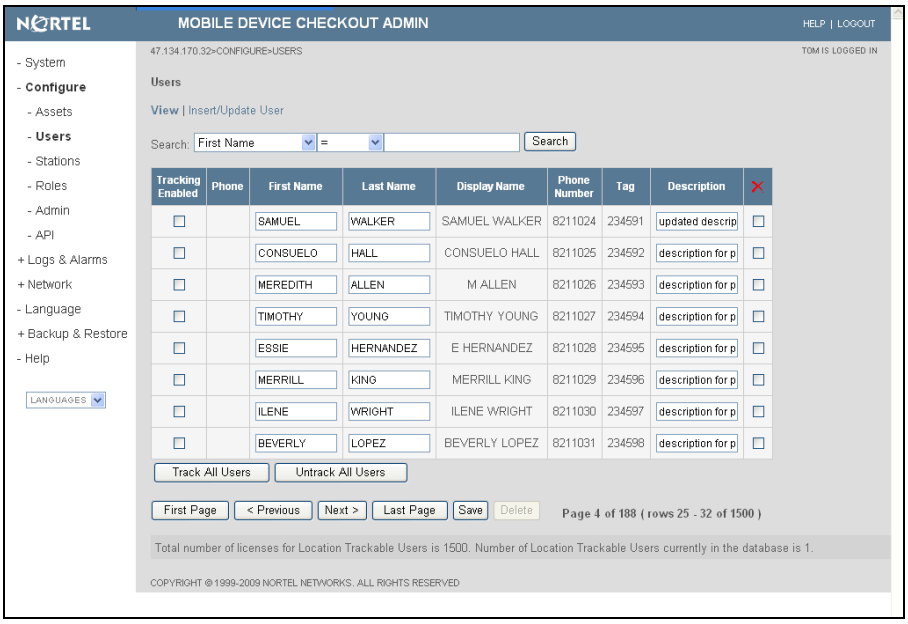


Figure 119: Updating Users from View Assets Screen

If you attempt to navigate away from the View Users screen while there are unsaved changes, a warning dialog will pop up.

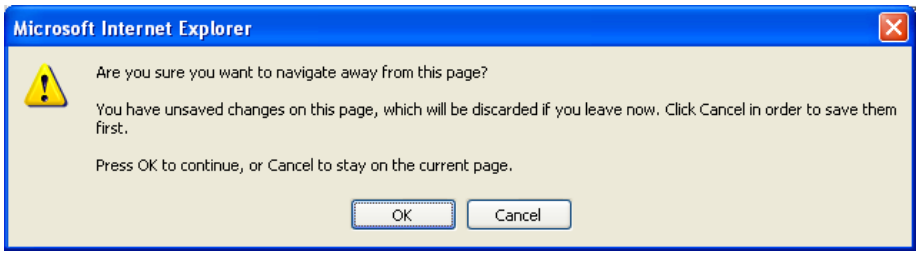


Figure 120: Warning of Unsaved Modifications to Users

7. Click the **Save** button at the button of the table to save all the updates to the users table.
6. The View screen will be refreshed and the latest users data will be displayed. A successful update message is displayed. You can view the changes you made to the users.

11.5 Update Users from Insert/Update Screen

Description:

This applies to making changes to previously provisioned users on MDC.

Note: Barcode and Tag Type cannot be updated from the Insert/Update screen.

The number of location-tracked users permitted on an MDC is controlled by license. Ensure that you have sufficient licenses for location-tracked users when enabling location tracking. If the licensing information has changed within the last 5 hours, you may need to manually refresh the licensing information using the procedure in Section 7.7 *Update Licensing Information in the* MDC.

WARNING: User information on the MDC Admin GUI must exactly match the user configuration on the call server and must remain synchronized. Any mismatch of information will impair service.

WARNING: With CS 1000 call servers, the Get Display Name button will not be able to retrieve user data from the call server if there are any the call server administrators or applications (including MDC) using backup or similar activities at the same time. If this condition cannot be avoided, the MDC administrator has the option to manually enter the user data when the Get Display Name button is unable to retrieve this data. The Get Display Name button is not available when the user is on a CS 2100 call server.

Required information:

- Users which need to be updated identified by tag number
- Updated information for user: Phone Number, Display Name, First Name, Last Name, Description, or Tracking Enabled Status.

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Users** from either the main task area or the Configure submenu on the left navigation menu.
4. The Users screen appears. The main Users screen is the View screen, which displays a list of users in a table format. On a newly installed MDC, there will initially be no users to display.
5. Click **Insert/Update User** from the Users main task working area to update a user on the MDC.
6. The Insert/Update User screen appears. The Insert/Update User screen will look different depending on which call server is integrated with MDC:
    - If the call server is CS 1000, the Insert/Update User screen has a Get Display Name button.
    - If the call server is CS 2100, the Insert/Update User screen does not have a Get Display Name button

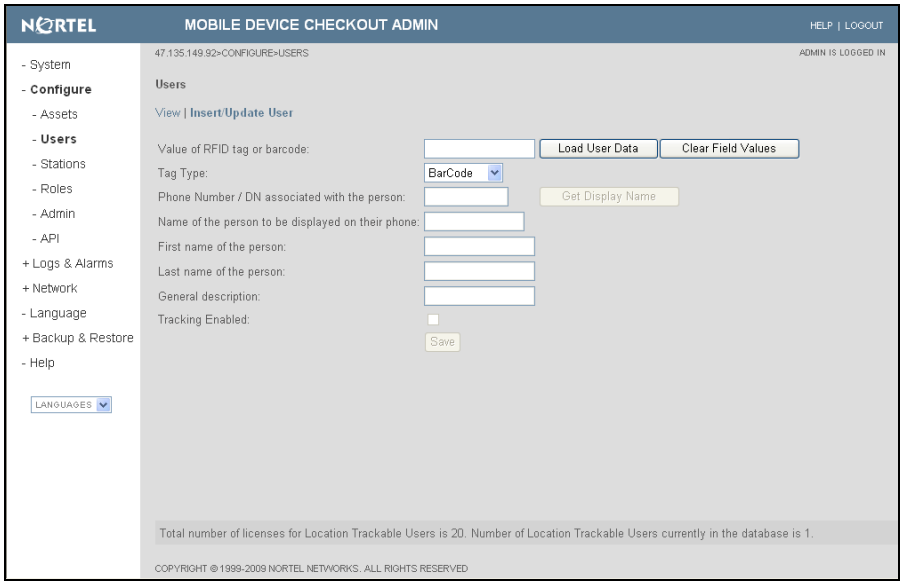


Figure 121: Insert/Update User Screen of MDC Admin GUI (with Get Display Name button)

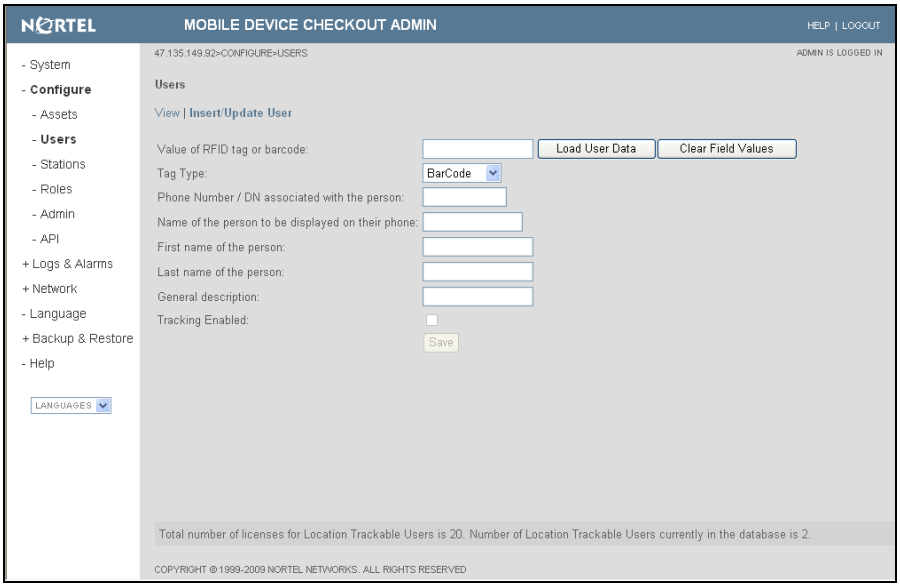


Figure 122: Insert/Update User Screen of MDC Admin GUI (without Get Display Name button)

7. Enter the **Value of RFID tag or barcode** associated with the user's employee badge for which you want to make changes. Choose one of the following two methods to enter this information into the MDC:
    - Using the barcode reader:
        - Place the cursor in the text box for Value of RFID tag or barcode.
        - Use the barcode reader to scan the barcode/RFID on the user's employee badge. This will read and type the barcode/RFID digits into the text box automatically.
    - Manually read and type barcode/RFID digits into the text box.
8. Click **Load User Data** button.
    - For barcodes/tags already provisioned to a user, this will retrieve the information from the MDC database about this user and display it on the screen. This is the expected behavior if an existing user is being modified.

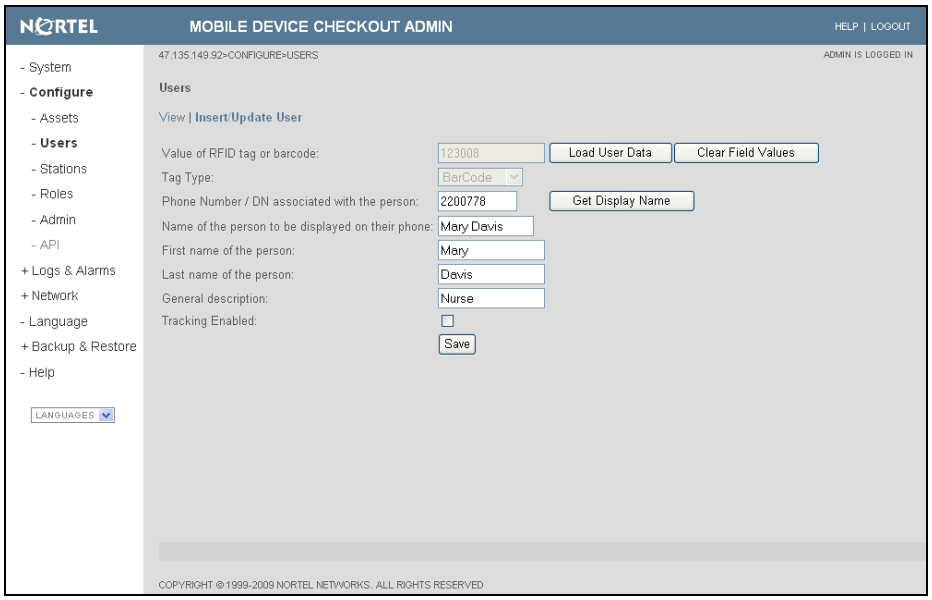


Figure 123: Load User Data for existing User (with Get Display Name button)

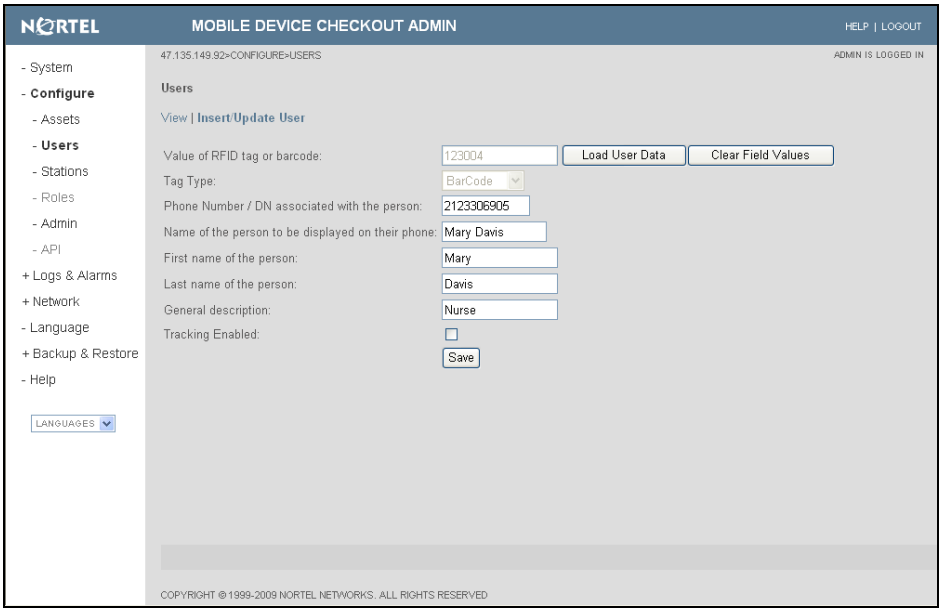


Figure 124: Load User Data for existing User (without Get Display Name button)

- For barcodes/tags which are not known, a message will be displayed indicating no user found for tag value. This is not the expected behavior if an existing user is being modified. If this occurs, make sure the barcode of the user's employee badge has been entered correctly and press the **Load User Data** button again.
- If this barcode/tag has been assigned to an asset, an error message will popup.

9. The following fields can be updated from the Insert/Update screen. The DN and Display name must match with what has been provisioned in the call server. Note: Manually entering information into this field does not change the call server configuration:

a. **Phone Number/ DN associated with the person:** This is the directory number associated with the user.

- If applicable, type in the new phone number/DN for the user. For CS 2100, the phone number specified must be the full 10 digit DN, even if extension dialing is supported.
- If using a CS 1000 call server only, click the **Get Display Name** button. This will trigger the MDC to retrieve this user's phone information from the call server. Retrieving information from the call server will help to ensure the MDC data matches the call server configuration.
  - After a few moments, the following retrieved information should be displayed on the screen:
    - Name of the person to be displayed on their phone
    - First name of person
    - Last name of person

    Verify that this is the user information which should be associated with the employee tag number entered.

    If you get a pop message indicating the MDC was unable to retrieve the data, this indicates you have either entered an unknown DN/phone number OR there was no display name associated with the phone number. Ensure the **Phone Number/DN** is correct and click the **Get Display Name** button again. If you are unable to retrieve the data from the call server automatically, you can manually enter the user name information.

b. **Name of the person to be displayed on their phone:** Display name assigned to the user in the call server. If using CS 1000 call server, the display name can be automatically retrieved from the call server using the Get Display Name button and the procedure described in step a above.

c. **First name of the person**: This is a text field containing the first name of the user. If using CS 1000 call server, the display name can be automatically retrieved from the call server using the Get Display Name button and the procedure described in step a above.

d. **Last name of the person**: This is a text field containing the last name of the user. If using CS 1000 call server, the display name can be automatically retrieved from the call server using the Get Display Name button and the procedure described in step a above.

e. **General Description:** This is a general description text for the user.

f. **Tracking Enabled**: This field is a check box that indicates whether the user is RF location tracked or not.

- The number of location-tracked users permitted on an MDC is controlled by license. If there are no available location-tracked user licenses, a popup dialog will appear to warn the user if they try to check the Tracking Enabled box.
- Tracking enabled cannot be disabled while a location-tracked user has an asset checked out.
- For convenience, this field can be enabled when a non-location-tracked user has an asset assigned; however, location tracking does not take effect until the next time the user checks out an asset. The phone icon associated with the user will remain a gray non-tracked phone icon to indicate that the user is not currently being location tracked (even though they have tracking enabled).

10. Click **Save** to save the modifications for the asset into the MDC database.

    If you see an error popup dialog indicating the update failed because the phone number already exists:

a. You may have inadvertently entered a phone number/DN already associated with another employee tag number. Type in the correct the Phone number/DN associated with this person and click **Get Display Name** again if the asset is on a CS 1000 call server.

b. You may have inadvertently associated the wrong employee number with a phone number in a previous step. You should click **View** to return to the View screen and delete the incorrect entry from the View screen (see Section 11.8 *Delete Users*). You will be prompted by a popup dialog to confirm that you want to leave the Insert/Update User screen without saving the changes. Click **OK**.

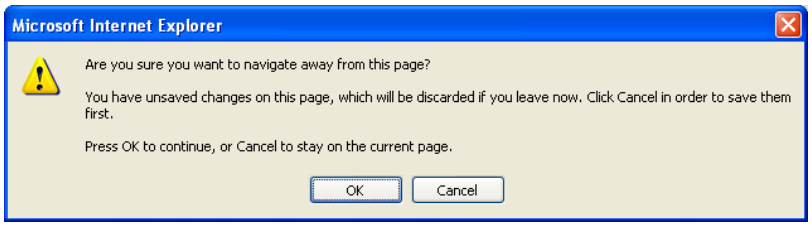


Figure 125: Unsaved Changes Warning

11. Ensure that a successfully updated message is displayed to confirm that the changes were saved. The data fields will be blanked to facilitate inserting or updating another user.

    Click **View** to return to the main Users screen. The View screen will be refreshed and the latest users data will be displayed, including the changes you made to the specific user.

11.6 Enable Location Tracking for All Users

Description:

Use this procedure to enable location tracking for all users.

Note: For convenience, location tracking can be enabled when the user has an asset assigned; however, location tracking does not take effect until the next time the user checks out an asset. In this instance, the phone icon associated with the user will remain a gray non-tracked phone icon to indicate the user is not currently being location tracked

The number of location-tracked users permitted on an MDC is controlled by license. Ensure that you have sufficient licenses for location-tracked users when enabling location tracking. . If the licensing information has changed within the last 5 hours, you may need to manually refresh the licensing information using the procedure in Section 7.7 *Update Licensing Information in the* MDC.

This function is disabled (grayed out) when all users are already enabled for location tracking.

WARNING: It is recommended to save any changes made to users in the View screen prior to enabling location tracking for all users. You will be warned if there are unsaved changes.

Required information:

- None

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Users** from either the main task area or the Configure submenu on the left navigation menu.
4. The Users screen appears. The main Users screen is the View screen, which displays a list of users in a table format. On a newly installed MDC, there will initially be no users to display.

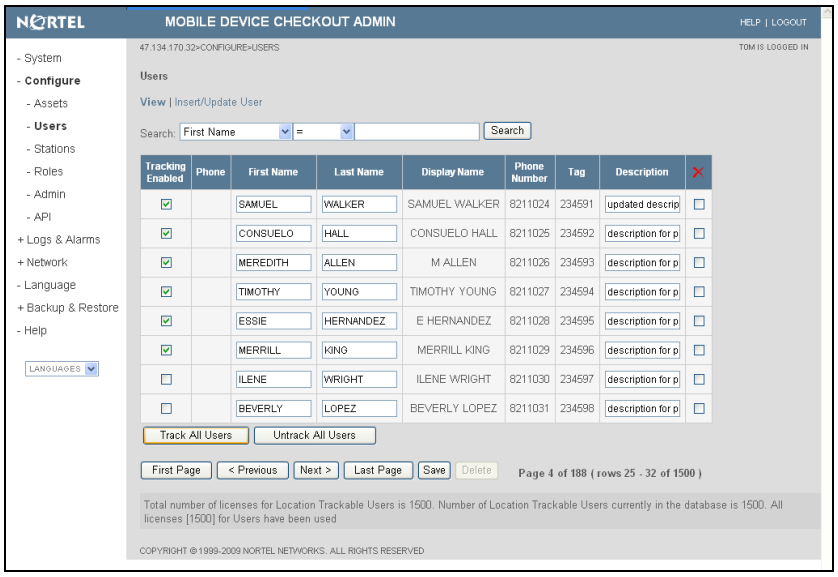


Figure 126: View Users on MDC Admin GUI

5. Click the **Track All Users** button to enable location tracking for all assets. Note: For convenience, location tracking can be enabled when the user has an asset assigned; however, location tracking does not take effect until the next time the user checks out an asset. This button is disabled (grayed out) when all users are already enabled for location tracking.
6. The View screen will be refreshed and the latest users data will be displayed. The Tracking Enabled box is updated for all users.

11.7 Disable Location Tracking for All Users

Description:

Use this procedure to disable location tracking for all users. Note: This will apply only to location-tracking-enabled users that are not currently assigned to an asset.

This function is disabled (grayed out) when all users are already disabled for location tracking.

WARNING: It is recommended to save any changes made to users in the View screen prior to disabling location tracking for all users. You will be warned if there are unsaved changes.

Required information:

- None

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Users** from either the main task area or the Configure submenu on the left navigation menu.
4. The Users screen appears. The main Users screen is the View screen, which displays a list of users in a table format. On a newly installed MDC, there will initially be no users to display.

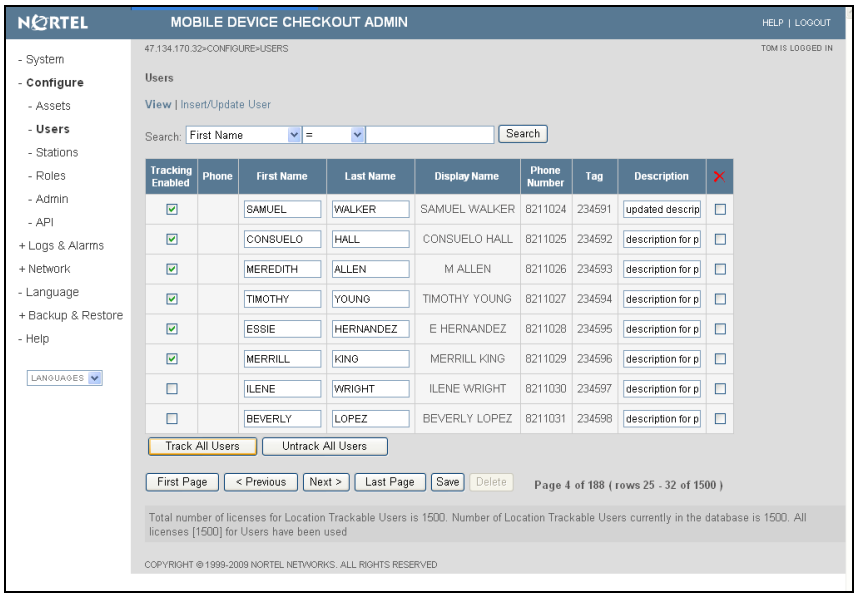


Figure 127: View Users on MDC Admin GUI

5. Click the **Untrack All Users** button to disable location tracking for all users. Note: This will not apply to location-tracked users that currently have an asset checked out. This button is disabled (grayed out) when all users are already disabled for location tracking.

   With a large number of users, it may take up to one minute to untrack all users. A popup dialog will appear to inform the administrator the action is in progress.



Figure 128: Tracking Disabled on all Users

6. The View screen will be refreshed and the latest users data will be displayed. Confirm that the Tracking Enabled box is updated for all users not assigned to assets.

11.8 Delete Users

Description:

Use this procedure to delete users. Users cannot be deleted while they have assets checked out.

WARNING: It is recommended to save any changes made to users in the View screen prior to deleting users. The Save button is enabled when there is an unsaved change.

Required information:

- User that needs to be deleted identified by one of these fields: First Name & Last Name, Display Name, Phone Number, Tag Number, or Description

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Users** from either the main task area or the Configure submenu on the left navigation menu.
4. The Users screen appears. The main Users screen is the View screen, which displays a list of users in a table format. On a newly installed MDC, there will initially be no users to display.

   Note: The **Delete** button, below the users table, does not become enabled until there are entries marked for deletion from the users table.

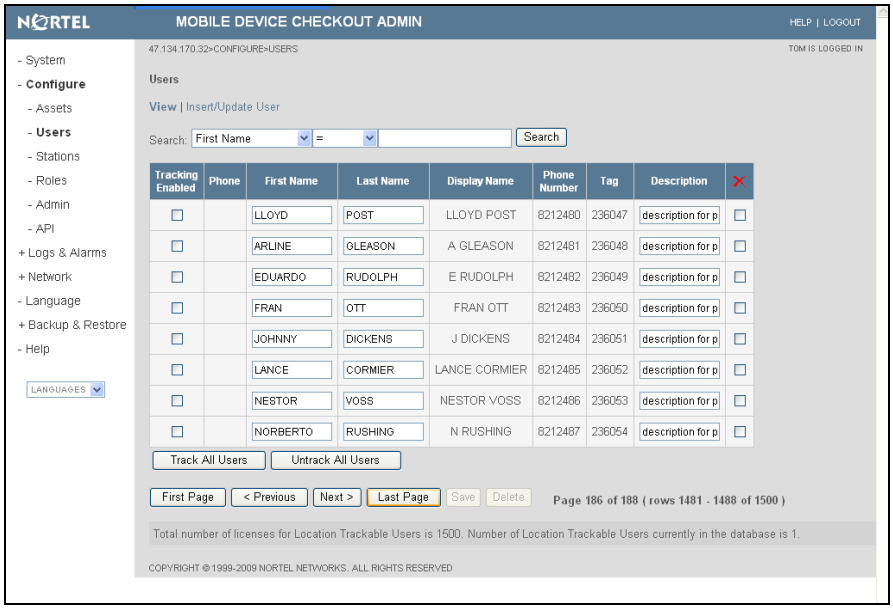


Figure 129: View Users in MDC Admin GUI

5. Locate the table entry of the user you want to remove. See the procedures in View Assets for options to sort and search the users table. Check the box in the **Delete** column (rightmost column in the table) to delete a particular user. Once any users have been marked for deletion from the View Users table, the **Delete** button, below the table, becomes enabled to indicate that there are pending deletions. You may mark multiple users for deletion. If you use the page control buttons, the entries you have marked for deletion may no longer be displayed on the screen.

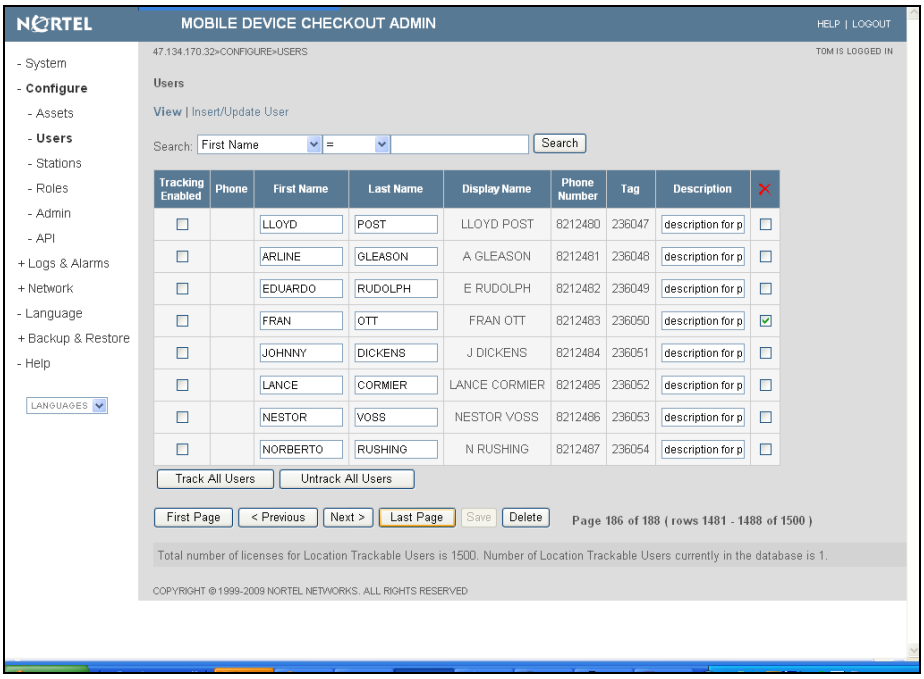


Figure 130: Deleting Users from View Users

If you attempt to navigate away from the View Users screen while there are users marked for deletion, a warning dialog will pop up.

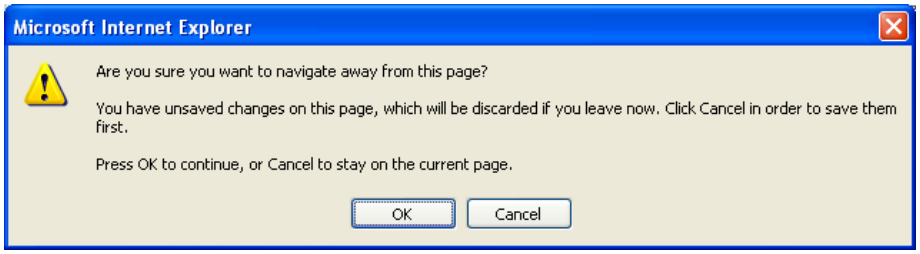


Figure 131: Warning of users marked for Deletion

Note: Users cannot be deleted while they have assets checked out.

6. Click **Delete** button, below the users table, to delete the marked user(s).
7. A delete confirmation popup dialog will appear. Click **OK** to confirm deleting the user(s).

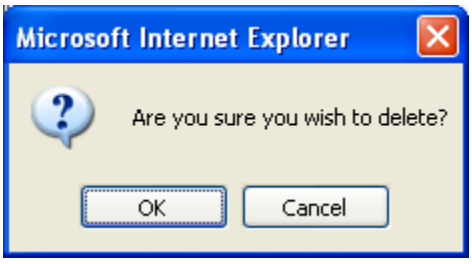


Figure 132: Delete User Confirmation Dialog

8. The View screen will be refreshed and the latest user data will be displayed. The deleted user(s) has been removed from the list of users.

11.9 Bulk loading of Users

Description:

To assist with the coordination of large numbers of assets and users, scripts have been created to take specific formatted files as their input for the purpose of creating, deleting, and, updating of assets and users on the MDC Server. These scripts were designed to synchronize MDC with the information contained in other administrative directories or databases.

This script must be executed on the MDC Server.

WARNING: User information on the MDC must exactly match the user configuration on the call server and must remain synchronized. Any mismatch of information will impair service. The input files used with the bulk loading scripts should be derived from a primary data source used to drive the call server configuration, such as LDAP.

WARNING: The number of location-tracked users and the number of assets permitted on an MDC is controlled by license. Ensure that you have sufficient licenses when using bulk loading scripts.

WARNING: It is strongly recommended that a manual MDC backup be performed prior to using bulk loading of assets and users. In the event of errors or the use of out-of-date input, a backup will permit the user to restore the current view of users and assets into the MDC database.

WARNING: A bulk loading script cannot operate at the same time as any backup or restore activities or another bulk loading script.

Note:

- The bulk loading is intended to be used to coordinate large numbers of assets and users for the purposes of adding, deleting and synchronizing information. The input files are expected to specify all assets/users needed by the MDC Server, thus:
  - Users and assets are designated either as manually added through the MDC Administration GUI or added via bulk loading scripts. The bulk loading scripts will update or delete only those users and assets that were originally added through bulk loaded scripts. They will not update nor modify users or assets that were originally manually added through the MDC Administration GUI.
  - If a user/asset is present in the bulk loading input file but not present in the MDC database, this will be interpreted as an addition of user/asset by the scripts. There must be available licenses on the MDC Server for the addition of any new tracking-enabled users and new assets.
  - If an existing user/asset in the MDC database is not present in the bulk loading input file, this will be interpreted as a deletion of user/asset by the scripts.
  - If a user/asset is present in both the input file and the MDC database, any field associated with the user/asset will be updated, if needed, based on the information in the input file.
- The input files are delimited. The default delimiter is a comma. However, optionally, the user can specify another delimiter character. If the delimiter is a tab, then type (CTRL_V CTRL_I) to put in the delimiter on the command line in UNIX.
- The scripts will go through the following steps:
  - Validate the format of the input file. The scripts automatically check the input file for correct format and will inform the user if formatting errors are discovered. Unfortunately, the scripts cannot determine whether the data is correct.
  - Verify that there are sufficient licenses for the changes (taking into account the additions and deletions).
  - Apply the changes to the MDC database: additions, updates and deletions.

- Data validation is performed by the MDC database and invalid input will be skipped.
- Upon completion, the script will summarize what actions were taken:
  - how may new assets/users were added
  - how many assets/users were deleted
  - how many assets/users were updated
  - how many records were rejected from the input file
- The scripts will issue a start and end log with severity INFO. Failure logs with severity CRITICAL will be generated if needed.
- The fields of the user input file are fixed as shown below. The General Description field is optional. Additional data restrictions may apply depending on the call server. For example, for CS 2100, the phone number specified must be the full 10 digit DN, even if extension dialing is supported. The user input file shown below is compatible with CS 1000 call server:

Barcode	Tag Type	Last Name	First Name	Phone Number	Tracking Enabled	General Description
5572398	Barcode	BOURNE	HARRIET	33169	1	Leader Radiology Team
5507898	Barcode	BARRY	RAJAN	33543	1	ENT Doctor
5794344	Barcode	DAINTRY	EUGENE	35420	1	IC Nurse
5084671	Barcode	FELSKE	JOHANNA	57566	1	Social Worker
5498239	Barcode	JONES	ANGELO	57083	1	Audiologist

- The script is **LoadUserScript.php** located in **/opt/nortel/ebs/mdc/backup**

Required information:

- IP address of the MDC Server
- Unix userid and password
- User input file formatted as described above

Steps:

- Example invocation:

  php -f LoadUserScript.php -- -fOSM.txt -d' '

  where -f parameter is the input file (OSM.txt).

  where -d parameter is the delimiter. When the delimiter is a tab (CTRL_V CTRL_I) will specify the tab delimiter on the UNIX command line.

- Sample of output from another invocation:

  php -f LoadUserScript.php -- -f/tmp/sandra/persons.csv

  where -f parameter is the input file (/tmp/sandra/persons.csv).

  where there is no -d parameter used to specify the delimiter. This parameter is optional, as a comma is the default delimiter.

  Example:

  [root@sc-mdc-2 backup]# php -f LoadUserScript.php -- -f/tmp/sandra/persons.csv

  Validating Data...

```
Validating Licenses...
Applying Data File...
|XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX____| 93%

[root@sc-mdc-2 backup]# php -f LoadUserScript.php -- -f/tmp/sandra/persons.csv
Validating Data...
Validating Licenses...
Applying Data File...
|XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX| 100%
Done
2000 record(s) added
0 record(s) updated
0 record(s) rejected
0 old record(s) deleted
Done.
```

12 Managing Roles

MDC can optionally be configured to support role based checkout. Like users, roles are meant to represent people in an organization. Whereas users map to specific employees, roles represent functions or capacities within an organization. For example, in a hospital, there might be roles such as “Cardiologist on call” or “Social Worker on call”. During checkout, a user can checkout a phone and [optionally] a role.

Depending on the role and organization, multiple individuals may assume the same role during a shift or only a single person may be assigned to a role per shift. In either case, with the timing of arrivals and departures in a shift change, there may be an overlap of time when the person arriving for a shift may assume a role before the person currently in the role has left. This overlap may be a mandatory procedure to ensure smooth transitions. Therefore, multiple users are permitted to be associated with a role. However, each user can be associated with a maximum of one role (or no role). There is a visual indicator in the View Users screen to indicate when a user has a role checked out on their phone.

When a role phone number is dialed different people may be reached. If Multiple Call Ringing (MCR)/Multiple Call Arrangement (MCA) in used, if there is already a role call in progress with the phone of an individual in the role when the role DN is called again, the other phones with the role assigned will still ring. If multiple people may be assigned the same role (even for a short duration), it is strongly recommended that the line mode be MCR/MCA for all the roles and users on the call server. The type of the call arrangement is part of the call server integration information on a per MDC Server basis. From a call server provisioning point of view, a role must comply with the same configuration requirements as the users of MDC.

Whether the personal phone number is assigned during checkout or “role only” checkouts are performed can be configured on a per MDC Station location basis. Phone assets will need to have multiple phone lines configured to support assignment of both the role phone number and the user personal phone number if this configuration is permitted. The assignment of phone number (personal or role) to specific line numbers on the phone is also configurable on a MDC Server basis. This assignment of phone number to phone lines only applies when both the role and personal phone numbers are assigned during checkout. If only one phone number (either personal phone number or role phone number) is assigned during checkout, this single number is always assigned to the primary line on the phone. There is a visual indicator in the View Asset screen to indicate when a role has been checked out on a phone.

“Role only” checkouts restrict any checked out of assets to assigning only the role phone number to the primary line of the phone. The only exception to this “role only” assignment could occur if the “No Role” role is used. When a user selected the “No Role” role when “Role Only” assignments are in effect, then the personal phone number of the user will be assigned to the primary line of the phone.

The support of roles is controlled by licensing. The role selection is accessed via the MDC Stations. To enable the roles functionality on an MDC Server, the number of role licenses must match (or be greater than) the number of MDC Station licenses. The MDC Admin GUI role administration screens are not accessible if there are no role licenses. If there is insufficient number of role licenses or the role Try-n-Buy licenses have expired, the Role administration screens will no longer be accessible and the role selection screens will no longer appear on any MDC Stations. However, any existing data is retained in the database and can be reactivated when the role licensing problem is corrected. If the licensing information has changed within the last 5 hours, you may need to manually refresh the licensing information using the procedure described in Section 7.7 *Update Licensing Information in the MDC.* Refer to Section 7 *MDC Licensing and Keycode Retrieval System (KRS)* for more information on MDC licensing.

A summary of how to enable roles is described in Section 12.1 *Overview of Enabling Roles*.

Note: Deploying new or modified role configuration may be service affecting. It is recommended that role configuration changes be made between shifts or during maintenance periods to minimize service impact.

Note: Location Tracking is not supported for roles. Location Tracking can only be optionally enabled for users (and assets).

12.1 Overview of Enabling Roles

This is a high level overview of the steps to enable roles on an existing MDC server:

- Provision the role DNs on the call server
- [Optional] Ensure the WLAN handsets being used for MDC are configured with two lines if both roles and personal DNs will be used when the phones are checked out by users.
- If multiple people may be assigned the same role (even for a short duration), it is strongly recommended that the line mode be MCR/MCA for all the roles and users on the call server.
    - SCR/SCA permits only a single active call on a phone number. MCR/MCA permits additional calls on a phone number even when there is already an active call on that phone number. In the case of MCR/MCA, if a second call is made to the phone number, the other unused phones will ring. The line mode is important when there are multiple phones with the same phone number. Multiple phones may be assigned the same phone number when the user has permanent phone in addition to their mobile phone. Multiple phones may be assigned the same phone number when roles are being used.
- Update MDC Server with a license that enables roles. See Section 7 *MDC Licensing and Keycode Retrieval System (KRS)* for the details.
- [Optional] Update configuration of which lines on the handset will be assigned role DN and personal DN when both DNs are assigned during checkout. Updating is only needed if both lines will be assigned during checked out and the default settings are not acceptable. The default assignments are:
    - On CS 1000 call server, the role DN will be assigned to line 0 and the personal DN to line 1 of the handset during checkout. See Section 9.1 *Configure and Test Connection to CS 1000 from MDC Server* for details on how to change the default settings.
    - On CS 2100 call server, the role DN will be assigned to line 1 and the personal DN to line 2 of the handset during checkout. Section 9.2 *Configure and Test Connection to CS 2100 from MDC Server* for details on how to change the default settings.

At this point, the administrator can proceed to configure the roles, role categories and role templates using the procedures in this section. The list of procedures described in this section is:

- Overview of Enabling Roles (this section)
- Roles procedures:
    - Insert New Roles
    - 12.3View Roles
    - 12.4Updating Roles from View Screen
    - 12.5Updating Role from Insert Role Screen
    - 12.6Delete Role
- Categories procedures:
    - 12.7Grouping Roles into Categories
    - 12.7.1Create a New Category
    - View a Category

- 12.7.3Modify a Category
- 12.7.4Delete a Category

- Templates procedures:
  - 12.8Role Template
  - 12.8.1Create a New Template
  - 12.8.2View a Template
  - 12.8.3Modify a Template
  - 12.8.4Delete a Template

Once the roles templates are defined, the administrator can:

- Associate a role template with a MDC Station location. This will enable any MDC Station with that MDC location to offer role assignment via the configured role template. A role template can be associated with one or more MDC Station locations.
- Designate a MDC Station location as “role only”.

See Section 13.6 *Insert Station Location* and Section 13.7 *Modify Station Location* for further details.

Note: Deploying new or modified role configuration requires a reboot of the MDC Station which is service affecting. It is recommended that role configuration changes be made between shifts or during maintenance periods to minimize service impact.

The following sections describe the visual indicators when roles have been assigned on users and assets:

- Section 10.3 View Assets
- Section 11.2 View Users

WARNING: The support of roles is controlled by license. Ensure that you have sufficient licenses for roles. If the licensing information has changed within the last 5 hours, you may need to manually refresh the licensing information using the procedure described in Section 7.7 *Update Licensing Information in the MDC.* Without sufficient licenses for roles, the administrative screens relating to roles will not be accessible. Refer to Section 7 *MDC Licensing and Keycode Retrieval System (KRS)* for more information on MDC licensing.

12.2 Insert New Roles

Description:

This procedure describes adding a new role to the MDC.

The role configuration MUST already be provisioned on the call server.

WARNING: Role information on the MDC Admin GUI must exactly match the role configuration on the call server and must remain synchronized. Any mismatch of information will impair service. If changes have been made to the call server, update the associated roles in MDC.

WARNING: The Get Display Name button will not be able to retrieve role data from the call server if there are any call server administrators using backup or similar maintenance activities at the same time. If this condition cannot be avoided, the MDC administrator has the option to manually enter the role data when the Get Display Name button is unable to retrieve this data. The Get Display Name button is not available when the user is on a CS 2100 call server.

Required information:

For each role added to MDC:

- Role name: This is name of the role. It must be unique as it will be used to identify this role on the MDC Admin GUI.
- Role Button Line 1: This is the first line of the label for this role which would be displayed to the user during role selection.
- [Optional]Role Button Line 2: This is the second line of the label for this role which would be displayed to the user during role selection.
- Phone number. This must be unique across all roles.
- Display name. This is the display provisioned on the call server and displayed on the handsets.
- [Optional] Brief text description of the role

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Roles** from either the main task area or the Configure submenu on the left navigation menu.
4. The Roles screen appears. The main Roles screen is the View screen, which displays a list of roles in a table format. On a newly installed MDC, there will initially be no roles to display.

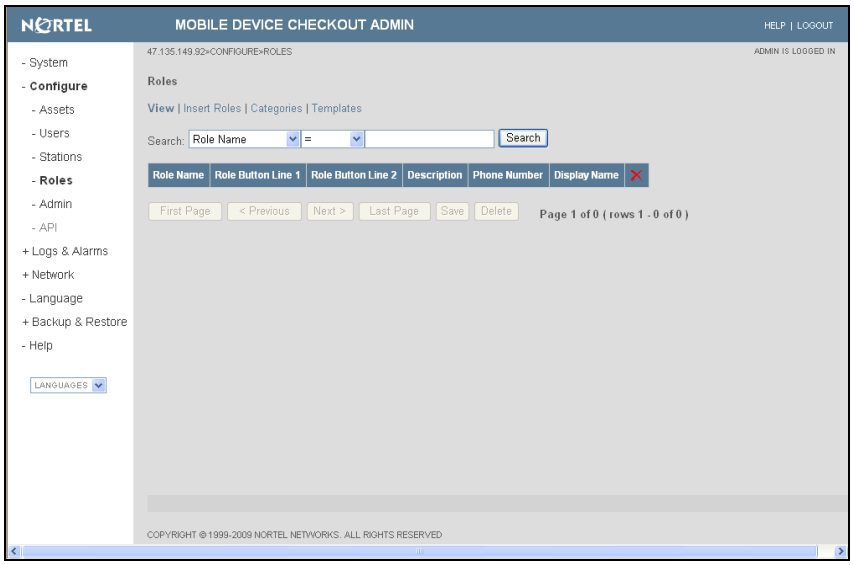


Figure 133: View Roles Screen without Roles

5. Click **Insert Roles** from the Roles main task working area to add a role to MDC.
6. The Insert Roles screen appears. The Insert/Update Roles screen will look different depending on which call server is integrated with MDC:
    - If the call server is CS 1000, the Insert/Update Roles screen has a Get Display Name button.

- If the call server is CS 2100, the Insert/Update Roles screen does not have a Get Display Name button.

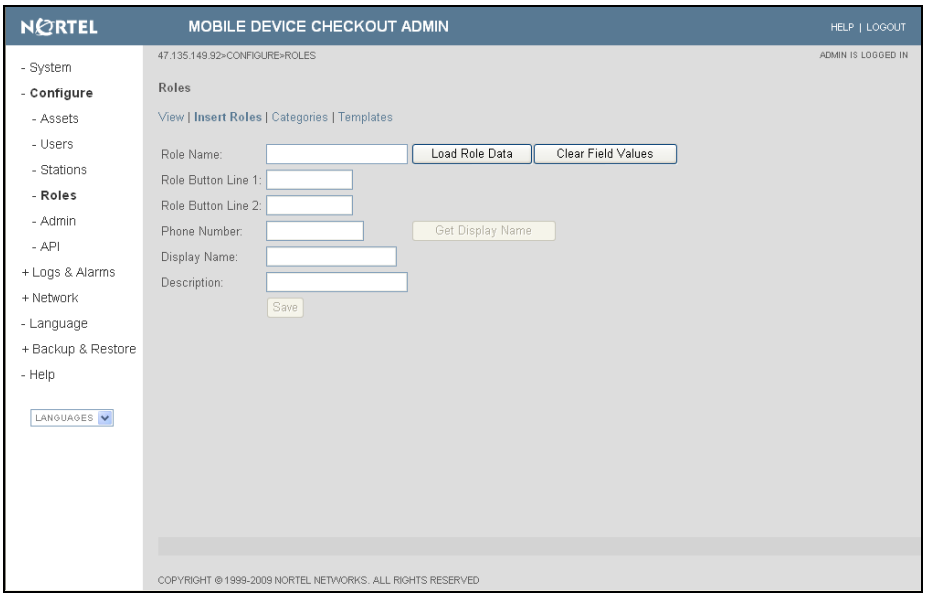


Figure 134: Insert Roles Screen (with Get Display Name button)

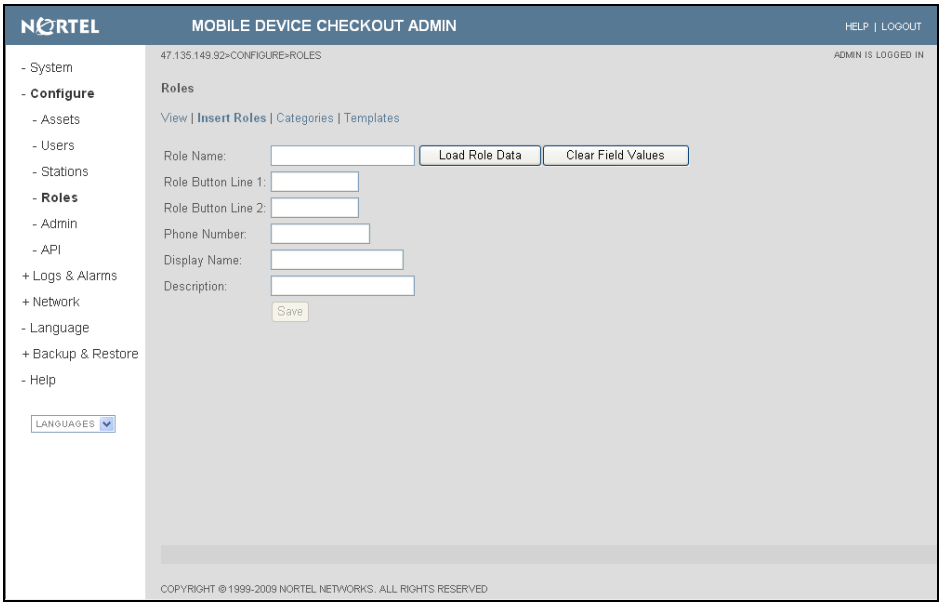


Figure 135: Insert Roles Screen (without Get Display Name button)

7. To insert a new role, use the information which has been provisioned in the call server. Enter in the following parameters:
    a. **Role Name**: This is name of the role. It must be unique as it will be used to identify this role on the MDC Admin GUI.

b. Click the **Load Role Data** button.

- For a role which is not known (i.e. new), a message will appear on the message banner indicating that no role has been found with the given role name. This is the expected behavior when a new role is being added. The text fields will become editable to permit the input of the role information.
- For roles already provisioned, this will retrieve the information from the MDC database about this role and display it on the screen. This is not the expected behavior if a new role is being added. If this occurs, make sure the role name has been entered correctly and all roles have unique names.

8. Type in **Role Button Line 1** and **Role Button Line 2**. These two fields allow the administrator to create the label for this role as it will appear to the user on the MDC Station screen during role selection.
9. Type in the **Phone Number.** This is the directory phone number associated with this role. For CS 2100, the phone number specified must be the full 10 digit DN, even if extension dialing is supported.
10. Only if the call server integrated with MDC is a CS 1000 (i.e. the Insert/Update User screen has a Get Display Name button) do these steps:
    - Click the **Get Display Name** button. This will trigger the MDC to retrieve the role information from the call server
    - After a few moments, the retrieved Display Name information should be displayed on the screen.
    - Confirm that this is the name of the role being added.

    If you have entered an unknown phone number or if there was a communication problem, a popup message dialog will appear. Check and correct the **Phone Number** if needed. Click **Get Display Name** again.



Figure 136: Unable to retrieve data for Requested DN.

If you have the correct phone number, this message may indicate there is no display name configured against the phone number on the call server or communication problems persist. You can manually enter the role display name. Note: Manually entering information into these fields will not change the call server configuration:

- **Display Name**: Name of the role which will be displayed on the phone. This is the Display name assigned to the role in the call server. Manually entering information into this field does not change the call server configuration.

11. Only if the call server integrated with MDC is a CS 2100 (i.e. the Insert/Update User screen does not have a Get Display Name button) do the following steps:
    - Type in the **Display Name**: Name of the role which will be displayed on the phone. This is the Display name assigned to the role in the call server. Manually entering information into this field does not change the call server configuration
12. Type in the **Description** of this role. This is a brief text description of the role.

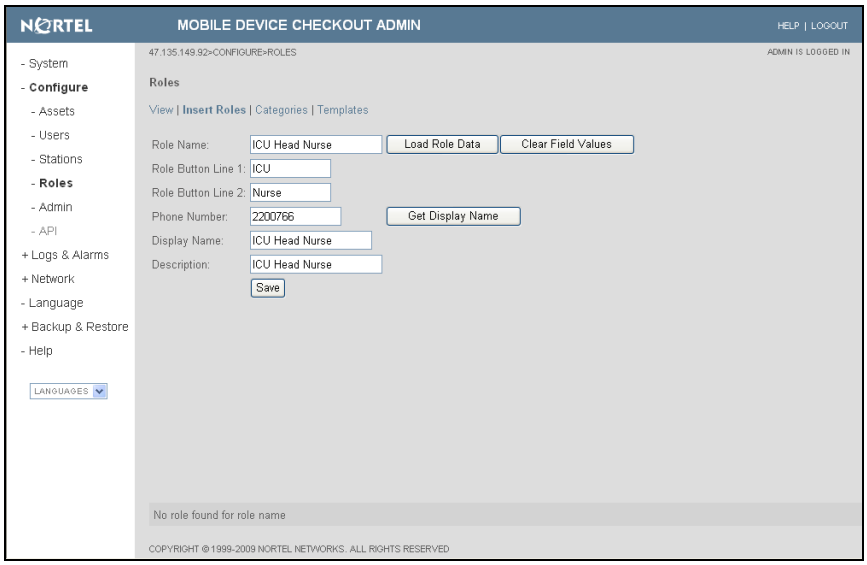


Figure 137: Data filled Insert Roles Screen (with Get Display Name button)

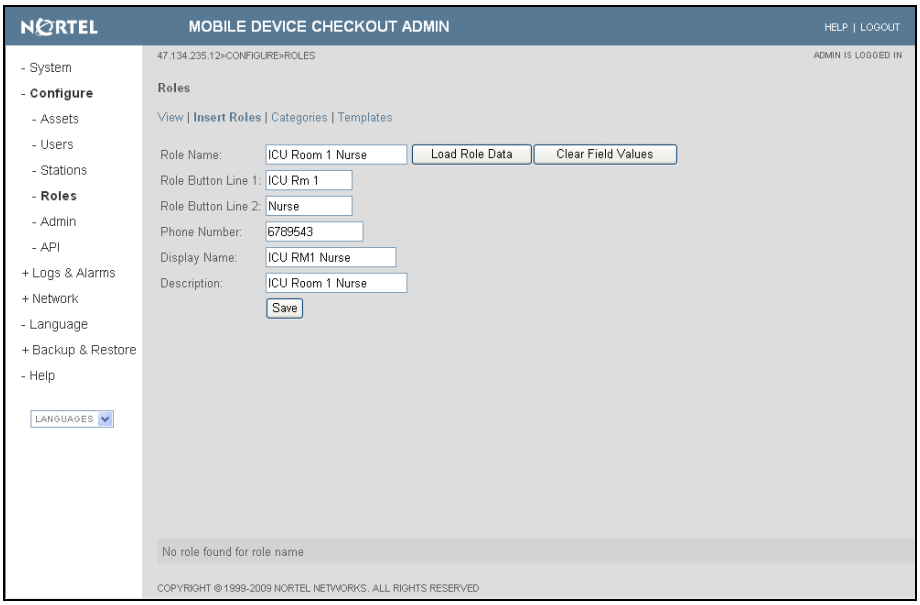


Figure 138: Data filled Insert Roles Screen (without Get Display Name button)

13. Click **Save** to insert the displayed role into the MDC database.
14. Ensure that a successfully inserted message is displayed to confirm that the role was added. The data fields will be blanked to facilitate inserting the next role.
15. When you have completed adding all the roles, click **View** from the main task area menu. The main Roles screen is the View screen, which displays a list of roles in a table format. You should see all the roles you have just added to the MDC displayed.

12.3 View Roles

Description:

This procedure describes how to view the list of roles from the MDC Admin GUI.

Required information:

- None

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Roles** from either the main task area or the Configure submenu on the left navigation menu.
4. The Roles screen appears. The main Roles screen is the View screen, which displays a list of roles in a table format. On a newly installed MDC, there will initially be no roles to display.

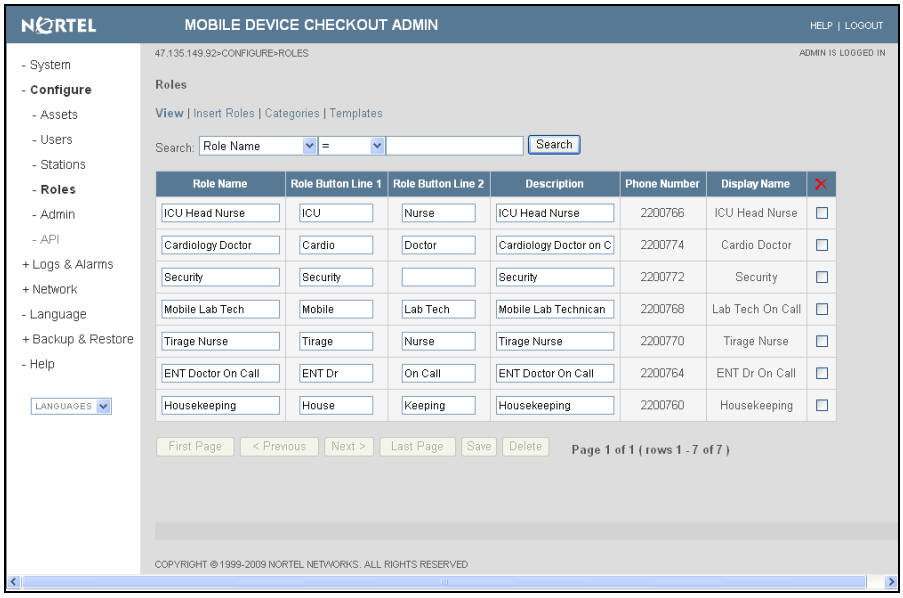


Figure 139: View Roles on MDC Admin GUI

The columns in the roles table are:

- Role Name: Text field with the name of the role displayed to the user during role selection.
- Role Button Line 1: This is the first line of the label for the role which is displayed during role selection.
- Role Button Line 2: This is the second line of the label for the role which is displayed during role selection.
- Description: A text description of the role.
- Phone Number: Directory number associated with the role
- Display Name: Display name assigned to the role in the call server.
- Delete: This field is checked to delete the role from the MDC.

When there are a large number of roles in the list, only some of the roles will be displayed on the screen at a time. This is considered a “page.” The page number is shown on the screen out of the total number of available pages at the bottom of the table to help orient the user within the view roles table. The equivalent row information for these entries in the roles table is also given in parentheses.

There are a number of options to view other roles not displayed on the screen:

- Paging
- Sort
- Search

See Section 5.2.4 *MDC Admin GUI Paging, Sort, and Search* for a description of paging, sorting and searching and an explanation of how to use these features.

12.4 Updating Roles from View Screen

Description:

This applies to making changes to previously provisioned roles on MDC.

Note: Only some fields that can be updated from the View Roles screen.

Note: if you modify a role label (i.e. Role button Line 1 or Role button Line 2) being used in a role template deployed to a MDC Station, you will need to reboot the MDC Station before the updated role label will take effect on the MDC Station.

Required information:

- Role which needs to be updated identified by one of these fields: Role Name, Role Button Line 1, Role Button Line 2, Phone Number, or Display Name
- Updated information for role: Role Name, Role Button Line 1, Role Button Line 2, or Description

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Roles** from either the main task area or the Configure submenu on the left navigation menu.
4. The Roles screen appears. The main Roles screen is the View screen, which displays a list of roles in a table format. On a newly installed MDC, there will initially be no roles to display.

   Note: The **Save** button, below the roles table, does not become enabled until there are changes made to entries in the roles table.

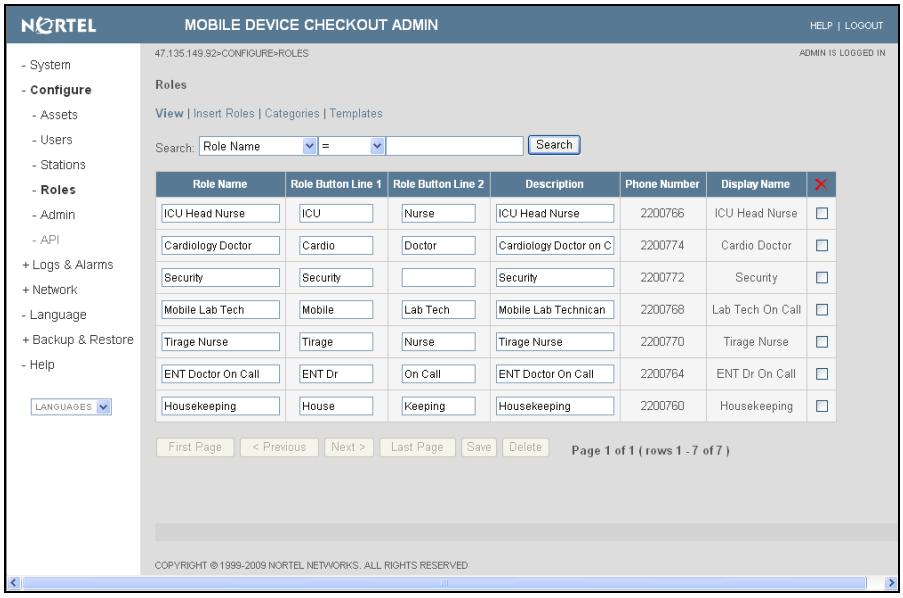


Figure 140: View Roles in MDC Admin GUI

5. Locate the table entry of the role you want to modify. See the procedures on View Roles for options to sort and search the roles table. The following fields can be updated from the View screen:

    a. **Role Name**: This is name of the role. It must be unique as it will be used to identify this role on the MDC Admin GUI.

    b. **Role Button Line 1** & **Role Button Line 2**: These two fields allow the administrator to create the label for this role as it will appear to the user during role selection.

    c. **Description**: This is a text description of the role.

    Once changes have been made to fields in the View Roles table, the **Save** button, below the table, becomes enabled to indicate that there are role entries which have been modified. You can modify multiple entries in the View Roles table. If you use the page control buttons, the entries you have modified may not be displayed on the screen.

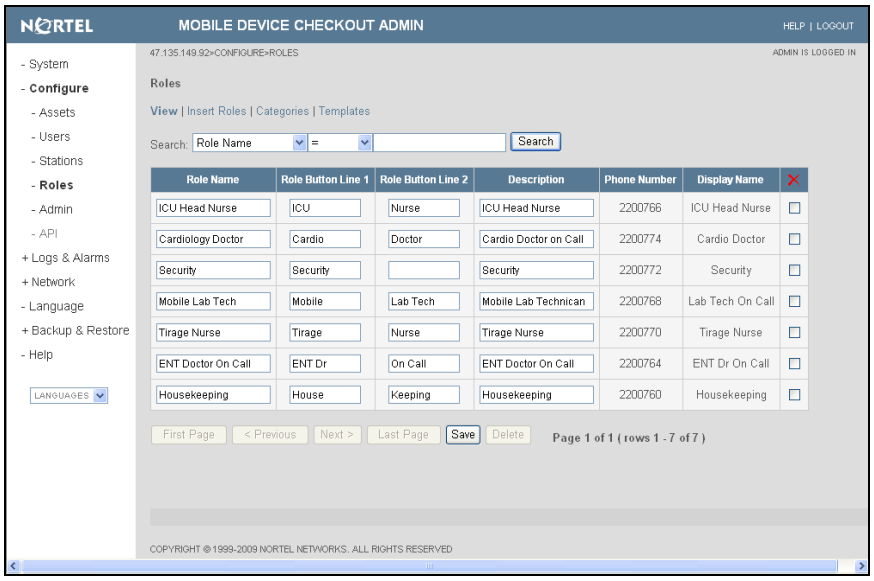


Figure 141: Updating Roles from View Roles Screen

If you attempt to navigate away from the View Roles screen while there are unsaved changes, a warning dialog will pop up.

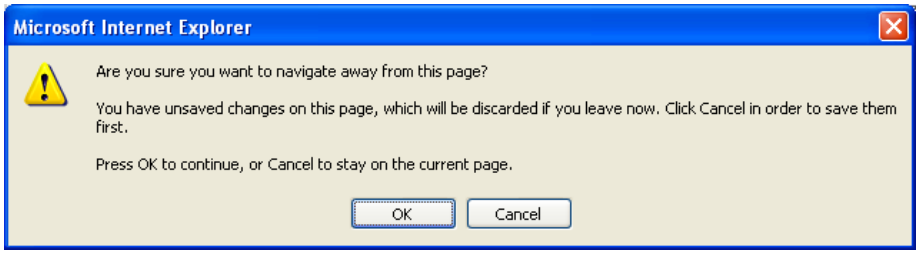


Figure 142: Warning of Unsaved Modifications to Roles

6. Click the **Save** button at the button of the table to save all the updates to the Roles table.

   The View screen will be refreshed and the latest Roles data will be displayed. A successful update message will be displayed. You may verify that the changes were made to the roles. If you use the page control buttons, the entries you have modified may not be displayed on the screen.

7. If you have modified a role label (i.e. Role Button Line 1 or Role Button Line 2) being used in a role template deployed to a MDC Station, you will need to reboot the MDC Station before the updated role label will take effect on the MDC Station. If you are uncertain of which MDC Stations are impacted, it is recommended that all MDC Station be rebooted during a suitable maintenance period once all the role related configuration changes have been completed. See Section 13.11 *Reboot All MDC Stations* or Section 13.10 *Reboot MDC Station* for the detailed procedure.

12.5 Updating Role from Insert Role Screen

Description:

This applies to making changes to previously provisioned roles on MDC.

Note: if you modify a role label (i.e. Role Button Line 1 or Role Button Line 2) being used in a role template deployed to a MDC Station, you will need to reboot the MDC Station before the updated role label will take effect on the MDC Station.

WARNING: Role information on the MDC Admin GUI must exactly match the role configuration on the call server and must remain synchronized. Any mismatch of information will impair service.

WARNING: The Get Display Name button will not be able to retrieve role data from the call server if there are any call server administrators using backup or similar activities at the same time. If this condition cannot be avoided, the MDC administrator has the option to manually enter the role data when the Get Display Name button is unable to retrieve this data. The Get Display Name button is not available when the user is on a CS 2100 call server.

Required information:

- Role name of role which needs to be updated
- Updated information for role: Role Name, Phone Number, Display Name, or Description.

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Roles** from either the main task area or the Configure submenu on the left navigation menu.
4. The Roles screen appears. The main Roles screen is the View screen, which displays a list of roles in a table format. On a newly installed MDC, there will initially be no roles to display.
5. Click **Insert Roles** from the Roles main task working area to update a role on the MDC.
6. The Insert Roles screen appears. The Insert/Update Roles screen will look different depending on which call server is integrated with MDC:
    - If the call server is CS 1000, the Insert/Update Roles screen has a Get Display Name button.
    - If the call server is CS 2100, the Insert/Update Roles screen does not have a Get Display Name button.

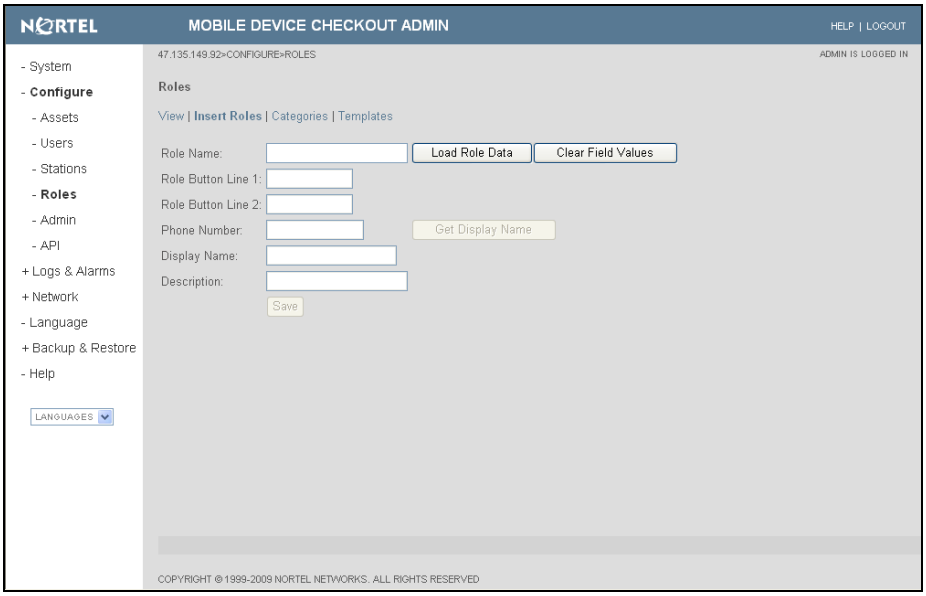


Figure 143: Insert Roles Screen of MDC Admin GUI (with Get Display Name button)

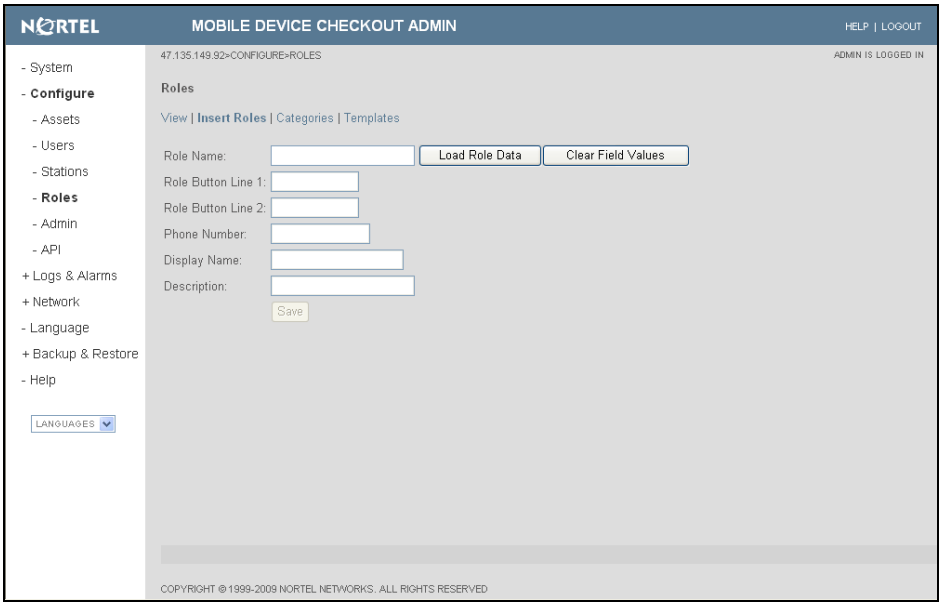


Figure 144: Insert Roles Screen of MDC Admin GUI (without Get Display Name button)

7. Enter the **Role Name** associated with the role for which you want to make changes.
8. Click the **Load Role Data** button.
    - For roles already provisioned, this will retrieve the information from the MDC database about this role and display it on the screen.

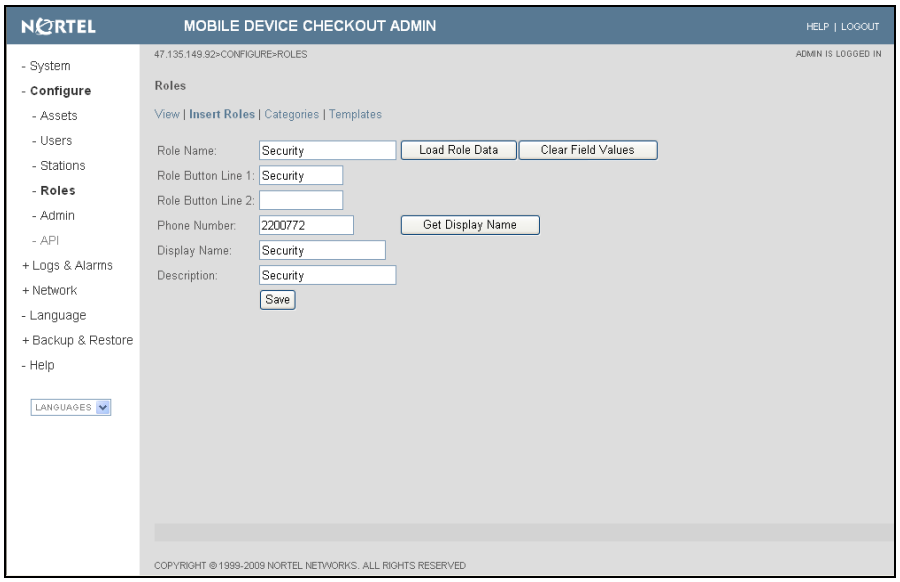


Figure 145: Loaded data on Insert Roles (with Get Display Name button)

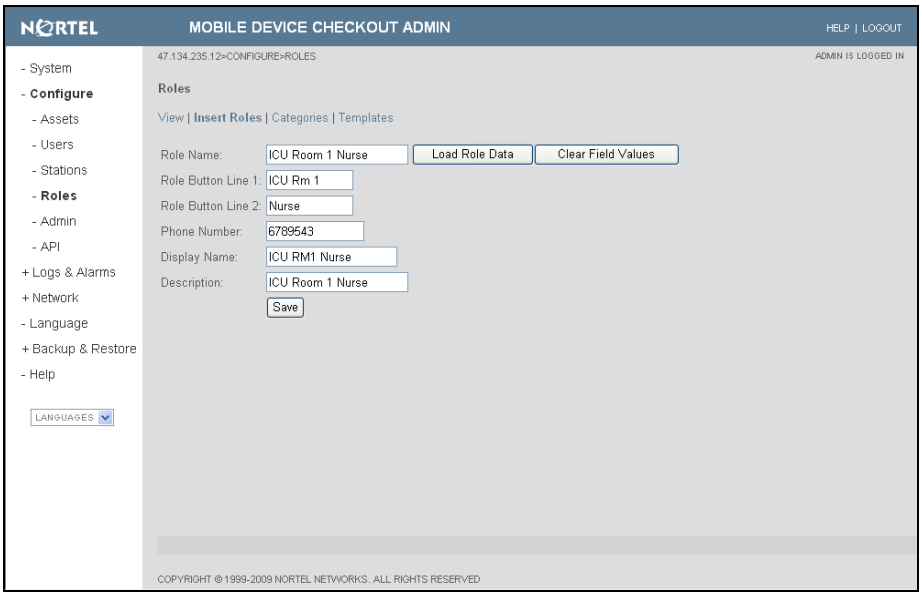


Figure 146: Loaded data on Insert Roles (without Get Display Name button)

- For a role which is not known (i.e. new), a message will appear on the message banner indicating that no role has been found with the given role name. This is not the expected behavior if an existing role is being modified. If this occurs, make sure the role name has been entered correctly and press the **Load Role Data** button again.

9. The following fields can be updated from the Insert Roles screen. The phone number and display name must match what has been configured on the call server. If the call server is a CS 1000, this can be facilitated by entering the phone number and using the Get Display Name button as described in step *a* below:

    a. **Phone Number**: This is the directory number associated with the role.

- If applicable, type in the new **Phone Number** for the role. For CS 2100, the phone number specified must be the full 10 digit DN, even if extension dialing is supported.
- Click the **Get Display Name** button. This will trigger the MDC to retrieve the role phone information from the call server. Retrieving information from the call server will help to ensure the MDC data matches the call server configuration.
    - After a few moments, the Display Name is retrieved and should be displayed on the screen.
    - Verify that this is the display name which should be associated with the role name entered.

    If you get a pop message indicating the MDC was unable to retrieve the data, this indicates you have either entered an unknown phone number OR there was a communication problem. Ensure the phone number is correct and click the **Get Display Name** button again. If you are unable to retrieve the Display Name from the call server automatically, you can manually enter the Display Name.

b. **Role Button Line 1**: This is the first line of the label for the role which is displayed during role selection.

c. **Role Button Line 2**: This is the second line of the label for the role which is displayed during role selection.

d. **Display Name**: Display name assigned to the role in the call server. If the call server is a CS 1000, the display name can be automatically retrieved from the call server using the procedure described in step a above.

e. **Description**: A text description of the role.

f. **Role Name:** This is name of the role displayed to the user during role selection. It must be unique as it will be used to identify this role on the MDC Admin GUI.

10. Click **Save** to save the modifications for the role into the MDC database.

    If you see an error popup dialog indicating the update failed because the phone number already exists, you have inadvertently entered a phone number already associated with another role. Type in the correct the phone number for this phone asset and click **Get Display Name** again if the role is on a CS 1000 call server.

    If you see an error popup dialog indicate the update failed because the role name already exists, make sure all roles have unique role names. Type in a unique role name and click **Save** button again.

11. Ensure that a successfully updated message is displayed to confirm that the changes were saved. The data fields will be blanked to facilitate inserting or updating another role.

12. Click **View** to return to the main Roles screen. The View screen will be refreshed and the latest Roles data will be displayed. Verify the changes you made against the specific role.

13. If you have modified a role label (i.e. Role Button Line 1 or Role Button Line 2) being used in a role template deployed to a MDC Station, you will need to reboot the MDC Station before the updated role label will take effect on the MDC Station. If you are uncertain of which MDC Stations are impacted, it is recommended that all MDC Station be rebooted during a suitable maintenance period once all the role related configuration changes have been completed. See Section 13.11 *Reboot All MDC Stations* or Section 13.10 *Reboot MDC Station* for the detailed procedure.

12.6 Delete Role

Description:

Use this procedure to delete roles.

The administrator will be warned if the role is referenced in one or more role templates or assigned to one or more role categories. In these instances, the administrator will need to confirm the role deletion as the role will be removed from the templates and categories where it is being referenced.

WARNING: If an administrator deletes a role name being used in a role template deployed to a MDC Station:

- If there is a warning dialog indicating the role is reference in one or more role templates, the administrator will need to review the layout pages associated with these affected role templates to ensure they are filled correctly. In MDC Release 2.0, all 12 positions of a role layout page of a role template must be assigned before adding another role layout page. All role layout pages except the last layout page must be completely filled. This condition must be maintained even when the role template is updated. For a role template using categories, this applies to layout pages for each category i.e. all layout pages except the last page for each category must be completely filled.
- The administrator will need to reboot the MDC Station before the removal of the role name will take effect on the MDC Station.

WARNING: A role cannot be deleted if that role is currently active on a phone i.e. a user has selected this role when checking out a phone.

WARNING: It is recommended to save any changes made to roles in the View screen prior to deleting roles. The Save button is enabled when there is an unsaved change.

Required information:

- Role which needs to be deleted identified by one of these fields: role name, description, phone number, or display name.

Steps:

From the MDC Admin GUI, click the **Configure** task on the left navigation menu.

1. The Configure screen of the Mobile Device Checkout Admin appears.
2. Click **Roles** from either the main task area or the Configure submenu on the left navigation menu.
3. The Roles screen appears. The main Roles screen is the View screen, which displays a list of roles in a table format. On a newly installed MDC, there will initially be no roles to display.

   Note: The **Delete** button, below the roles table, does not become enabled until there are entries marked for deletion from the roles table.

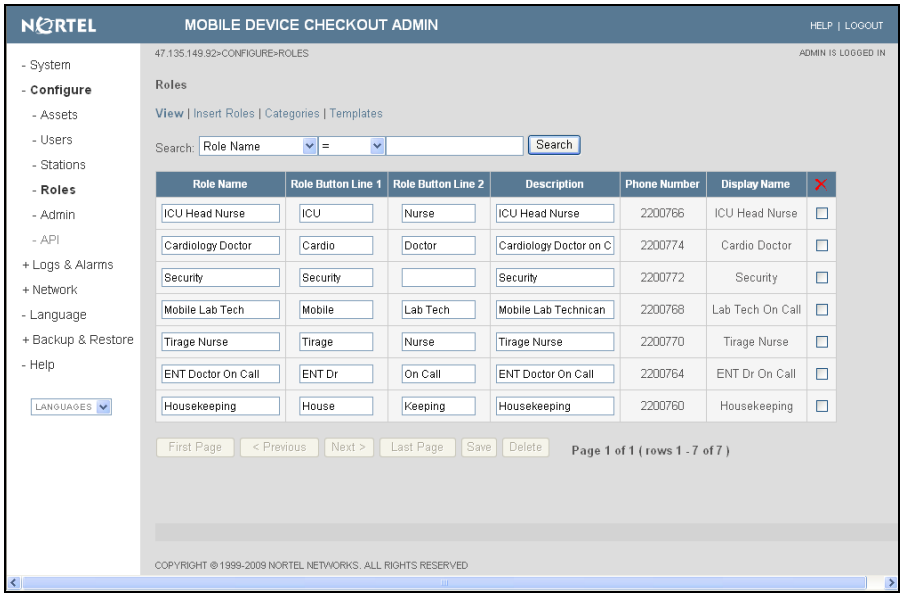


Figure 147: View Roles in MDC Admin GUI

4. Locate the table entry of the role you want to remove. See the procedures on View Roles for options to sort and search the role table. Check the box in the **Delete** column (rightmost column in the table) to delete a particular role. Once any roles have been marked for deletion from the View Roles table, the **Delete** button, below the table, becomes enabled to indicate that there are pending deletions. You may mark multiple roles for deletion. If you use the page control buttons, the entries you have marked for deletion may no longer be displayed on the screen.

   Note: A role cannot be deleted if that role is currently active on a phone i.e. a user has selected this role when checking out a phone. This prevents a role from being deleted while it is in use.

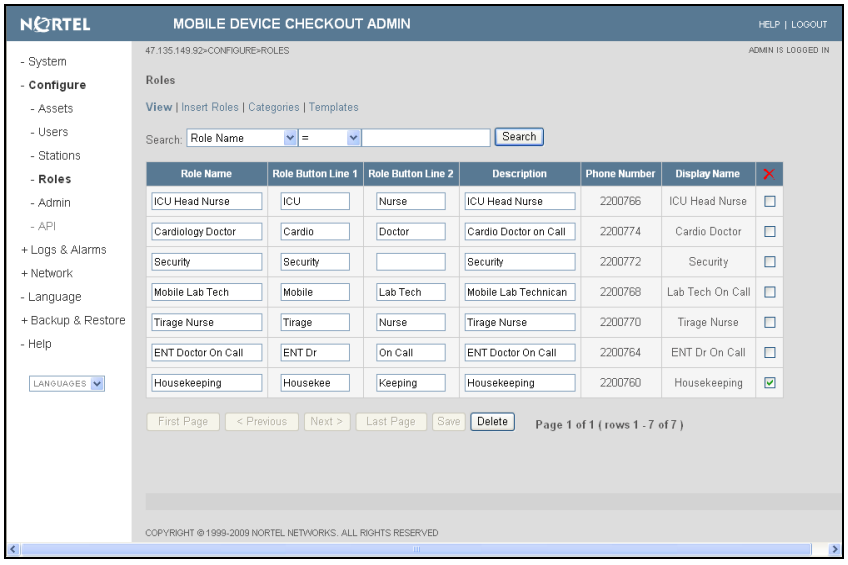


Figure 148: Deleting Roles from View Assets

If you attempt to navigate away from the View Roles screen while there are assets marked for deletion, a warning dialog will pop up.

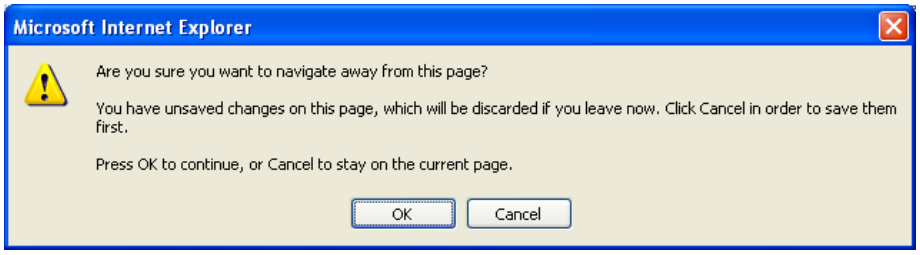


Figure 149: Warning of roles marked for Deletion

5. Click the **Delete** button, below the roles table, to delete the marked role(s).
6. A delete confirmation popup dialog will appear. Click **OK** to confirm deleting the role(s).

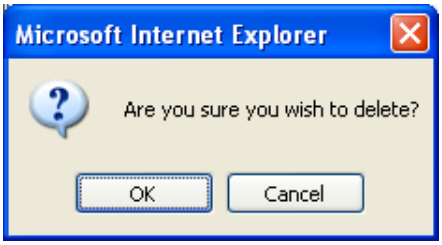


Figure 150: Delete Role Confirmation Dialog

Another warning dialog may appear if any role is in use against one or more role templates or assigned to one or more role categories. The specific relationships between the roles and its associated categories and templates will be listed. If the administrator confirms the deletion, the role will be removed from all the locations where it is references in categories and templates.

Note: When multiple roles are selected for deletion, no roles will be deleted without confirmation even those roles not referenced in any categories or templates.

Click **OK** to confirm deleting the role(s).

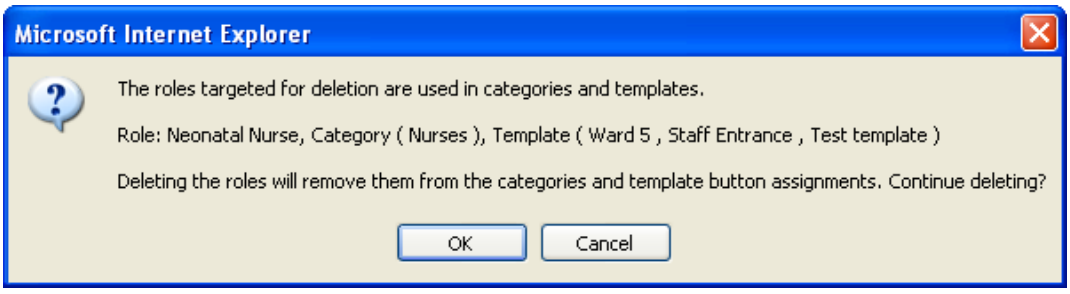


Figure 151: Sample Role Warning Dialog

A popup dialog may appear if the role cannot be deleted because this role is in use. Click **OK** to confirm this message.

7. The View screen will be refreshed and the latest roles data will be displayed. Any successfully deleted role(s) will be removed from the list of roles.

8. If you have deleted a role being used in a role template deployed to a MDC Station, you will need to reboot the MDC Station before the deletion will take effect on the MDC Station. If you are uncertain of which MDC Stations are impacted, it is recommended that all MDC Station be rebooted during a suitable maintenance period once all the role related configuration changes have been completed. See Section 13.11 *Reboot All MDC Stations* or Section 13.10 *Reboot MDC Station* for the detailed procedure.

12.7 Grouping Roles into Categories

A category is a group of roles. Categories are optional and can be used to group and organize roles. This can be convenient in an MDC system with many roles. A role can belong to none, one or multiple categories. There is no implied order of roles within a category.

The roles should be created prior to defining the role categories. A “No Role” is always available by default in the list of Available Roles. The “No Role” option permits a user to skip being assigned a role function when checking out a phone at a MDC Station location which supports the role functionality.

WARNING: The support of roles is controlled by license. Ensure that you have sufficient licenses for roles. If the licensing information has changed within the last 5 hours, you may need to manually refresh the licensing information using the procedure described in Section 7.7 *Update Licensing Information in the MDC.* Without sufficient licenses for roles, the administrative screens relating to roles will not be accessible. Refer to Section 7 *MDC Licensing and Keycode Retrieval System (KRS)* for more information on MDC licensing.

12.7.1 Create a New Category

Description:

This procedure describes how to create a role category.

Required information:

- Name of role category to be created
- Category Button Line 1: This is the first line of the label for this category which would be displayed to the user during role selection.
- [Optional] Category Button Line 2: This is the second line of the label for this category which would be displayed to the user during role selection.
- [Optional] Brief text description of the role category.
- List of roles associated with this role category

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Roles** from either the main task area or the Configure submenu on the left navigation menu.
4. The Roles screen appears. The main Roles screen is the View screen, which displays a list of roles in a table format. On a newly installed MDC, there will initially be no roles to display.
5. Click **Categories** from the Roles main task working area to create a role category on the MDC.
6. The Categories screen appears.

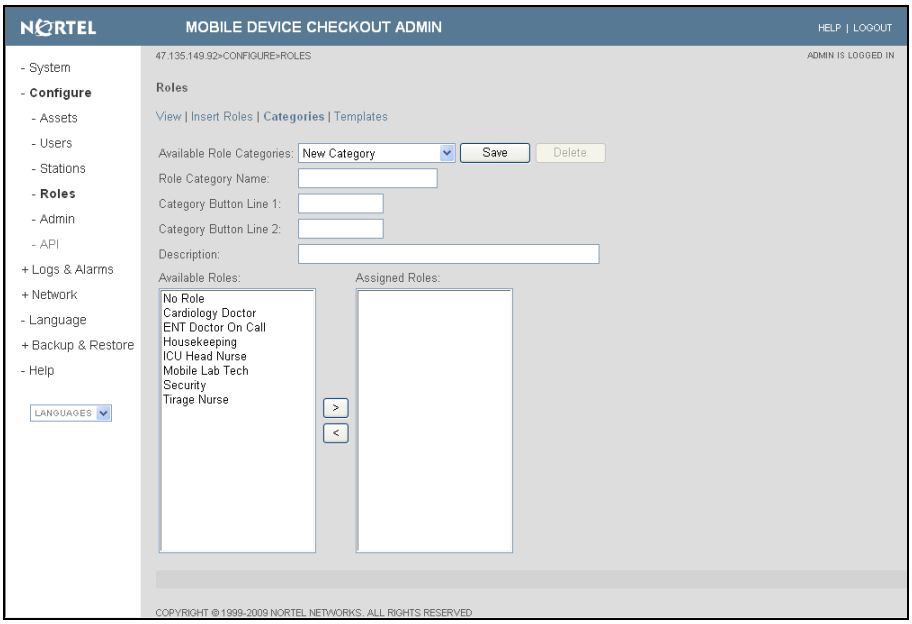


Figure 152: Categories Screen of MDC Admin GUI

7. To create a new category, select **New Category** from the pulldown menu for the field **Available Role Categories**.
8. Type in the **Role Category Name.** This should be a unique category name as it will be used to identify this category on the MDC Admin GUI.
9. Type in **Category Button Line 1** and **Category Button Line 2**. These two fields allow the administrator to create the label for this category as it will appear to the user during role selection.
10. Type in a text **Description** for this role category.
11. Select the roles for this category. A role can belong to none, one or multiple categories.

    To add a role to this category:

    a. Locate the role in the **Available Roles** list. The Available Roles is an alphabetically ordered list of all the roles defined.

       Search Tip: Placing the cursor in the list and typing the first letter of the role name you are searching for. The cursor will be place on the first role name in the list starting with that letter. As you repeatedly type in the first letter of the name, the cursor will automatically go to the next name in the list starting with that letter. Eventually, as the letter is repeatedly selected, the cursor scrolls over all the names starting with the selected letter.

    b. Use the **> button** to move the role from the Available Roles list into the **Assigned Role** list for this category. The Assigned Role list is an alphabetically order list of roles for the shown category.

    To remove a role from the Assigned Role list, select the role in the Assigned Role list. The search tip using first letter will work on this list as well. Use the **< button** to move the role from the Assigned Role list back into the Available Roles list.

    A “No Role” is always available by default in the list of Available Roles. The “No Role” option permits a user to skip being assigned a role function when checking out a phone at a MDC Station location which supports role assignment.

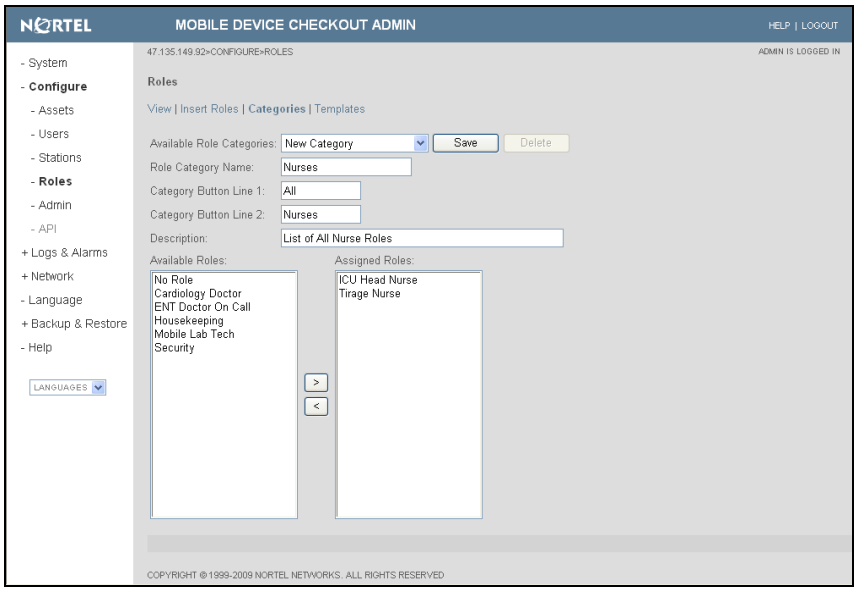


Figure 153: New Category on MDC Admin GUI

12. When you have completed selecting the roles for this category, click the **Save** button to save the new category.
13. A successful category update message will appear. The Available Roles Categories will change from New Category to the Role Category Name you typed in. The new category will be part of the pulldown menu for Available Roles Categories.

12.7.2 View a Category

Description:

This procedure describes how to view an existing role category.

Required information:

- Role category name of the category which you want to view.

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Roles** from either the main task area or the Configure submenu on the left navigation menu.
4. The Roles screen appears. The main Roles screen is the View screen, which displays a list of roles in a table format. On a newly installed MDC, there will initially be no roles to display.
5. Click **Categories** from the Roles main task working area to create a role category on the MDC.
6. The Categories screen appears.
7. To view an existing category, select the role category name from the pulldown menu of **Available Role Categories**.

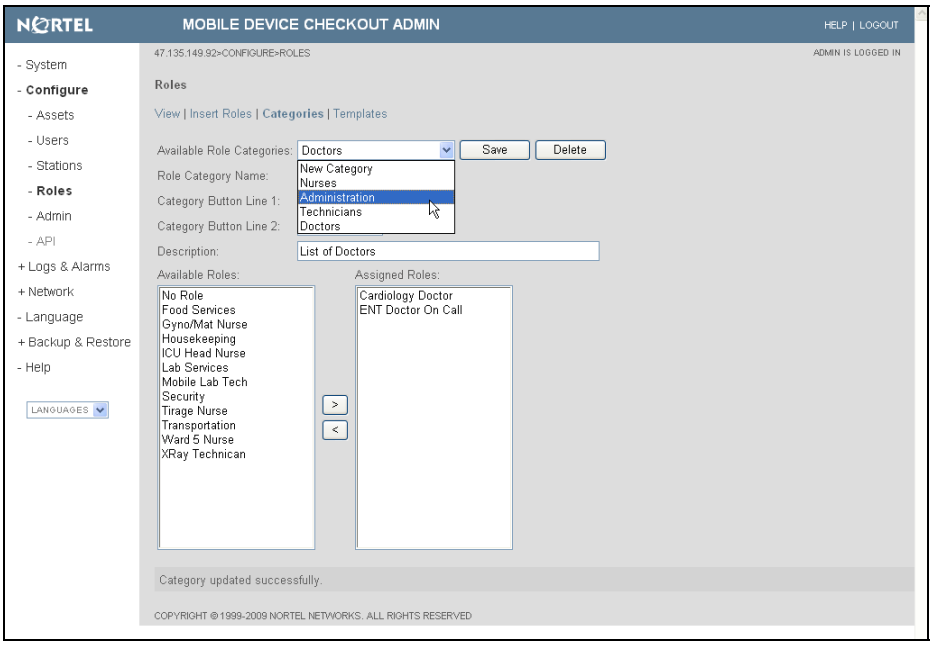


Figure 154: Select Available Role Categories

8. The information for the select category will be displayed on the screen:
    a. **Role Category Name**: unique name for the category
    b. **Category Button Line 1**: This is the first line of the label for the category which is displayed during role selection
    c. **Category Button Line 2**: This is the second line of the label for the category which is displayed during role selection
    d. **Description**: text description for the category
    e. **Assigned Roles**: list of roles assigned to this category. The Available Roles is an alphabetically ordered list of all the roles defined.

        Search tip to find a role in the Assigned Roles list: Placing the cursor in the list and typing the first letter of the role name you are searching for. The cursor will be place on the first role name in the list starting with that letter. As you repeatedly type in the first letter of the name, the cursor will automatically go to the next name in the list starting with that letter. Eventually, as the letter is repeatedly selected, the cursor scrolls over all the names starting with the selected letter.



Figure 155: Categories Screen of MDC Admin GUI

12.7.3 Modify a Category

Description:

This procedure describes how to modify an existing role category.

NOTE: When removing roles from a category, the administrator will be warned if the role from this category is referenced in one or more role templates. In these instances, the administrator will need to confirm the change as the role will be removed from the templates where it is being referenced

WARNING: If the administrator modifies a category being used in a role template deployed to a MDC Station:

- If the administrator has deleted roles associated with a category and there is a warning dialog indicating the category is reference in one or more role templates, the administrator will need to review the layout pages associated with these affected role templates to ensure they are filled correctly. In MDC Release 2.0, all 12 positions of a role layout page of a role template must be assigned before adding another role layout page. All role layout pages except the last layout page must be completely filled. This condition must be maintained even when the role template is updated. For a role template using categories, this applies to layout pages for each category i.e. all layout pages except the last page for each category must be completely filled.
- Any MDC Stations with station locations associated with these affected templates must be rebooted before the template changes will take effect on the MDC Station.

Required information:

- Role category name of the category which needs to be modified.
- Updated information for the category: Role Category Name, Category Button Line 1, Category Button Line 2, Description, or Assigned Roles.

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Roles** from either the main task area or the Configure submenu on the left navigation menu.
4. The Roles screen appears. The main Roles screen is the View screen, which displays a list of roles in a table format. On a newly installed MDC, there will initially be no roles to display.
5. Click **Categories** from the Roles main task working area to create a role category on the MDC.
6. The Categories screen appears.

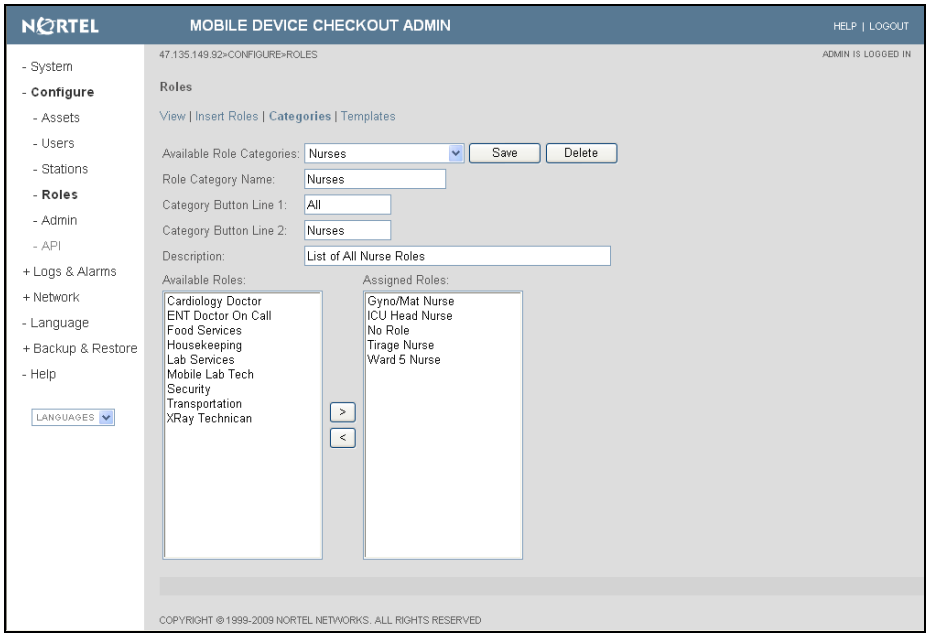


Figure 156: Categories Screen of MDC Admin GUI

7. To modify an existing category, select the role category name which needs modification from the pulldown menu of **Available Role Categories**.
8. The information for the select category will be displayed on the screen. The following fields can be updated:
    a. **Role Category Name**: unique name for the category which may be displayed during role selection.
    b. **Category Button Line 1**: This is the first line of the label for this category which would be displayed to the user during role selection.
    c. **Category Button Line 2**: This is the second line of the label for this category which would be displayed to the user during role selection.
    d. **Description**: text description for the category
    e. **Assigned Roles**: list of roles for this category. A role can belong to none, one or multiple categories.
        - To add a role, select the role in the **Available Roles** list which is the list of all the roles defined. Use the **> button** to move the role from the Available Roles list into the **Assigned Role** list for this category.

- To remove a role from the Assigned Role list, select the role in the Assigned Role list (the search tip on first letter works on this list as well). Use the **< button** to move the role from the Assigned Role list back into the Available Roles list

Search tip to find a role in the Available Roles or Assigned Roles list: Placing the cursor in the list and typing the first letter of the role name you are searching for. The cursor will be place on the first role name in the list starting with that letter. As you repeatedly type in the first letter of the name, the cursor will automatically go to the next name in the list starting with that letter. Eventually, as the letter is repeatedly selected, the cursor scrolls over all the names starting with the selected letter.

A “No Role” is always available by default in the list of Available Roles. The “No Role” option permits a user to skip being assigned a role function when checking out a phone at a MDC Station location which supports role assignment.

9. When you have completed the modifications for this category, click the **Save** button to save the new category.

   A warning dialog may appear if the roles being removed from this category are used in one or more role templates. The affected templates will be listed. If the administrator confirms the deletion, the role will be removed from all the locations where it is references in these templates.

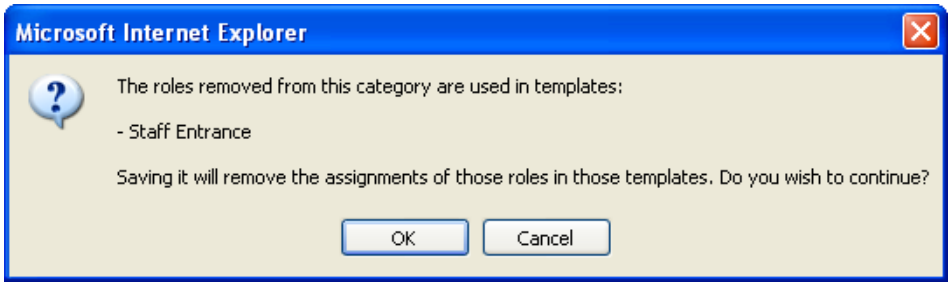


Figure 157: Categories Screen of MDC Admin GUI

10. A successful category update message will appear.
11. If you have modified a category name or category label (i.e. Category Button Line 1 or Category Button Line 2) and/or there was a warning dialog about impact to one or more role templates, the changes to this category may have impacted a role template deployed to a MDC Station. You need to reboot the MDC Station before the updated category name or deleted roles will take effect on the MDC Station. If you are uncertain of which MDC Stations are impacted, it is recommended that all MDC Station be rebooted during a suitable maintenance period once all the role related configuration changes have been completed. See Section 13.11 *Reboot All MDC Stations* or Section 13.10 *Reboot MDC Station* for the detailed procedure.

12.7.4 Delete a Category

Description:

This procedure describes how to delete an existing role category.

NOTE: When removing a category, the administrator will be warned if this category is referenced in one or more role templates. In these instances, the administrator will need to confirm the change as the category will be removed from the templates where it is being referenced

Note: if you delete a category being used in a role template deployed to a MDC Station, you will need to reboot the MDC Station before the removal of the role name will take effect on the MDC Station.

Required information:

- Role category name of the category which needs to be removed.

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Roles** from either the main task area or the Configure submenu on the left navigation menu.
4. The Roles screen appears. The main Roles screen is the View screen, which displays a list of roles in a table format. On a newly installed MDC, there will initially be no roles to display.
5. Click **Categories** from the Roles main task working area to create a role category on the MDC.
6. The Categories screen appears.
7. To delete an existing category, select the role category name which needs to be deleted from the pulldown menu of **Available Role Categories**.

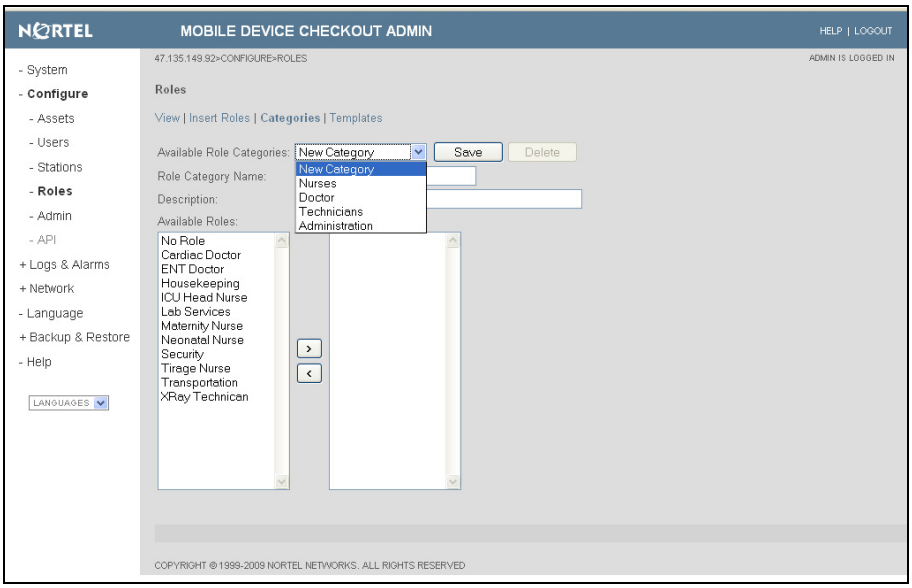


Figure 158: Categories Screen of MDC Admin GUI

8. The information for the select category will be displayed on the screen. Confirm this is the category which needs to be deleted.
9. Click the **Delete** button to delete the shown category.
10. A delete confirmation popup dialog will appear. Click **OK** to confirm deleting the category.

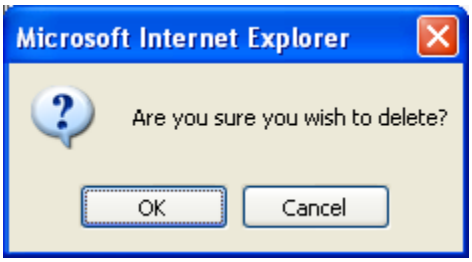


Figure 159: Delete Category Confirmation Dialog

A warning dialog may appear if the category is being used in one or more role templates. The affected templates will be listed. If the administrator confirms the deletion, any role from this category will be removed from all the locations where it is references in these templates. Click **OK** to confirm these changes.

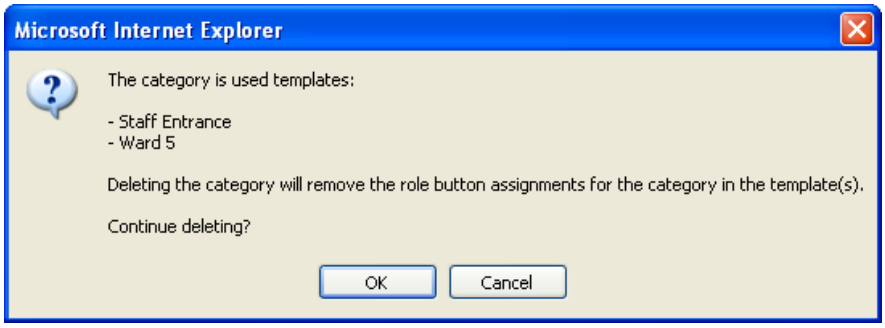


Figure 160: Sample Category in Use Confirmation Dialog

11. A successful category delete message will appear.
12. If there was a warning dialog about impact to one or more role templates, the deletion of this category may have impacted a role template deployed to a MDC Station. You need to reboot the MDC Station before the deletion of this category will take effect on the MDC Station. If you are uncertain of which MDC Stations are impacted, it is recommended that all MDC Station be rebooted during a suitable maintenance period once all the role related configuration changes have been completed. See Section 13.11 *Reboot All MDC Stations* or Section 13.10 *Reboot MDC Station* for the detailed procedure.

12.8 Role Template

A role template is used by users to select a role assignment during checkout. A role template is a set of roles organized into a layout presentation. The layout presentation consists of one or more pages where each page has 12 positions for roles organized into three rows and four columns. The administrator can place each role in a specific position within a specific page for the template. The layout is based on what a user would see on an MDC Station screen when selecting a role function as part of checking out an asset. The role label (role button label 1 and role button label 2) are used on the layout presentations.

The administrator can optionally use categories when creating a role template. When categories are used, each category has separate role layout pages associated with it. The administrator can select which roles will be used from the category and place those roles on the layout pages associated with the category. From a user perspective during checkout, if the MDC Station supports roles assignment using a template based on categories,

the user would first select a category and then a specific role from the role layout pages for that category. A category will only be associated with a template if at least one role is used from that category.

In MDC Release 2.0 when configuring a role template, all 12 positions of a role layout page must be assigned before adding another role layout page. All role layout pages except the last layout page must be completely filled. For a role template using categories, this applies to layout pages for each category i.e. all layout pages except the last page for each category must be completely filled. The administrator must manually ensure the layout pages are full when the role template is updated by the following actions:

- Role used in the role template is deleted
- Role is deleted from a category used in the role template

When a category used in the role template is deleted, all its associated role layout pages will be deleted so the administrator does not have to review the affected role templates.

As described above, a role template can either be based on individual roles or it can be based on roles from categories. When a template is based on individual roles, each role can appear only once in a template. A role can appear in one or more templates. When a template is based on categories, each role within a category can only be used once for that category. Categories can appear in one or more role templates.

There can be multiple roles templates on a MDC. Templates are deployed through MDC Station Locations. See Section 13.6 *Insert Station Location* and Section 13.7 *Modify Station Location* for more details on associating role templates to MDC Station locations. When possible, it is recommended to create customize role templates for the various MDC Station location so that the most frequent users of the MDC Station at that location will be able to quickly access their roles. For example, create a nurse template for all the MDC Station locations that are at nursing stations.

A “No Role” is always available by default in the list of Available Roles. The “No Role” option permits a user to skip being assigned a role function when checking out a phone at a MDC Station location which supports role assignment.

A role template cannot be deleted if the template is in use against one or more Station Locations.

WARNING: The support of roles is controlled by license. Ensure that you have sufficient licenses for roles. If the licensing information has changed within the last 5 hours, you may need to manually refresh the licensing information using the procedure described in Section 7.7 *Update Licensing Information in the MDC.* Without sufficient licenses for roles, the administrative screens relating to roles will not be accessible. Refer to Section 7 *MDC Licensing and Keycode Retrieval System (KRS)* for more information on MDC licensing.

12.8.1 Create a New Template

Description:

This procedure describes how to create a role template.

Templates may optionally use categories. A maximum of 12 categories may be used. If more than 12 categories are used, those categories which appear alphabetically after the 12th category will not be visible during role selection.

Search tip for any of the role or category lists: Placing the cursor in the list and typing the first letter of the name you are searching for. The cursor will be place on the first name in the list starting with that letter. As you repeatedly type in the first letter of the name, the cursor will automatically go to the next name in the list starting with that letter. Eventually, as the letter is repeatedly selected, the cursor scrolls over all the names starting with the selected letter.

Required information:

- Name of role template to be created
- Brief text description of the role template

- Whether categories will be used with this role template
- List of roles associated with this template
- Arrangement of the roles onto role layout pages
- [Optional] List of categories and the roles within those categories which will be used to with this role template

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Roles** from either the main task area or the Configure submenu on the left navigation menu.
4. The Roles screen appears. The main Roles screen is the View screen, which displays a list of roles in a table format. On a newly installed MDC, there will initially be no roles to display.
5. Click **Templates** from the Roles main task working area to create a role template on the MDC.
6. The Templates screen appears.

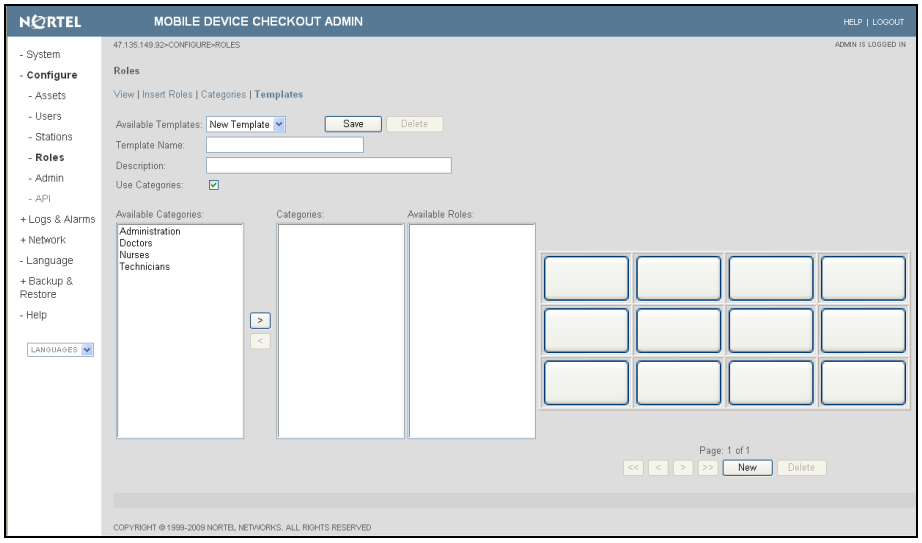


Figure 161: Template Screen of MDC Admin GUI

7. To create a new template, select **New Template** from the pulldown menu for the field **Available Templates**.
8. Type in the **Template Name.** This should be a unique template name.
9. Type in a text **Description** for this role category.
10. If this role template will be based on role categories, ensure the **Use Categories** box is checked. Otherwise, uncheck the Use Categories box if this role template will be created from individual roles.

    When changing the value of the Use Categories box, a popup dialog will appear to warn that any unsaved changes to the template configuration will be lost. Only click the **OK** button to continue and lose all unsaved changes.

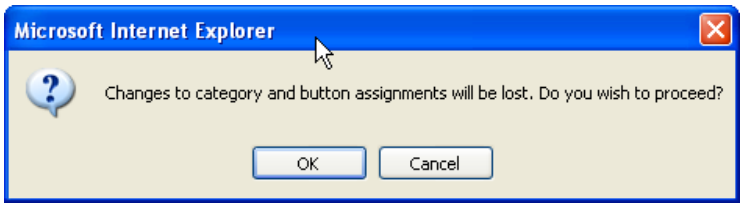


Figure 162: Changing Use Categories Warning Dialog

11. If this template is based on categories, select the categories which will be used with this template. A maximum of 12 categories may be selected for each template. If more than 12 categories are selected, those categories which appear alphabetically after the 12th category will not be visible during role selection:

    NOTE: The Role Category Name is used in the Available Categories and Categories lists on the MDC Admin GUI. However, during role selection at the MDC Station, the user will see the category labels (i.e. Category Button Line 1 and Category Button Line 2) on the MDC Station screen.

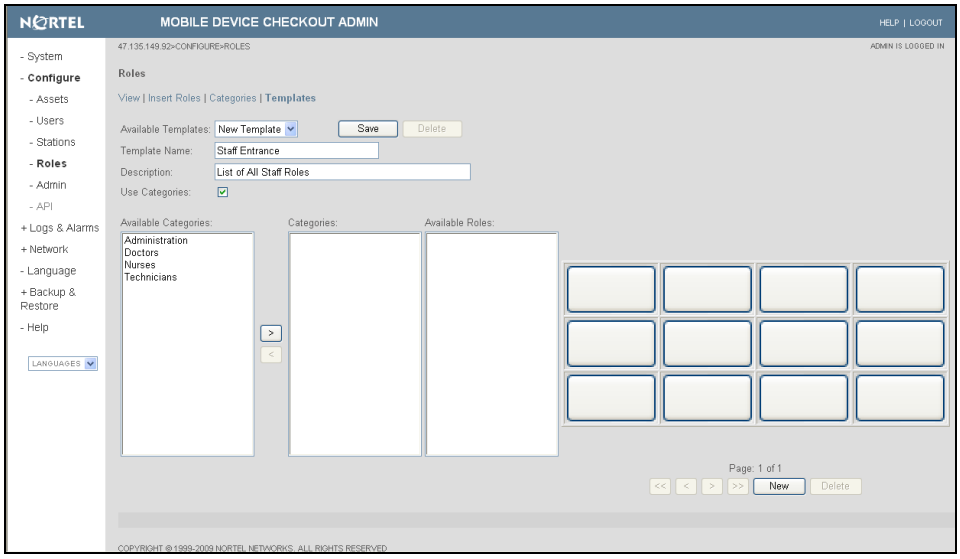


Figure 163: Template Using Categories Screen of MDC Admin GUI

a. To add a category to this template:

   i. Locate the category in the **Available Categories** list. The search tip using first letter will work on this list. The Available Category is a list of all the categories which are not being used in the template. Initially, this will list all the defined categories.

   ii. Use the **> button** to move the category from the Available Categories list into the **Categories** list for this template.

b. To remove a category from this template:

   i. Select the category in the **Categories** list. The search tip using first letter will work on this list.

   ii. Use the **< button** to move the category from the Categories list back into the Available Categories list.

   iii. A warning dialog will appear indicating that any pages of roles created from this category will be deleted when the category is removed from the Categories list for this template. Click the **OK** button.

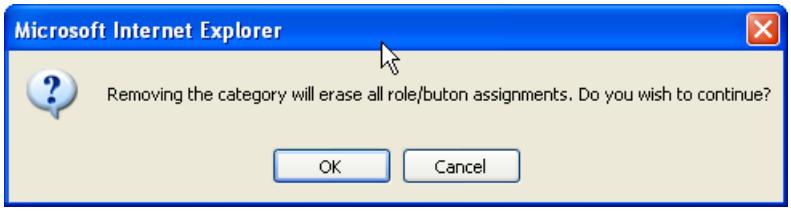


Figure 164: Removing Category Warning Dialog

c. For each category in the Categories list for this template, select the roles which apply to this template and arrange how the roles will appear on the role layout pages. Each category has its own separate role layout pages within a template. A category will remain associated with a template only if roles from the category are being used in the template.

NOTE: In MDC Release 2.0 when configuring a role template, all 12 positions of a role layout page for a category must be assigned before adding another role layout page. Only the last layout page does not have to be full. This condition must be maintained even when the role template is updated.

NOTE: The Role Names are used in the Available Roles list. When the role is placed into the role layout page, the role label (Role Button Line 1 and Role Button Line 2) instead of role name will be shown on the MDC Admin GUI. The administrator is able to view the template as the end customer will see it on the MDC Station screen during role selection.

i. Select the category in the **Categories** list by clicking on the category name.

ii. The Available Roles will list those roles associated with the selected category which are not being used in the template. Initially, all the roles associated with that category will appear in the **Available Roles** list.

The first page of the layout pages for the selected category will also be shown. Initially, there will only be one layout page and no roles assigned to a layout position.

iii. Select a role from the list of **Available Roles** by clicking on the role name.

iv. **Click** one of the positions on the layout page to place the selected role. The role label will be shown on the layout page.

- If the position is vacant, the selected role will be place into the position.
- If the position was occupied by another role, the selected role will still be placed into the position and the previous occupant role will be returned to the Available Roles list.
- If an additional layout page needs to be created for this category, click the **New** button under the layout page. A new page will be created after the current page and this new page will automatically be displayed.
- The current layout page number and the total number of layout pages are shown. Use the buttons beneath the layout page to navigate between the layout pages for this category:

<< Moves the view to the first layout page for this category

< Moves the view the view to the previous layout page for this category

> Moves the view to the next layout page for this category

>> Moves the view to the last layout page for this category

- To delete the current layout page number, click the **Delete** button under the layout page. A popup dialog will ask for confirmation for the deletion. Click the **OK** button. Any roles on the page will be returned to the Available Roles list. If there is only a single layout page for a category, this page cannot be deleted.

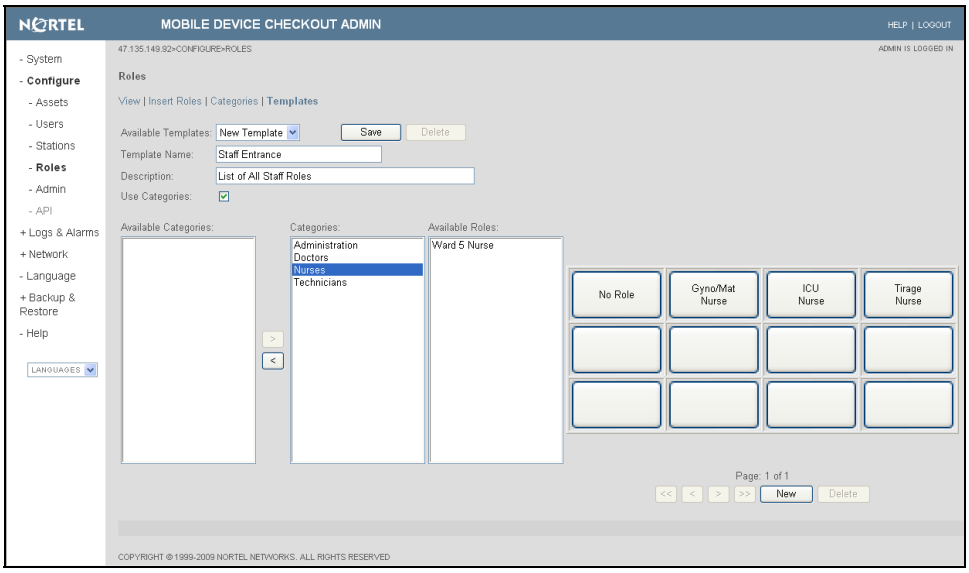


Figure 165: Category based Role Template on MDC Admin GUI

12. If this template is based on individual roles (i.e. does not use categories), select the roles which apply to this template and arrange how the roles will appear on the role layout pages.

    NOTE: In MDC Release 2.0 when configuring a role template, all 12 positions of a role layout page must be assigned before adding another role layout page. Only the last layout page does not have to be full. This condition must be maintained even when the role template is updated.

    NOTE: The Role Names are used in the Available Roles list. When the role is placed into the role layout page, the role label (Role Button Line 1 and Role Button Line 2) instead of role name will be shown on the MDC Admin GUI. The administrator is able to view the template as the end customer will see it on the MDC Station screen during role selection.

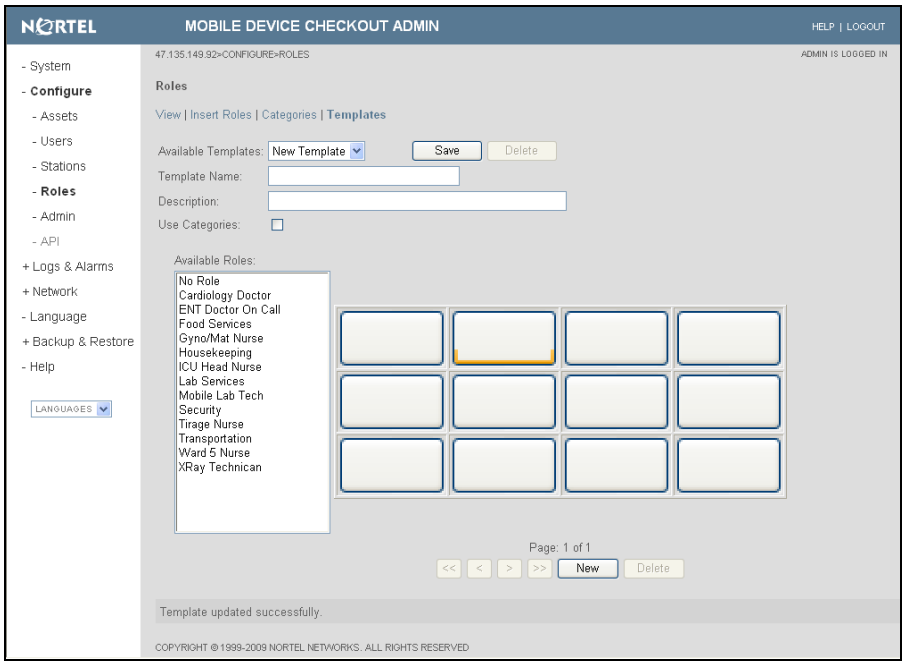


Figure 166: Template Not Using Categories Screen of MDC Admin GUI

a. Select a role from the list of **Available Roles** by clicking on the role name.

   The Available Roles will list the roles which are not being used in the template. Initially, all the roles will appear in the **Available Roles** list.

b. **Click** one of the positions on the layout page to place the selected role.

   i. If the position is vacant, the selected role will be place into the position.

   ii. If the position was occupied by another role, the selected role will still be placed into the position and the previous occupant role will be returned to the Available Roles list.

   iii. If an additional layout page needs to be created, click the **New** button under the layout page. A new page will be created after the current page and this new page will automatically be displayed.

   iv. The current layout page number and the total number of layout pages are shown. Use the buttons beneath the layout page to navigate between the layout pages:

   << Moves the view to the first layout page for this template

   < Moves the view to the previous layout page for this template

   > Moves the view to the next layout page for this template

   >> Moves the view to the last layout page for this template

   v. To delete the current layout page number, click the **Delete** button under the layout page. A popup dialog will ask for confirmation for the deletion. Click the **OK** button. Any roles on the page will be returned to the Available Roles list. If there is only a single layout page, this page cannot be deleted.

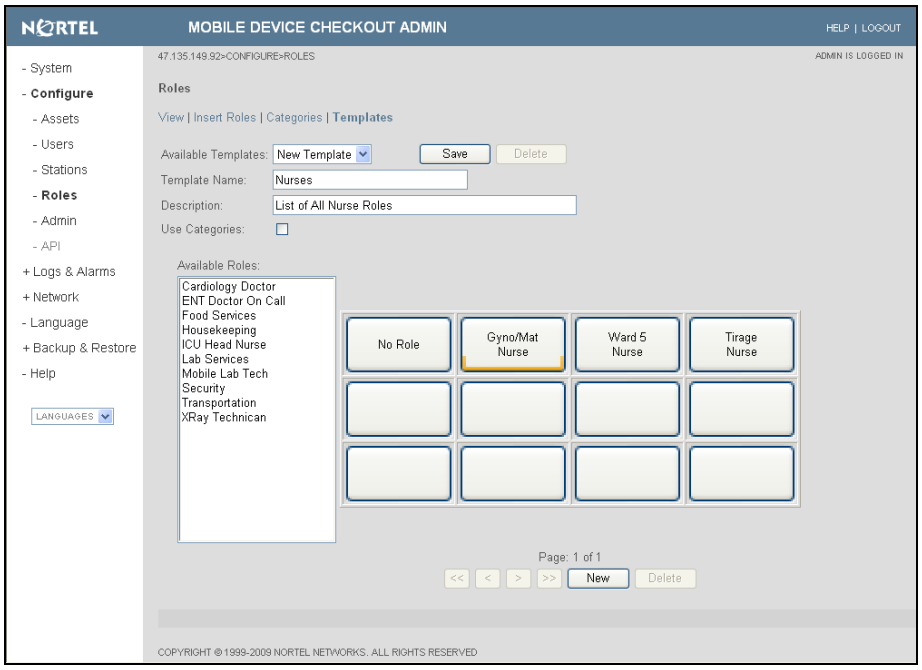


Figure 167: Non-Category based Role Template on MDC Admin GUI

13. When you have completed selecting the roles and layout for this template, click the **Save** button at the top of the screen to save the new template.
14. A successful template update message will appear. The Available Templates will change from New Template to the Template Name you typed in. The new template will be part of the pulldown menu for Available Templates.

12.8.2 View a Template

Description:

This procedure describes how to view an existing role template.

Required information:

- Name of role template to be viewed

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Roles** from either the main task area or the Configure submenu on the left navigation menu.
4. The Roles screen appears. The main Roles screen is the View screen, which displays a list of roles in a table format. On a newly installed MDC, there will initially be no roles to display.
5. Click **Templates** from the Roles main task working area to create a role category on the MDC.
6. The Templates screen appears.

7. To view an existing template, select the role template name from the pulldown menu for the field **Available Templates**.

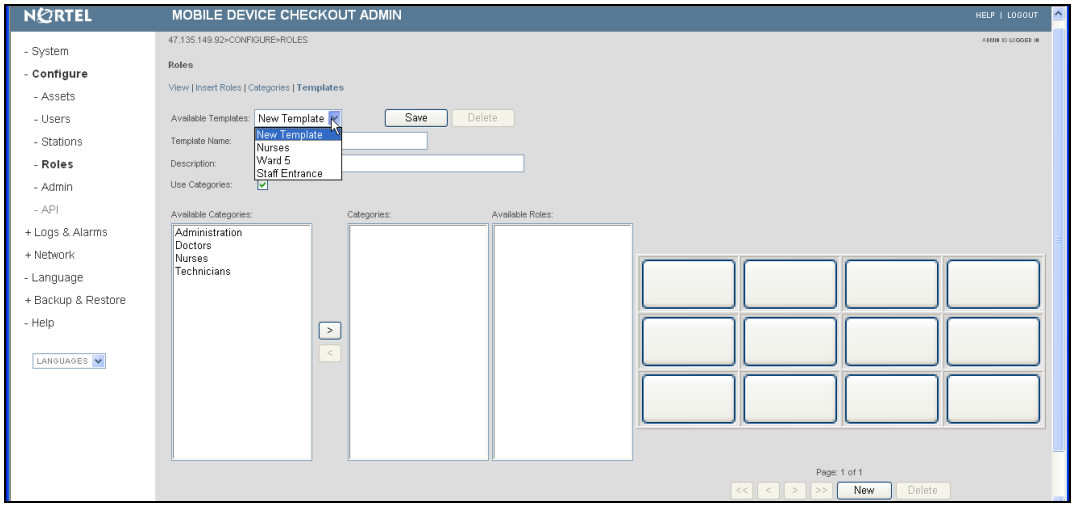


Figure 168: Select Available Role Template on MDC Admin GUI

8. The information for the select template will be displayed on the screen:
    a. Template Name: unique name for the template
    b. Description: text description for the template
    c. Use Categories: will be checked if categories are used for the template
    d. If categories are used on the template, the following will be displayed:

    NOTE: The Role Category Name is used in the Available Categories and Categories lists on the MDC Admin GUI. However, during role selection, the user will see the category labels (i.e. Category Button Line 1 and Category Button Line 2) on the MDC Station screen.

    NOTE: The Role Names are used in the Available Roles list. When the role is placed into the role layout page, the role label (Role Button Line 1 and Role Button Line 2) instead of role name will be shown on the MDC Admin GUI. The administrator is able to view the template as the end customer will see it on the MDC Station screen during role selection.

        i. Available Categories: list of all the categories which are not being used in the template.
        ii. Categories: list of all the categories being used in the template. The first category will be selected.
        iii. Available Roles: list of all the roles for the selected category which are not used in the template.
        iv. Roles Layout Page: the first layout page for the selected category.

        The current layout page number and the total number of layout pages are shown. Use the buttons beneath the layout page to navigate between the layout pages for this category:

        << Moves the view to the first layout page for this category

        < Moves the view to the previous layout page for this category

        > Moves the view to the next layout page for this category

        >> Moves the view to the last layout page for this category

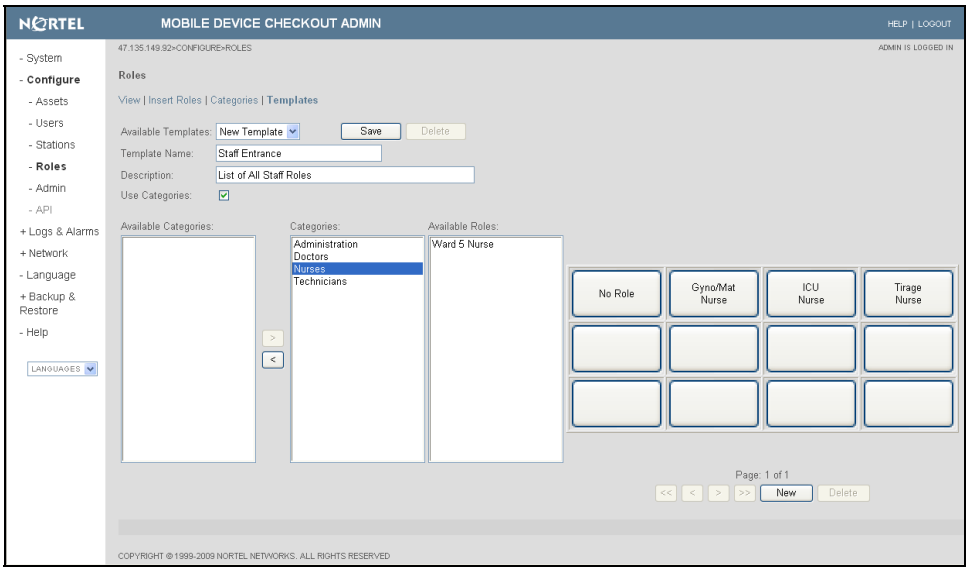


Figure 169: Category Based Template Screen of MDC Admin GUI

e. If categories are not used on the template, the following will be displayed:

NOTE: The Role Names are used in the Available Roles list. When the role is placed into the role layout page, the role label (Role Button Line 1 and Role Button Line 2) instead of role name will be shown on the MDC Admin GUI. The administrator is able to view the template as the end customer will see it on the MDC Station screen during role selection.

i. Available Roles: list of all the roles which are not used in the template.

ii. Roles Layout Page: the first layout page for the template

The current layout page number and the total number of layout pages are shown. Use the buttons beneath the layout page to navigate between the layout pages:

<< Moves the view to the first layout page for this template

< Moves the view to the previous layout page for this template

> Moves the view to the next layout page for this template

>> Moves the view to the last layout page for this template

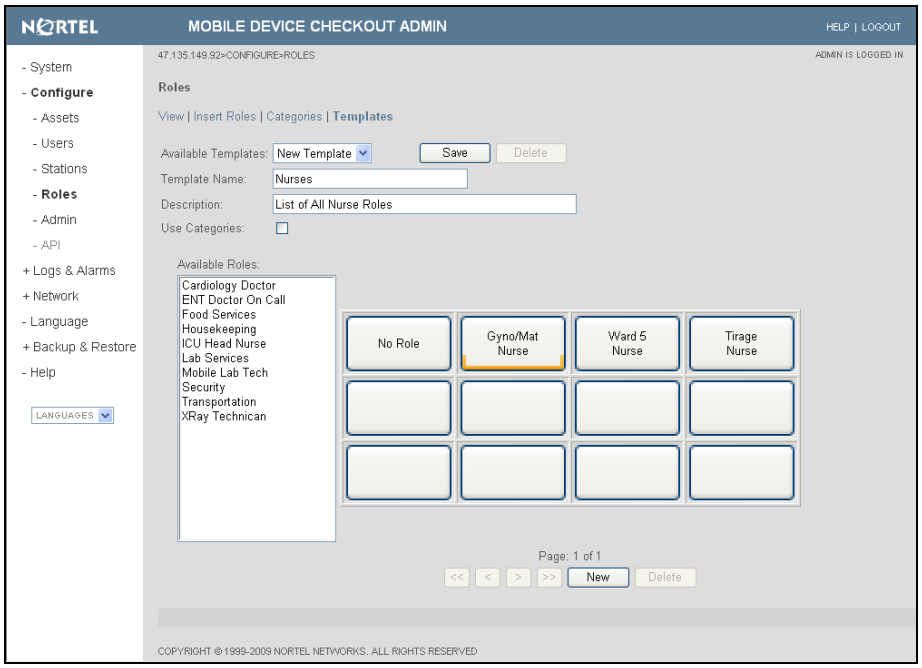


Figure 170: Non-Category Based Template Screen of MDC Admin GUI

12.8.3 Modify a Template

Description:

This procedure describes how to modify an existing role template.

Required information:

- Name of role template to be modified
- Updated information for the template:
  - Brief text description of the role template
  - Whether categories will be used with this role template
  - List of roles associated with this template
  - Arrangement of the roles onto role layout pages
  - [Optional] List of categories and the roles within those categories which will be used to with this role template

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Roles** from either the main task area or the Configure submenu on the left navigation menu.
4. The Roles screen appears. The main Roles screen is the View screen, which displays a list of roles in a table format. On a newly installed MDC, there will initially be no roles to display.
5. Click **Templates** from the Roles main task working area to create a role category on the MDC.
6. The Templates screen appears.

7. To view an existing template, select the role template name from the pulldown menu for the field **Available Templates**.

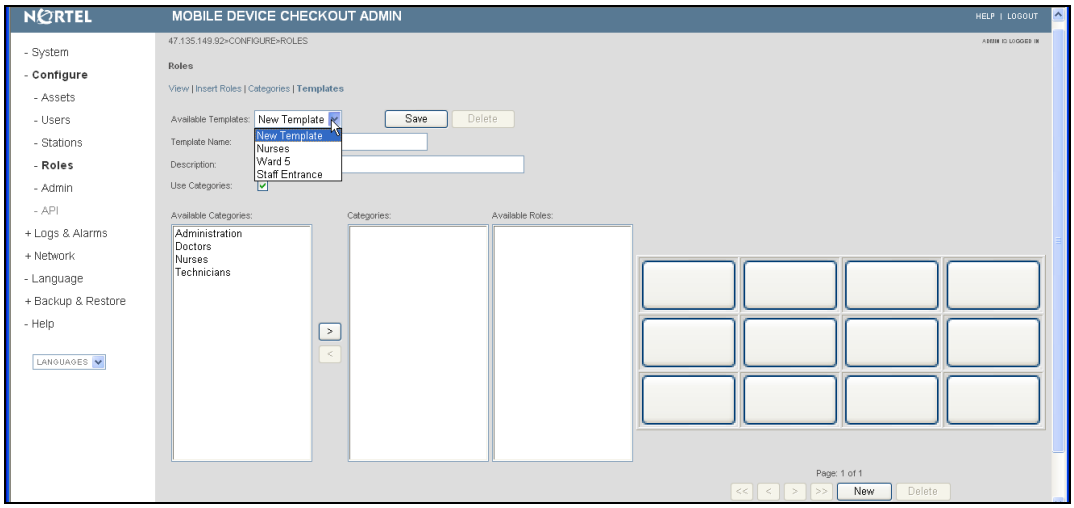


Figure 171: Template Screen of MDC Admin GUI

8. The information for the select template will be displayed on the screen.
9. The following information for the select template can be modified:
    a. **Template Name**: unique name for the template
    b. **Description**: text description for the template
    c. **Use Categories**: can be checked if categories are used for the template or unchecked if individual roles will be used. When changing the value of the Use Categories box, a popup dialog will appear to warn that any unsaved changes to the template configuration will be lost. Click the **OK** button.
10. If this template is based on categories, you can modify the categories and the roles used from the categories for this template. You can also rearrange how the roles will appear on the role layout pages. Each category has its own separate role layout pages within a template. A category will only remain associated with a template if roles from the category are being used in the template. A maximum of 12 categories may be selected for each template. If more than 12 categories are selected, those categories which appear alphabetically after the 12th category will not be visible during role selection:

    NOTE: In MDC Release 2.0 when configuring a role template, all 12 positions of a role layout page for a category must be assigned before adding another role layout page. Only the last layout page does not have to be full. This condition must be maintained even when the role template is updated.

    NOTE: The Role Category Name is used in the Available Categories and Categories lists on the MDC Admin GUI. However, during role selection at the MDC Station, the user will see the category labels (i.e. Category Button Line 1 and Category Button Line 2) on the MDC Station screen.

    NOTE: The Role Names are used in the Available Roles list. When the role is placed into the role layout page, the role label (Role Button Line 1 and Role Button Line 2) instead of role name will be shown on the MDC Admin GUI. The administrator is able to view the template as the end customer will see it on the MDC Station screen during role selection.

    a. To add a category to this template:
        i. Locate the category in the **Available Categories** list. The search tip using first letter will work on this list.

ii. Use the **> button** to move the category from the Available Categories list into the **Categories** list for this template.

b. To remove a category from this template:

i. Select the category in the **Categories** list. The search tip using first letter will work on this list.

ii. Use the **< button** to move the category from the Categories list back into the Available Categories list.

iii. A warning dialog will appear indicating that any pages of roles created from this category will be deleted when the category is removed from the Categories list for this template. Click the **OK** button.

c. To add a role from a category to this template:

i. Select the category in the **Categories** list by clicking on the category name.

ii. The list of roles associated with this category which are not being used in the template will appear in the **Available Roles** list.

The first page of the layout pages for the selected category will also be shown.

iii. Select a role from the list of **Available Roles** by clicking on the role name.

iv. **Click** one of the positions on the layout page to place the selected role. Note: The role label will be used on the layout page:

- If the position is vacant, the selected role will be place into the position.
- If the position was occupied by another role, the selected role will still be placed into the position and the previous occupant role will be returned to the Available Roles list.
- If an additional layout page needs to be created for this category, click the **New** button under the layout page. A new page will be created after the current page and this new page will automatically be displayed.
- The current layout page number and the total number of layout pages are shown. Use the buttons beneath the layout page to navigate between the layout pages for this category:

<< Moves the view to the first layout page for this category

< Moves the view to the previous layout page for this category

> Moves the view to the next layout page for this category

>> Moves the view to the last layout page for this category

d. To remove a role of a category from this template:

i. Select the category in the **Categories** list by clicking on the category name.

ii. The list of roles associated with this category which are not being used in the template will appear in the **Available Roles** list.

iii. Locate the role which needs to be removed on the layout pages for this category.

The current layout page number and the total number of layout pages are shown. Use the buttons beneath the layout page to navigate between the layout pages for this category:

<< Moves the view to the first layout page for this category

< Moves the view to the previous layout page for this category

> Moves the view to the next layout page for this category

>> Moves the view to the last layout page for this category

iv. **Click** the position on the layout page with the role you want to remove. This will remove the role from the layout page and place this role on the Available Roles list for this category.

e. To rearrange a role position on the layout pages for this category:

i. First remove the role from the template using the procedure described in step *d* above.

ii. Re-add the role in the correct layout page and role position using the procedure described in step *c* above.

f. To add a layout page for a category from this template:

i. Select the category in the **Categories** list by clicking on the category name.

ii. Locate the layout page after which you want a new layout page. Use the buttons beneath the layout to navigate between layout pages.

iii. If an additional layout page needs to be created for this category, click the **New** button under the layout page. A new page will be created after the current page and this new page will automatically be displayed.

g. To delete a layout page for a category from this template:

i. Select the category in the **Categories** list by clicking on the category name.

ii. Locate the layout page you want to remove. Use the buttons under the layout to navigate between layout pages.

iii. To delete the current layout page number, click the **Delete** button under the layout page. A popup dialog will ask for confirmation for the deletion. Click the **OK** button. Any roles on the page will be returned to the Available Roles list. If there is only a single layout page for a category, this page cannot be deleted.

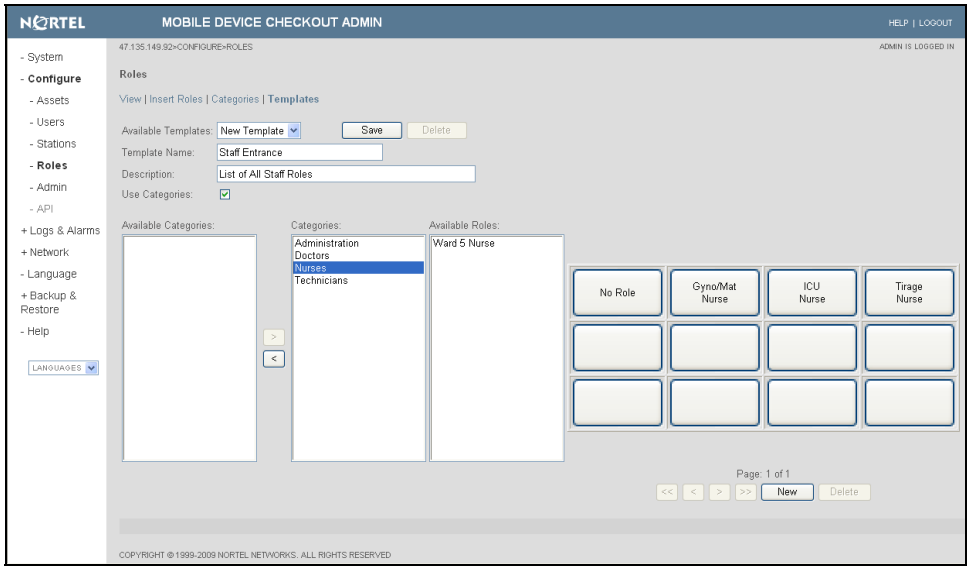


Figure 172: Category based Role Template on MDC Admin GUI

11. If this template is based on individual roles (i.e. does not use categories), you can modify the roles which apply to this template and arrange how the roles will appear on the role layout pages:

NOTE: In MDC Release 2.0 when configuring a role template, all 12 positions of a role layout page must be assigned before adding another role layout page. Only the last layout page does not have to be full. This condition must be maintained even when the role template is updated.

NOTE: The Role Names are used in the Available Roles list. When the role is placed into the role layout page, the role label (Role Button Line 1 and Role Button Line 2) instead of role name will be shown on the MDC Admin GUI. The administrator is able to view the template as the end customer will see it on the MDC Station screen during role selection.

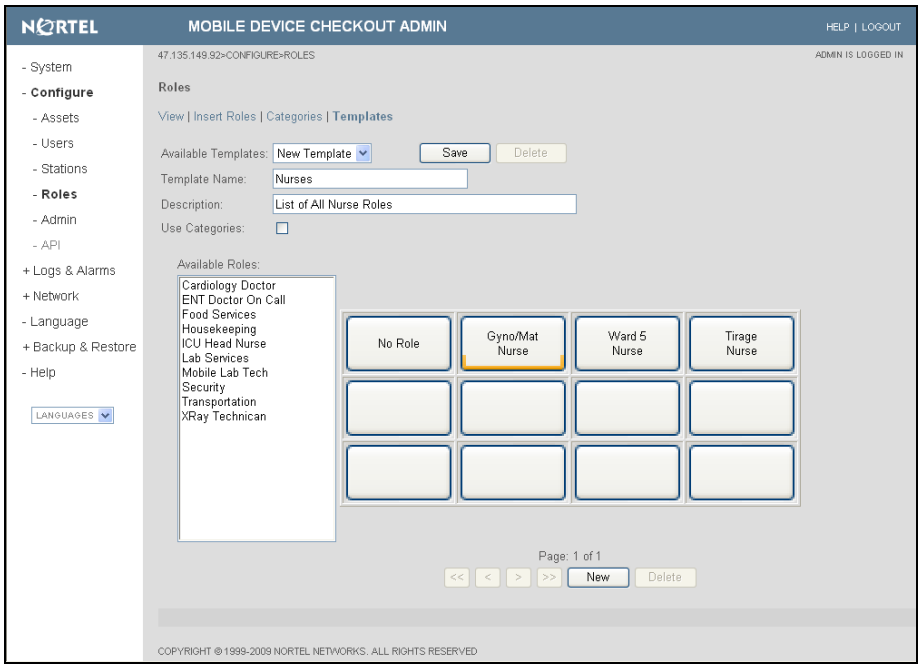


Figure 173: Non-Category based Role Template on MDC Admin GUI

a. To add a role to this template:

   i. Select a role from the list of **Available Roles** by clicking on the role name. The list of roles which are not being used in the template will appear in the **Available Roles** list.

   ii. **Click** one of the positions on the layout page to place the selected role in this template.

   - If the position is vacant, the selected role will be place into the position.
   - If the position was occupied by another role, the selected role will still be placed into the position and the previous occupant role will be returned to the Available Roles list.
   - If an additional layout page needs to be created, click the **New** button under the layout page. A new page will be created after the current page and this new page will automatically be displayed.
   - The current layout page number and the total number of layout pages are shown. Use the buttons beneath the layout page to navigate between the layout pages for this category:

     << Moves the view to the first layout page for this category

     < Moves the view to the previous layout page for this category

> Moves the view to the next layout page for this category

>> Moves the view to the last layout page for this category

b. To remove a role from this template:

i. Locate the role which needs to be removed on the layout pages for this template.

The current layout page number and the total number of layout pages are shown. Use the buttons beneath the layout page to navigate between the layout pages for this category:

<< Moves the view to the first layout page for this category

< Moves the view to the previous layout page for this category

> Moves the view to the next layout page for this category

>> Moves the view to the last layout page for this category

ii. **Click** the position on the layout page with the role you want to remove. This will remove the role from the layout page and place this role on the Available Roles list for this category.

c. To rearrange a role position on the layout pages for this template:

i. First remove the role from the template using the procedure described in step b above.

ii. Re-add the role in the correct layout page and role position using the procedure described in step a above.

d. To add a layout page to this template:

i. Locate the layout page after which you want a new layout page. Use the buttons beneath the layout to navigate between layout pages.

ii. If an additional layout page needs to be created, click the **New** button under the layout page. A new page will be created after the current page and this new page will automatically be displayed.

e. To delete a layout page from this template:

i. Locate the layout page you want to remove. Use the buttons beneath the layout to navigate between layout pages.

ii. To delete the current layout page number, click the **Delete** button under the layout page. A popup dialog will ask for confirmation for the deletion. Click the **OK** button. Any roles on the page will be returned to the Available Roles list. If there is only a single layout page for a category, this page cannot be deleted.

12. When you have completed modifying the roles and layout for this template, click the **Save** button at the top of the screen to save the modification to this template.
13. A successful template update message will appear.
14. If this template has been associated with an MDC Station location and is being used on some MDC Stations, those MDC Stations will need to be rebooted before the template changes will take effect. If you are uncertain of which MDC Stations are impacted, it is recommended that all MDC Stations be rebooted during a suitable maintenance period once all the role related configuration changes have been completed. See Section 13.11 *Reboot All MDC Stations* or Section 13.10 *Reboot MDC Station* for the detailed procedure.

12.8.4 Delete a Template

Description:

This procedure describes how to delete an existing role template.

A role template cannot be deleted if the template is in use against one or more Station Locations.

Required information:

- Name of role template to be deleted

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Roles** from either the main task area or the Configure submenu on the left navigation menu.
4. The Roles screen appears. The main Roles screen is the View screen, which displays a list of roles in a table format. On a newly installed MDC, there will initially be no roles to display.
5. Click **Templates** from the Roles main task working area to create a role category on the MDC.
6. The Templates screen appears.

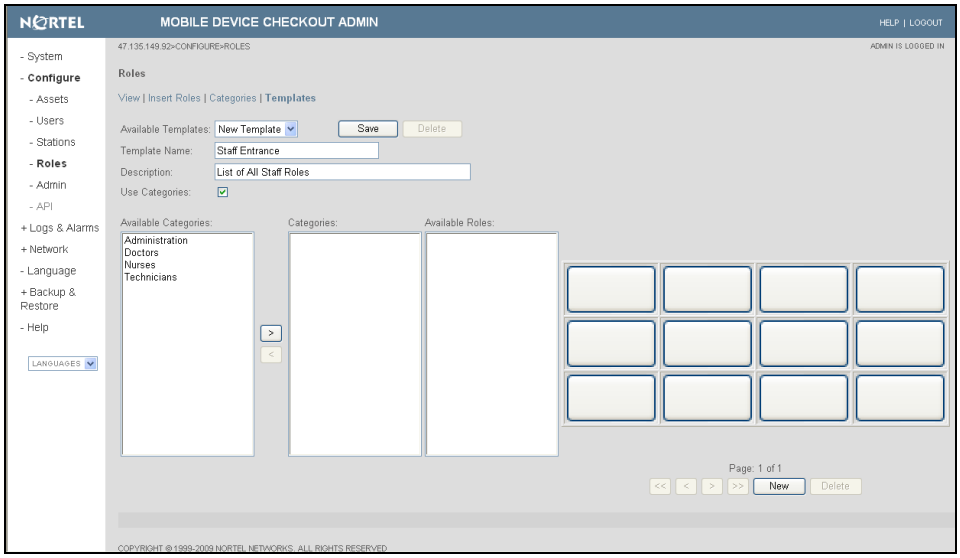


Figure 174: Template Screen of MDC Admin GUI

7. To delete an existing template, select the template name which needs to be deleted from the pulldown menu of **Available Templates**.
8. The information for the select template will be displayed on the screen. Confirm this is the template which needs to be deleted.
9. Click the **Delete** button to delete the shown template.
10. A delete confirmation popup dialog will appear. Click **OK** to confirm deleting the template.

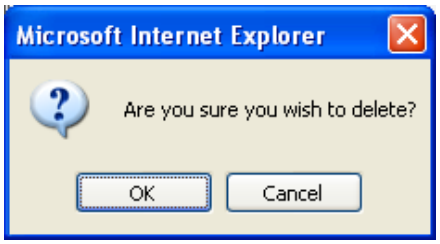


Figure 175: Delete Template Confirmation Dialog

A successful template delete message will appear.

Otherwise, a warning popup dialog will appear if the role template cannot be deleted because the template is in use against one or more Station Locations. Click the **OK** button. You will need to remove this role template from any Station Locations where it is being used before you can successfully delete this role template. See Section 13.7 *Modify Station Location* for the detailed procedure.

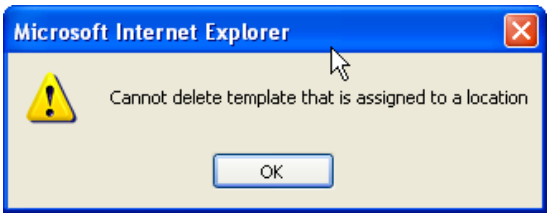


Figure 176: Template Assigned to Station Location Warning Dialog

13 Managing MDC Stations

This section describes procedures and MDC Admin GUI screens associated with managing the MDC Stations.

The number of stations permitted on an MDC is controlled by license. At the bottom of the station screens, the total number of licensed stations is displayed, along with a running tally of the number of licensed stations in use. It is possible for an error message to appear, indicating that there are no license files, OR a warning message that all licenses for stations are in use. When the license file is updated, new license information may not appear for up to 5 hours on existing MDC Admin GUI sessions. However, the user may choose to manually refresh their licensing information. Refer to Section 7 *MDC Licensing and Keycode Retrieval System (KRS)* for more information on MDC licensing.

The MDC Station screen graphics are controlled by files located on the MDC Server. These files are downloaded to the MDC Station during registration and initialization. The MDC Station screen graphics are hardware specific so the graphics available to an MDC Station are based on its hardware type. The graphics displayed on a MDC Station is determined its **station location**. Each station location is specific to a station hardware type. As well, the administrator can associated a **station graphics template** by selecting from the list of graphic templates available for a particular station hardware type.

If the MDC Server has been licensed for roles, additional role related information may be required when creating a new station location. The role template will specify which roles will be available during checkout at an MDC Stations based on its station location.

The section contains the following procedures:

- Add MDC Station
- View MDC Stations
- Language on MDC Station
- Set Message Banner and Help Number for Stations
- View Station Locations
- Insert Station Location
- Modify Station Location
- Delete Station Location
- Update MDC Station Information
- Reboot MDC Station
- Reboot All MDC Stations
- Delete MDC Station
- Relocate MDC Station

Other MDC Station related procedures are:

- The document NN49010-501 Nortel Healthcare Solutions MDC Deployment Guide contains the initial configuration, initialization and test procedures for the MDC Stations hardware devices. It also describes how to create a station graphic template to customize the logo shown on the MDC Stations screens.

13.1 Add MDC Station

The MDC Stations are configured to communicate with the MDC Server. The list of MDC Stations will be automatically populated on the MDC Admin GUI, so there is no need to manually add stations. See Section 13.2

View MDC Stations for details on viewing the list of MDC Stations. See the document NN49010-501 Nortel Healthcare Solutions MDC Deployment Guide for details on configuring and customizing the MDC Stations.

MDC Stations are uniquely identified by their MAC addresses. In addition, their IP addresses and hostnames are displayed in the View Stations screen of the MDC Admin GUI. In order for the hostnames of the MDC stations to appear in the MDC Admin GUI, the DNS will need to be configured for the MDC Stations.

The number of stations permitted on an MDC is controlled by license. On the station screens, the total number of licensed stations is displayed along with a running tally of the number of licensed stations in use. It is possible for an error message to appear indicating that there are no license files, OR a warning message that all licenses for stations are in use. When the license file is updated, new license information may not appear for up to 5 hours on existing MDC Admin GUI sessions. However, the user may choose to manually refresh their licensing information. Refer to Section 7 *MDC Licensing and Keycode Retrieval System (KRS)* for more information on MDC licensing.

When the number of permitted licensed stations has been reached, any subsequent MDC Stations which initiate communication with the MDC Server will not be allowed to register and will not be functional. These stations will appear on the View Stations screen, but their Status icon will be red to indicate that they are not functional. The number of licensed stations will need to be increased to remedy the problem or existing unused stations that are using a license will need to be deleted to make those existing stations' licenses available. It is also possible that the licensing information has been changed; the MDC Stations that are unable to register may need to be rebooted for the new licensing information to take effect.

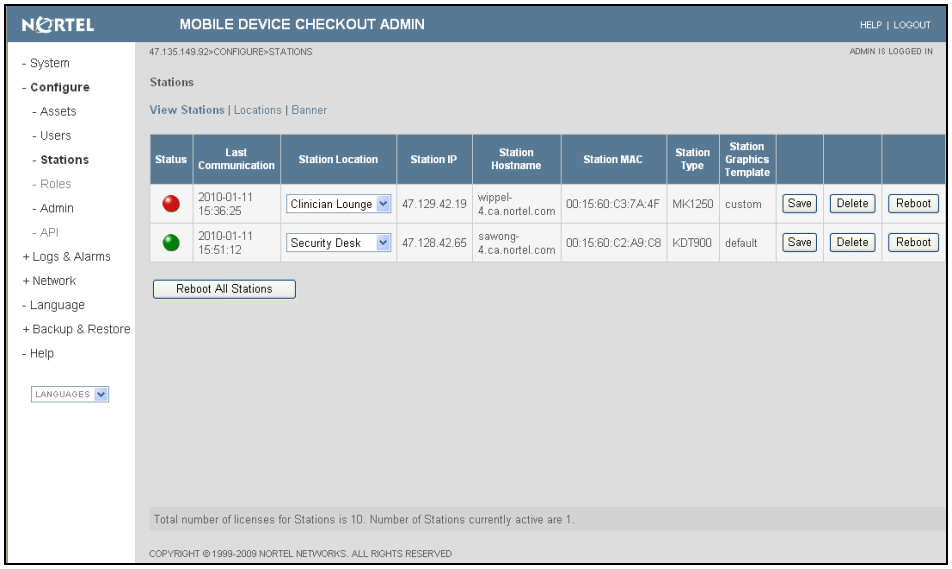


Figure 177: View Stations

13.2 View MDC Stations

Description:

This procedure describes how to view the MDC Stations on the MDC Admin GUI.

The View Station screen is automatically refreshed every 30 seconds with the most recent list of MDC Stations and their status. The status of a MDC Station reflects whether the device has been able to register and its ability to communicate with the MDC Server.

Note: The DNS server must be configured for MDC Stations before the hostname will be displayed in the MDC Admin GUI.

Required information:

- None

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Stations** from either the main task area or the Configure submenu on the left navigation menu.
4. The Stations screen appears. The main Stations screen is the View Stations screen, which displays a list of all the stations in a table format. On a newly installed MDC, there will initially be no stations to display.

   The columns in the stations table are:

   - Status: This field will display a color-coded icon to denote the status of communications with the station.
     - If the icon is green, it indicates that the station was able to register, there was an available license for the station and it has responded to the most recent heartbeat handshake with the MDC Server.
     - If the icon is red, it indicates that either the station was unable to register with the MDC Server because of an insufficient number of station licenses, OR there is a communication problem with this station for more than 2 minutes. Looking at the running tally of station licenses or referring to the MDC logs can help to determine the problem. You may also want to refresh the licensing information in the MDC Admin GUI and MDC Station. See Section 7.7 *Update Licensing Information in the MDC* Application for the details.
   - Last Communication: The time of the last communication with the station. This may be either due to activity at this station or because of the regularly scheduled heartbeat handshake between the MDC Stations and the MDC Server. The format is date and time with Year-Month-Day HH:MM:SS using a 24-hour time.
   - Station Location: Text description of the location of the station. This is a pulldown menu.
   - Station IP: IP address of the station.
   - Station Hostname: Hostname of the station.
   - Station MAC: MAC number of the station.
   - Station Type: Station hardware model type
   - Station Graphic Template: Station presentation graphics template in use

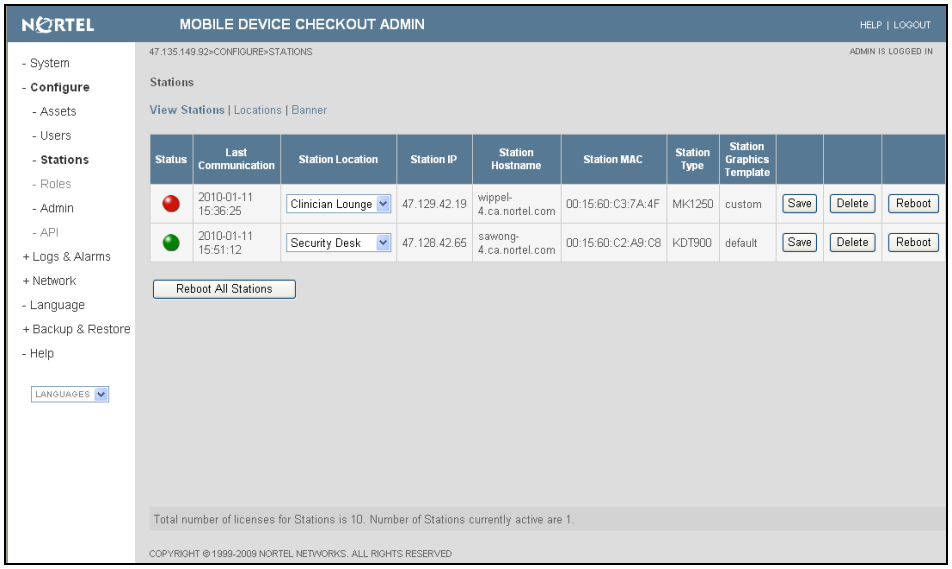


Figure 178: Stations Screen of MDC Admin GUI

13.3 Language on MDC Station

Description:

This configures the languages which will be supported in the MDC Stations and the order in which the languages will appear on the MDC Stations. By default, English is selected; if nothing is selected, the default language used on the MDC station will be English.

WARNING: This procedure is service affecting when the MDC Station is rebooted.

Required information:

- Languages and order of languages on the MDC Station

Steps:

1. From the MDC Admin GUI, click the **Language** task on the left navigation menu. (This is the first occurrence of Language in the navigation list and not the pulldown menu at the bottom of the list).
2. The Language screen of the Mobile Device Checkout Admin appears.
3. Using the following actions, select the languages and the order in which the languages will appear on the MDC Station:
    a. Uncheck the boxes of all languages which should not appear on the MDC Station.
    b. For each language to be supported on the MDC Station, click the check box beside the language to select it for inclusion.
    c. Re-organize the list of supported languages into the order in which they need to appear on the MDC Station by clicking the **up** or **down** selection beside a language to move its position in the list.

    For each action, a pop-up dialog will appear to remind the user that this change will not take effect until the MDC Stations have been restarted. Click the **OK** button. A successful language update message will also appear. Continue configuring until the necessary languages have been selected and their order arranged.

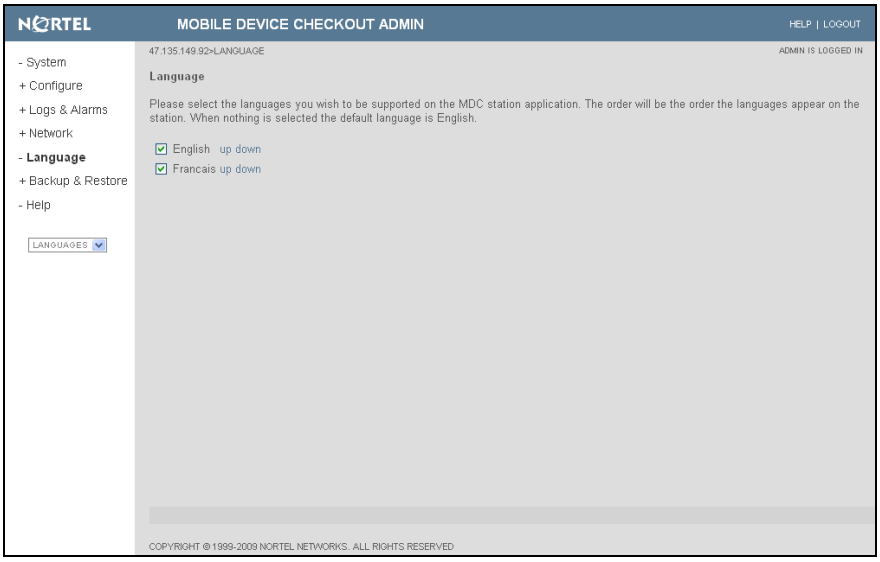


Figure 179: Configuring Languages displayed on MDC Station

4. The language changes will not take effect on MDC Station screens until that MDC Station is rebooted. See Section 13.11 *Reboot All MDC Stations* or Section 13.10 *Reboot MDC Station* for the detailed procedure.

13.4 Set Message Banner and Help Number for Stations

Description:

This procedure sets the text of the message banner and help number displayed on the stations.

Note: The banner message is a feature not utilized in the current MDC Release

WARNING: This procedure is service affecting when the MDC Station is rebooted.

Required information:

- [Optional] Message banner
- Help Desk number

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Stations** from either the main task area or the Configure submenu on the left navigation menu.
4. The Stations screen appears. The main Stations screen is the View Stations screen, which displays a list of all the stations in a table format. On a newly installed MDC, there will initially be no stations to display.
5. Click the **Banner** menu option from the main task area.
6. The Manage Station screen appears.

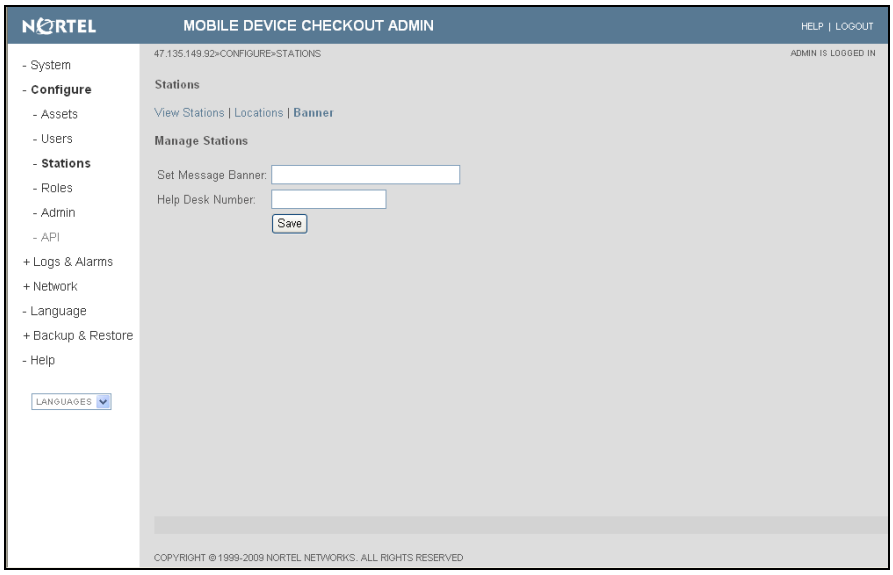


Figure 180: Manage Station Screen of MDC Admin GUI

7. You can ignore the text field labeled **Set Message Banner** and leave this field blank. The banner message is a feature not utilized in the current MDC Release.
8. Type in the Help Desk number in the text field labeled **Help Desk Number.**
9. Click **Save.**
10. A pop-up dialog will appear to remind the user that this change will not take effect until the MDC Stations have been restarted. Click the **OK** button. A message indicating the success of the action will also appear.
11. These changes will not take effect on MDC Station screens until that MDC Station is rebooted. See Section See Section 13.11 *Reboot All MDC Stations* or Section 13.10 *Reboot MDC Station* for the detailed procedure.

13.5 View Station Locations

Description:

This procedure describes how to view the list of the station locations where MDC Stations can be installed.

This list is used on the View Stations screen to select the location for individual MDC Stations. By default, there is an ADMIN TEST location always defined.

If the MDC Server has been licensed for roles, the administrator can view these additional columns on the Locations screen:

- Role Template: this column indicates the role template associated with a MDC Station location. This will enable a MDC Station with this MDC location to offer role assignment via the configured role template. If **No Template** is selected, role assignment will not be used with MDC Stations using this MDC Station location.
- Role Only: this column permits the administrator to restrict any check out of assets from a MDC Station with this MDC Station location to assigning only the role phone number to the primary key on the phone. This Role Only designation can only apply when a role template has been associated with the MDC Station location.

For more information on roles and role templates, refer to Section 12 *Managing Roles*.

For more information on customizing station graphics, refer to the document NN49010-501 Nortel Healthcare Solutions MDC Deployment Guide which describes the initial configuration, initialization and test procedures for the MDC Stations devices.

Note: The support of roles is controlled by license. If the licensing information has changed within the last 5 hours, you may need to manually refresh the licensing information using the procedure described in Section 7.7 *Update Licensing Information in the MDC.* Without sufficient licenses for roles, the fields relating to roles template administration will not be visible on the Locations screen. Refer to Section 7 *MDC Licensing and Keycode Retrieval System (KRS)* for more information on MDC licensing.

Note: The list of station locations is presented on a pulldown menu on the MDC Station during the registration process. During registration, the administrator selects a station location for the MDC Station. Each MDC Station will take a snapshot of the list of station locations configured at the time the MDC Station reboots. If station locations are modified (additions, deletions or changes) on the MDC Admin GUI after the MDC Station reboots, the MDC Station will need to be rebooted to update its list of station locations on the registration page. In addition, after an MDC Station has completed its initial registration with the MDC Server and is visible from the View Station screen, its location can be updated by the administrator from the View Station Screen.

Required information:

- None

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Stations** from either the main task area or the Configure submenu on the left navigation menu.
4. The Stations screen appears. The main Stations screen is the View Stations screen, which displays a list of all the stations in a table format. On a newly installed MDC, there will initially be no stations to display.
5. Click the **Locations** menu option from the main task area.
6. The Locations screen appears. This is a list of the locations where stations are destined to be installed. Additional columns relating to roles (Role Template and Role Only) are only displayed if roles are licensed on the MDC Server. On a newly installed MDC, there will initially only be the default ADMIN TEST location.

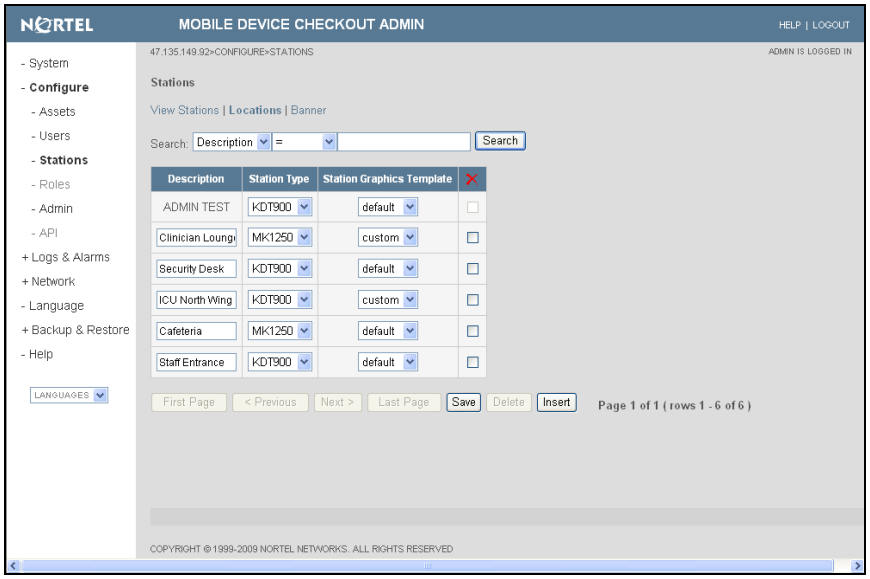


Figure 181: Locations Screen without Roles on MDC Admin GUI

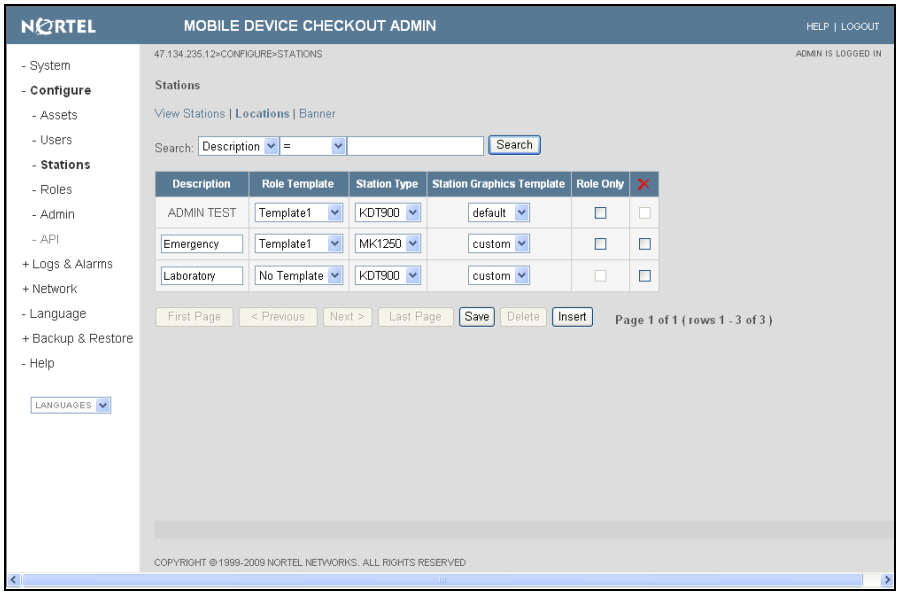


Figure 182: Locations Screen with Roles on MDC Admin GUI

The columns in the Location table are:

a. Description: Brief text description of the station location. The description is used to identify the location and should be unique.

b. Role Template: the role template associated with any MDC Station at this location. “No Template” indicates this location will not be using for role assignment. This column is only visible if roles are licensed for this MDC Server.

c. Station Type: Type of MDC Station hardware deployed at a given station location.

d. Station Graphics Template: The presentation graphics used on the MDC Stations deployed at a station location. “Default” indicates no custom graphics are being used.

e. Role Only: When checked, this column indicates that checkout of assets this MDC Station location will be restricted to assigning only the role phone number to the primary key on the phone. This column is only visible if roles are licensed for this MDC Server.

f. Delete: This field is checked to delete the station location from MDC.

When there are a large number of station locations in the list, only some of the locations will be displayed on the screen at a time. This is considered a “page.” The page number is shown on the screen along with the total number of available pages at the bottom of the table to help orient the user within the station location table. The equivalent row information for these entries in the station location table is also given in parentheses.

There are a number of options to view other station locations not displayed on the screen:

- Paging
- Sort
- Search

See Section 5.2.4 *MDC Admin GUI Paging, Sort, and Search* for a description of paging, sorting and searching and an explanation of how to use these features.

13.6 Insert Station Location

Description:

This procedure describes how to create a new station location.

A graphic template customizes the appearance of the MDC Station screens. A graphic template can be associated with a station location to customize the screens of MDC Stations based on their station location. Additional details on defining station graphic templates can be found in document NN49010-501 Nortel Healthcare Solutions MDC Deployment Guide.

If the MDC Server has been licensed for roles, additional role related information may be required when creating a new station location. This specifies the roles available during checkout at MDC Stations based on their station location. Additional details on roles can be found at Section 12 *Managing Roles*.

Note: The list of station locations is presented on a pulldown menu on the MDC Station during the registration process. During registration, the administrator selects a station location for the MDC Station. Each MDC Station will take a snapshot of the list of station locations configured at the time the MDC Station reboots. If station locations are modified (additions, deletions or changes) on the MDC Admin GUI after the MDC Station reboots, the MDC Station will need to be rebooted to update its list of station locations on the registration page. In addition, after an MDC Station has completed its initial registration with the MDC Server and is visible from the View Station screen, its location can be updated by the administrator from the View Station Screen.

Required information:

- Brief text description of the station location
- Type of MDC Station hardware which will be used at this location
- Station Graphic Template which will be used on MDC Stations at this location
- Role Template name for each station location. Only required if roles are licensed on MDC.

- Whether role assignments from a station location will be Role Only. Only required if roles are licensed on MDC and if a role template has been selected for the station location.

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Stations** from either the main task area or the Configure submenu on the left navigation menu.
4. The Stations screen appears. The main Stations screen is the View Stations screen, which displays a list of all the stations in a table format. On a newly installed MDC, there will initially be no stations to display.
5. Click the **Locations** menu option from the main task area.
6. The Locations screen appears. This is a list of the locations where stations are destined to be installed. Additional columns relating to roles (Role Template and Role Only) are only displayed if roles are licensed on the MDC Server. On a newly installed MDC, there will initially only be the default ADMIN TEST location.



Figure 183: Locations Screen without Roles on MDC Admin GUI

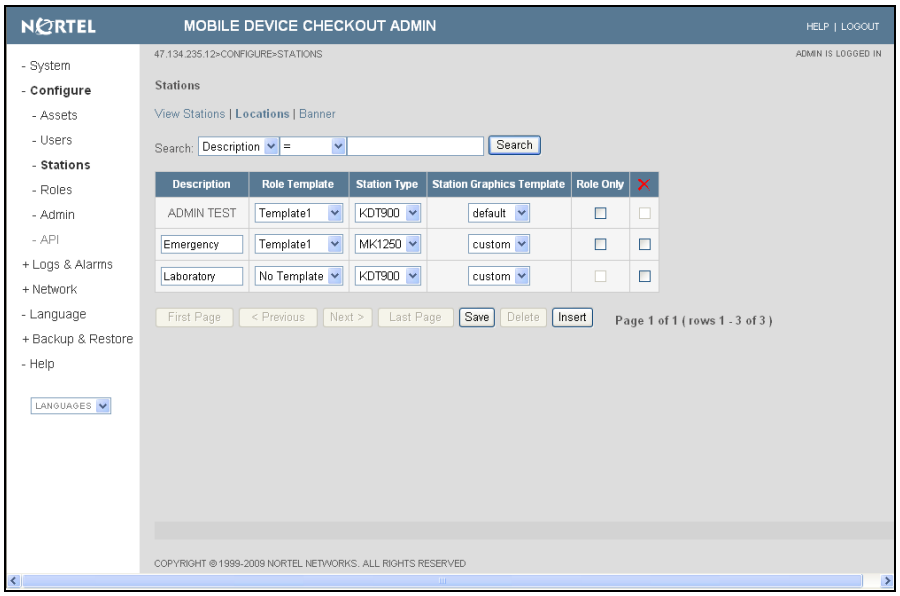


Figure 184: Locations Screen with Roles on MDC Admin GUI

7. Click the **Insert** button to add a new station location. A popup window will appear to enter the new station location information:
    a. **Description**: Type in a brief text description of the station location. The description is used to identify the location and should be unique.
    b. **Role Template**: **Select** the role template for this location from the pulldown menu. If this location will not be used for role assignment, ensure the Role Template is **No Template**. This field, Role Template, is only visible if roles are licensed for this MDC Server.
    c. **Station Type**: **Select** from the pulldown menu the type of MDC Station hardware deployed at this given station location.
    d. **Station Graphics Template**: **Select** from the pulldown menu the presentation graphics used on the MDC Stations deployed at this station location. **Default** indicates no custom graphics are being used.
    e. **Role Only**: If checkout of assets from this MDC Station location will be restricted to assigning only the role phone number to the primary key on the phone, **check** the **Role Only** box. This field, Role Only, can only be edited if roles are licensed for this MDC Server and a role template has been selected.

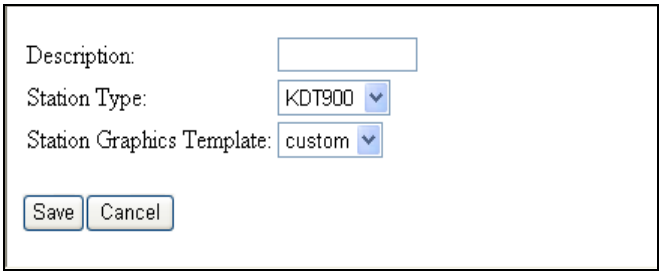


Figure 185: Insert New Station Location Window (without Roles)

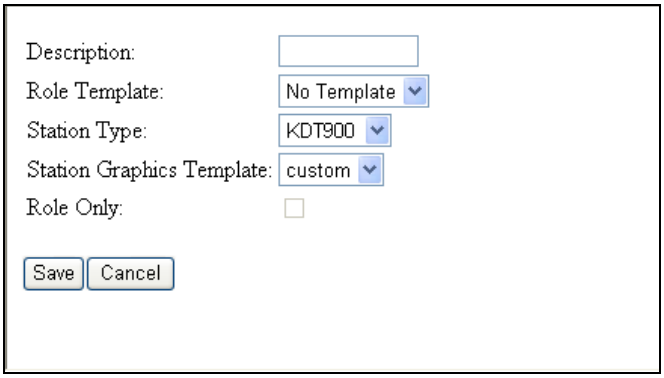


Figure 186: Insert New Station Location Window (with Roles)

8. Click the **Save** button to create a new station location.
9. A message indicating the success of the action will be displayed. If successful, the Station Location table will be updated with the newly added station location.
10. Any MDC Stations currently on the registration page will need to be rebooted before the change to the list of locations will be visible at the MDC Station. See Section 13.11 *Reboot All MDC Stations* or Section 13.10 *Reboot MDC Station* for the detailed procedure.

13.7 Modify Station Location

Description:

This procedure describes how to update the list of locations for MDC Stations.

WARNING: This procedure may be service affecting if MDC Stations need to be rebooted.

Note: The support of roles is controlled by license. If the licensing information has changed within the last 5 hours, you may need to manually refresh the licensing information using the procedure described in Section 7.7 *Update Licensing Information in the MDC.* Without sufficient licenses for roles, the fields relating to roles template administration will not be visible on the Locations screen. Refer to Section 7 *MDC Licensing and Keycode Retrieval System (KRS)* for more information on MDC licensing. For more information on roles and role templates, refer to Section 12 *Managing Roles*.

Note: The list of station locations is presented on a pulldown menu on the MDC Station during the registration process. During registration, the administrator selects a station location for the MDC Station. Each MDC Station will take a snapshot of the list of station locations configured at the time the MDC Station reboots. If station locations are modified (additions, deletions or changes) on the MDC Admin GUI after the MDC Station reboots, the MDC Station will need to be rebooted to update its list of station locations on the registration page. In addition, after an MDC Station has registration with the MDC Server and is visible from the View Station screen, its location can be updated by the administrator from the View Station Screen.

Required information:

- Existing station location description
- At least one of the following updated Station location information:
    - Updated station location description
    - Updated type of MDC Station hardware which will be used at this location

- Updated Station Graphic Template which will be used by MDC Stations at this location
- Updated role template for each station location. Only applicable if roles are licensed on MDC.
- Updated status of whether role assignments from a station location will be Role Only. Only applicable if roles are licensed on MDC and a role template has been selected.

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Stations** from either the main task area or the Configure submenu on the left navigation menu.
4. The Stations screen appears. The main Stations screen is the View Stations screen, which displays a list of all the stations in a table format. On a newly installed MDC, there will initially be no stations to display.
5. Click the **Locations** menu option from the main task area.
6. The Locations screen appears. This is a list of the locations where stations are destined to be installed. Additional columns relating to roles (Role Template and Role Only) are only displayed if roles are licensed on the MDC Server. On a newly installed MDC, there will initially only be the default ADMIN TEST location.

   Note: The **Save** button, below the Location table, does not become enabled until there are changes made to entries in the Admin table.
7. Locate the Location Description entry that needs to be updated. See the procedures on View Station Location for options to sort and search the Location table. The following fields can be updated from the Location screen:
   a. **Description**: Type in the updated brief text description of the station location. The description is used to identify the location and should be unique. Note: the description name of ADMIN TEST cannot be changed as ADMIN TEST is a mandatory station location used during MDC Station hardware commissioning.
   b. **Station Type**: Select from the pulldown menu the updated type of MDC Station hardware deployed at this given station location.
   c. **Station Graphics Template**: Select from the pulldown menu the updated presentation graphics used on the MDC Stations deployed at this station location. **Default** indicates no custom graphics are being used.
   d. If roles are licensed for this MDC Server, the following role related fields can be updated:
      i. **Role Template**: Select the updated role template for this location from the pulldown menu. If this location will not be used for role assignment, ensure the Role Template is **No Template**.
      ii. **Role Only**: If checkout of assets from this MDC Station location will be restricted to assigning only the role phone number to the primary key on the phone, **check** the **Role Only** box. This field, Role Only, can only be edited if a role template has been selected for this entry.

      The Role Template and Role only columns will only be visible if roles are licensed on the MDC Server.

   Once changes have been made to fields in the Location table, the **Save** button, below the table, becomes enabled to indicate that there are Location entries which have been modified. You can modify multiple entries in the Location table. If you use the page control buttons, the entries you have modified may not be displayed on the screen.

   If you attempt to navigate away from the Locations screen while there are unsaved changes, a warning dialog will pop up.

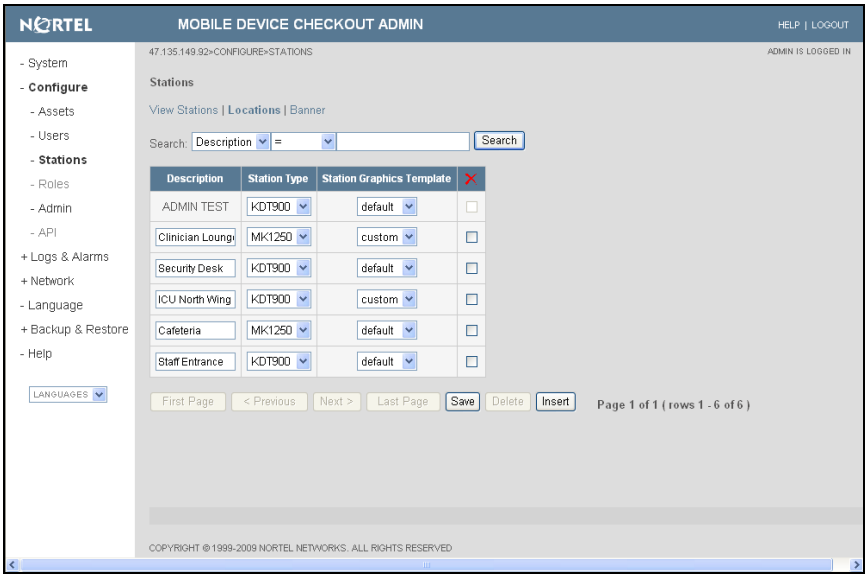


Figure 187: Modifying Station Location (without Roles)

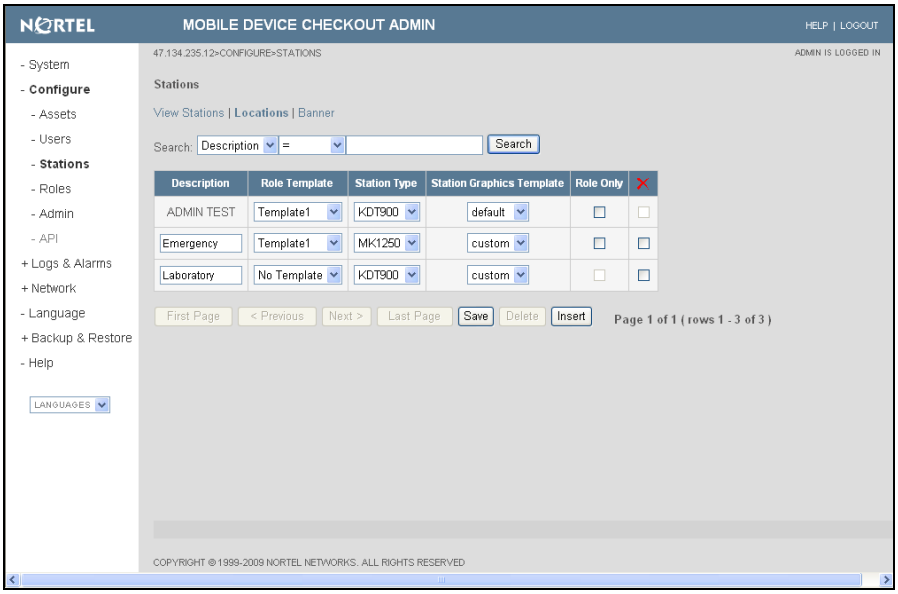


Figure 188: Modifying Station Location with Roles

8. Click the **Save** button at the bottom of the table to save all the updated to the Location table.
9. A message indicating the success of the action will be displayed. If successful, the location table will be updated. Verify that the modified location(s) are displayed.
10. Any MDC Stations currently on the registration page will need to be rebooted before the changes to the list of location descriptions will be visible at the MDC Station. See Section 13.11 *Reboot All MDC Stations* or Section 13.10 *Reboot MDC Station* for the detailed procedure.
11. If the Station Type, Station Graphic Template, Role Template or Role Only fields were changed, any MDC Station using a station location which was modified will need to be rebooted before the changes will be

visible at the MDC Station. See Section 13.10 *Reboot MDC Station* or Section 13.11 *Reboot All MDC Stations* for the detailed procedure.

13.8 Delete Station Location

Description:

This procedure describes how to delete an MDC Station location.

NOTE: the ADMIN TEST location cannot be deleted as ADMIN TEST is a mandatory station location used during MDC Station hardware commissioning.

WARNING: This procedure may be service affecting if MDC Stations needs to be rebooted.

WARNING: It is recommended to save any changes made to locations in the Station Locations screen prior to deleting locations. The Save button is enabled when there are unsaved changes. A warning will be given if there are any unsaved updates to the Locations table that may be lost.

WARNING: The operator will not be allowed to delete a location which is actively being used as the location for a station. If a particular location is being decommissioned, you must select new locations for all the stations which are using that particular location first.

WARNING: The list of station locations is presented on a pulldown menu on the MDC Station during the registration process. Each MDC Station will take a snapshot of the list of station locations configured at the time the MDC Station reboots. If station locations are modified (additions, deletions or changes) on the MDC Admin GUI after the MDC Station reboots, the MDC Station will need to be rebooted to update its list of station locations on the registration page. In addition, after an MDC Station has registration with the MDC Server and is visible from the View Station screen, its location can be updated by the administrator from the View Station Screen.

Required information:

- Existing station location description to delete

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Stations** from either the main task area or the Configure submenu on the left navigation menu.
4. The Stations screen appears. The main Stations screen is the View Stations screen, which displays a list of all the stations in a table format. On a newly installed MDC, there will initially be no stations to display.
5. Click the **Locations** menu option from the main task area.
6. The Locations screen appears. This is a list of the locations where stations are destined to be installed. Additional columns relating to roles (Role Template and Role Only) are only displayed if roles are licensed on the MDC Server. On a newly installed MDC, there will initially only be the default ADMIN TEST location.

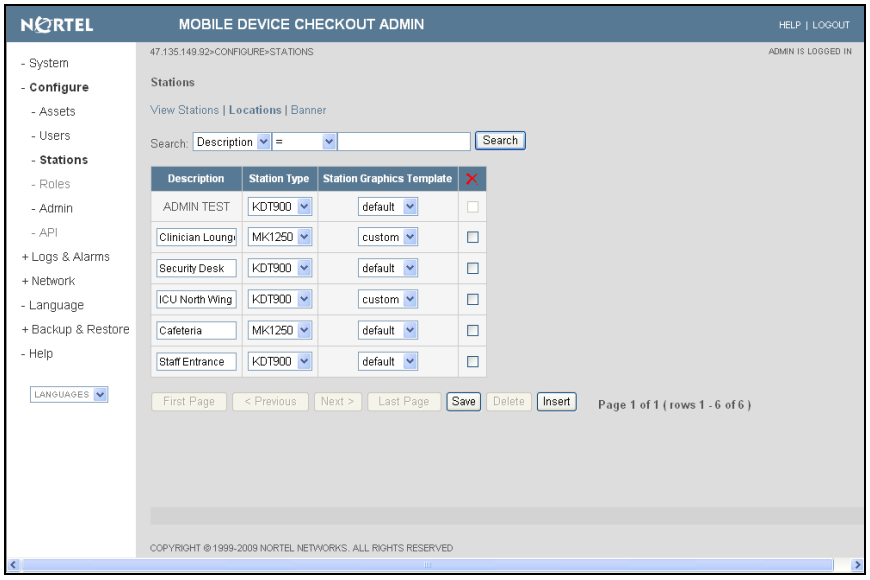


Figure 189: Locations Screen without Roles on MDC Admin GUI

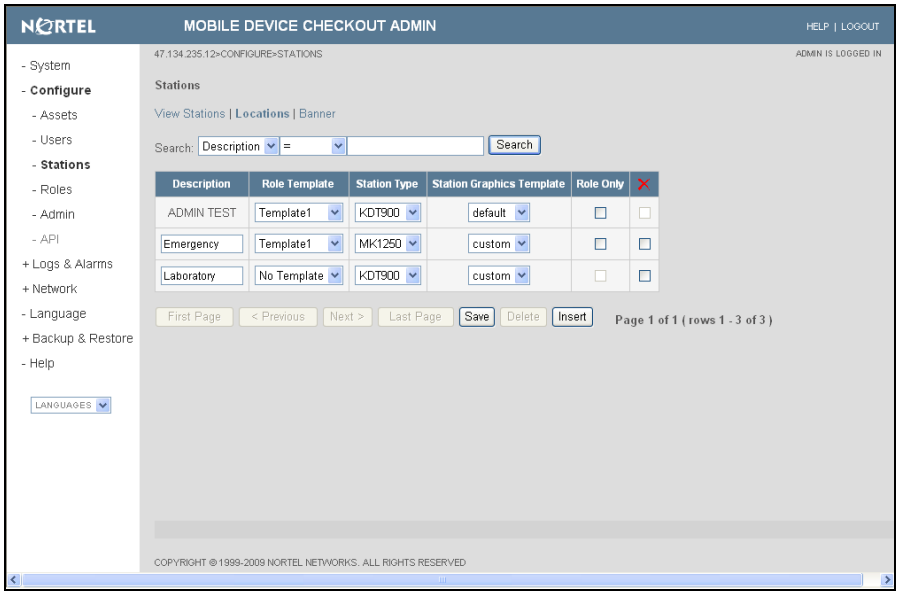


Figure 190: Locations Screen with Roles on MDC Admin GUI

7. Locate the table entry of the location description(s) you want to remove. See the procedures on View Station Location for options to sort and search the Location table. Check the box in the **Delete** column (rightmost column in the table) to delete a particular station location. Once any station location has been marked for deletion from the Locations table, the **Delete** button, below the table, becomes enabled to indicate that there are pending deletions. You may mark multiple locations for deletion. If you use the page control buttons, the entries you have marked for deletion may no longer be displayed on the screen.

   If you attempt to navigate away from the Locations screen while there are station locations marked for deletion, a warning dialog will pop up.

NOTE: the ADMIN TEST location cannot be deleted as ADMIN TEST is a mandatory station location used during MDC Station hardware commissioning.

8. Click the **Delete** button, below the Locations table, to delete the marked station location(s).
9. A delete confirmation popup dialog will appear. Click **OK** to confirm deleting the station location description(s).

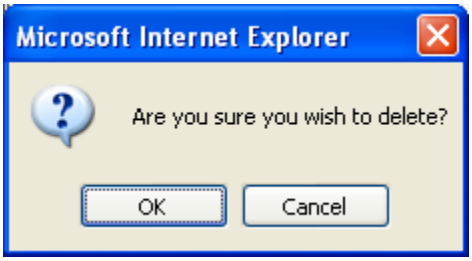


Figure 191: Delete Location Confirmation Dialog

10. A message indicating the success of the delete action will be displayed. If successful, the Locations screen will be refreshed and the deleted location(s) will be removed from the list of station locations.

    An error dialog may appear if any location is currently being used as the location for a station(s). If this is the case, you must select new locations for all the stations which are using that particular location first before deleting this location. See Section 13.9 *Update MDC Station Information* for steps on how to change the location of a station. Any other unused station locations marked for deletion will be deleted.
11. Any MDC Stations currently on the registration page will need to be rebooted before the change to the list of locations will be visible at the MDC Station. See Section 13.10 *Reboot MDC Station* for the detailed procedure.

13.9 Update MDC Station Information

Description:

This procedure describes how to update information for MDC Stations. Only the station location can be changed from the GUI. For accuracy, the station location is set from the station screen when the MDC Station is initially powered up and goes through its initial registration process with the MDC Server. This field should be changed with caution from the GUI when a correction is needed.

WARNING: This procedure is service affecting if the MDC Station needs to be rebooted.

WARNING: It is recommended that only a single entry row be modified at a time, as the Save will only save changes to a single entry row. Any updates to other entry rows in the View Station table will be lost when the table is refreshed after the Save.

WARNING: The location ADMIN TEST should be used with caution. Setting the MDC Station location to ADMIN TEST may cause the MDC Station to go through a registration process if it is rebooted or powered off/on. This means the MDC Station will not be operational without user intervention. This location is suitable only when the MDC Station is being tested prior to installation or if the MDC Station is being physically relocated.

Required information:

- MDC Station MAC address or hostname or IP address
- Updated station location description for this MDC Station

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Stations** from either the main task area or the Configure submenu on the left navigation menu.
4. The Stations screen appears. The main Stations screen is the View Stations screen, which displays a list of all the stations in a table format. On a newly installed MDC, there will initially be no stations to display.
5. Locate the Station entry that needs to be updated. Only update information for a single station at a time. To modify the station location, select the appropriate location from the pulldown menu of locations for stations. If an appropriate location does not appear, refer to Section 13.6 *Insert Station Location*.

   WARNING: The location ADMIN TEST should only be used with caution. Setting the MDC Station location to ADMIN TEST will cause the MDC Station to go through a registration process whenever it is rebooted or powered off/on. This means the MDC Station will not be operational without user intervention. This location is suitable only when the MDC Station is being tested prior to installation or if the MDC station is being physically relocated.

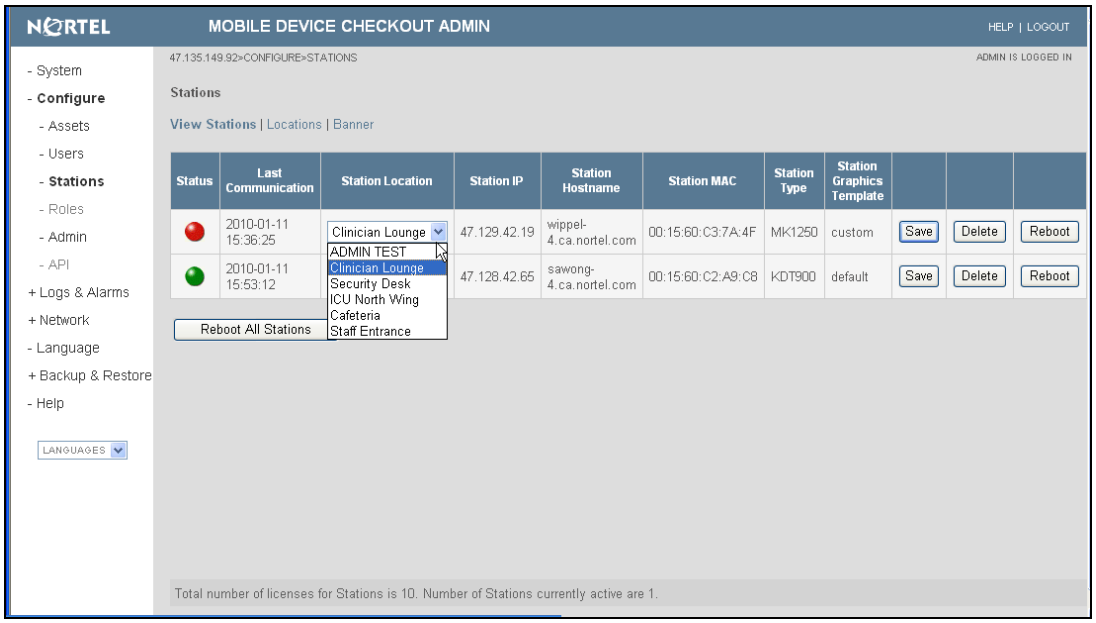


Figure 192: Select Station Location on MDC Admin GUI

6. Click the **Save** button on the row for that entry.
7. The stations table will be updated. Verify that the modified station location is displayed. Verify that a successfully updated message is displayed.
8. If roles have been licensed on this MDC Server, changing the station location for a MDC Station may impact the role template or role only attribute being used by this MDC Station. In this instance, the MDC Station will need to be rebooted before roles changes will be visible at the MDC Station. See Section 13.10 *Reboot MDC Station* for the detailed procedure.

13.10 Reboot MDC Station

Description:

This procedure describes how to reboot a single MDC Station.

WARNING: This procedure is service affecting.

WARNING: Any MDC Station with a station location of ADMIN TEST will reboot to the registration page and will not be operational without administrator intervention. The administrator can either select a location from the Station screen on the MDC Admin GUI OR the administrator can select the location from the kiosk screen to complete the registration.

WARNING: It is recommended to save any changes made to stations in the View Stations screen prior to rebooting. Any unsaved updates in the View Stations table will be lost when the table is refreshed after the reboot.

Required information:

- MDC Station MAC address or hostname or IP address

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Stations** from either the main task area or the Configure submenu on the left navigation menu.
4. The Stations screen appears. The main Stations screen is the View Stations screen, which displays a list of all the stations in a table format. On a newly installed MDC, there will initially be no stations to display.
5. Locate the Station entry that needs to be rebooted.

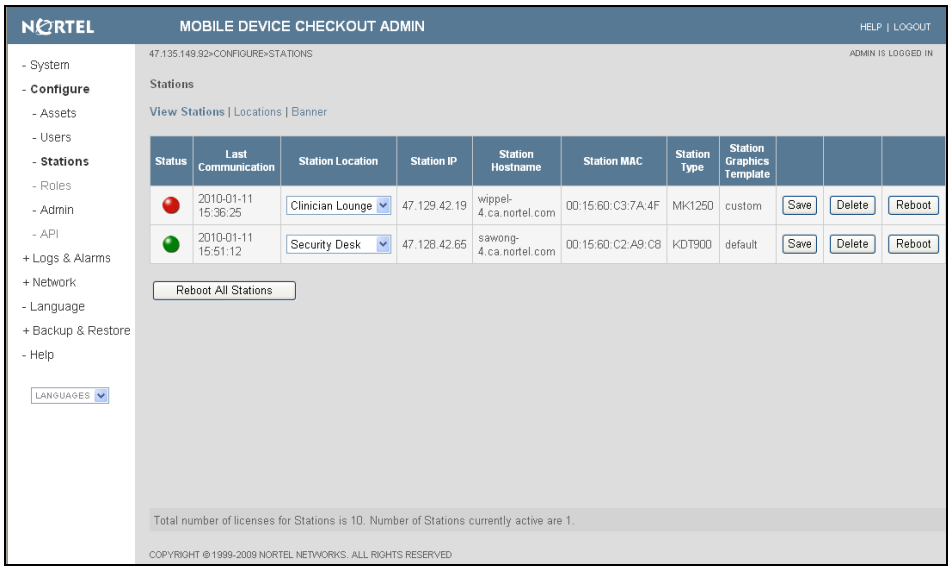


Figure 193: Reboot MDC Station on MDC Admin GUI

6. Click the **Reboot** button on the row for that entry.

7. A confirmation popup dialog will appear. Click **OK** to confirm rebooting the station. **WARNING**: Rebooting an MDC Station is service affecting.
8. The contents of the stations table will be refreshed. Verify a successfully initiated reboot message is displayed on the task area. This will indicate the MDC Station reboot has been started. NOTE: It may take several minutes for the MDC Station reboot to complete.

   If the reboot of the MDC Station could not be initiated, a popup dialog about the reboot failure will appear. Click **OK.** This failure may be due to communication problems with the MDC Station. Check the Status field for this MDC Station.

13.11 Reboot All MDC Stations

Description:

This procedure describes how to reboot all MDC Station.

WARNING: This procedure is service affecting.

WARNING: Any MDC Station with a station location of ADMIN TEST will reboot to the registration page and will not be operational without administrator intervention. The administrator can either select a location from the Station screen on the MDC Admin GUI OR the administrator can select the location from the kiosk screen to complete the registration.

WARNING: It is recommended to save any changes made to stations in the View Stations screen prior to rebooting. Any unsaved updates in the View Stations table will be lost when the table is refreshed after the reboot.

Required information:

- None

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Stations** from either the main task area or the Configure submenu on the left navigation menu.
4. The Stations screen appears. The main Stations screen is the View Stations screen, which displays a list of all the stations in a table format. On a newly installed MDC, there will initially be no stations to display.

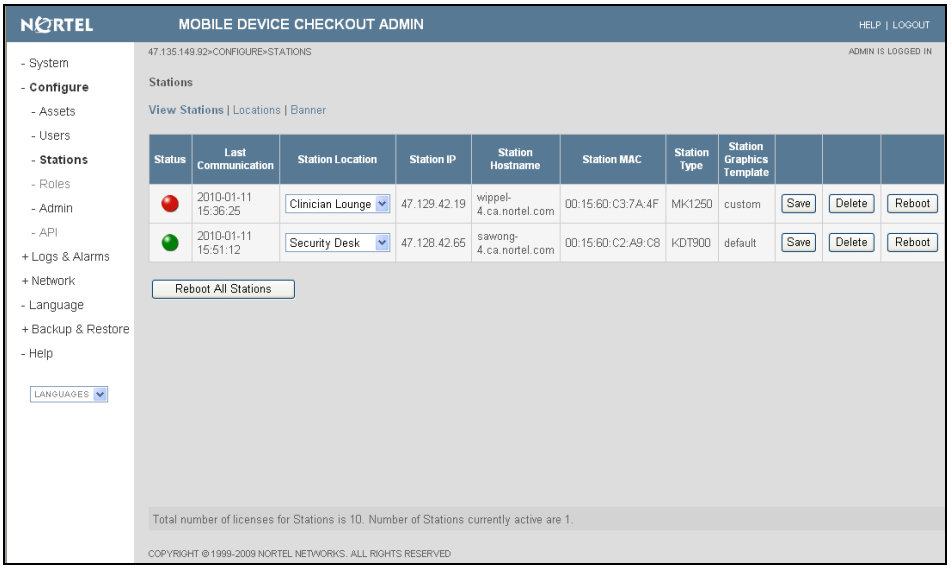


Figure 194: Reboot MDC Station on MDC Admin GUI

5. Click the **Reboot All Stations** button on the bottom of the stations table.
6. A confirmation popup dialog will appear. Click **OK** to confirm rebooting all the stations. **WARNING**: Rebooting an MDC Station is service affecting.

   A message will appear indicating the initiation of reboot on all of the stations may take several minutes.
7. The contents of the stations table will be refreshed. Verify a successfully initiated reboot message is displayed in the task area. This will indicate all the MDC Stations have successfully started rebooting

   If the reboot of one or more MDC Stations could not be initiated, a popup dialog will appear listing all the MDC Stations and their reboot initiated status. A failure to initiate reboot may be due to communication problems with the MDC Station. Check the Status field for the MDC Stations. The MDC logs will also indicate which MDC Station(s) did not reboot.

   NOTE: It may take several minutes for the MDC Station reboots to complete after a response message appears,

13.12 Delete MDC Station

Description:

This procedure describes how to delete an MDC Station from the MDC Admin GUI.

WARNING: It is recommended to save any changes made to stations in the View Stations screen prior to deleting locations. Any unsaved updates to other entry rows in the View Stations table will be lost when the table is refreshed after the delete.

WARNING: This procedure is service affecting.

WARNING: Once a station is deleted from the View Station screen, the station will be reset to the station registration page. The MDC Station will no longer be operational or visible from the MDC Administration GUI until a location is manually selected from the MDC Station screen.

Required information:

- MDC Station MAC address or hostname or IP address to delete

Steps:

1. From the MDC Admin GUI, click the **Configure** task on the left navigation menu.
2. The Configure screen of the Mobile Device Checkout Admin appears.
3. Click **Stations** from either the main task area or the Configure submenu on the left navigation menu.
4. The Stations screen appears. The main Stations screen is the View Stations screen, which displays a list of all the stations in a table format. On a newly installed MDC, there will initially be no stations to display.

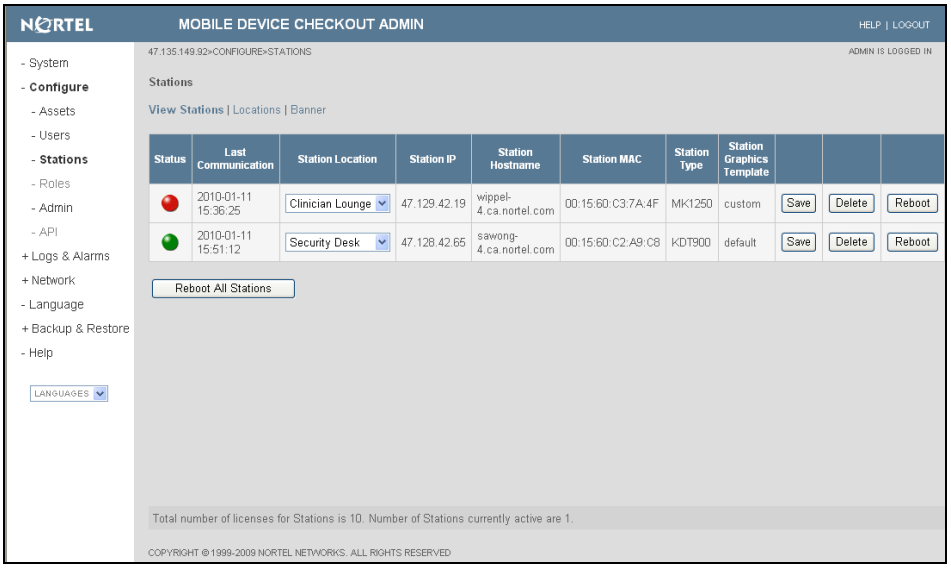


Figure 195: View Stations on MDC Admin GUI

5. Locate the station you want to remove. Click the **Delete** button on that table row to delete the station.
6. A delete confirmation popup dialog will appear. Click **OK** to confirm deleting the station.

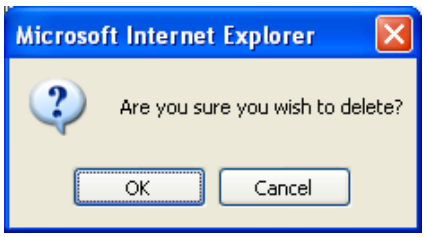


Figure 196: Delete Station Confirmation Dialog

7. The View Station screen will be refreshed and the latest list of stations will be displayed.
    a. Confirm that a successful deleted message appears.
    b. Confirm that the deleted station has been removed from the list of stations.

13.13 Relocate MDC Station

Description:

There are multiple ways to update the MDC Admin GUI when an MDC Station has to be relocated. The options described below are:

- Relocating an MDC Station when Future Location is Known
- Relocating an MDC Station when Future Location is Not Known

Note: In addition to the above options, it is also possible to delete the station when an MDC Station has to be physically relocated. This is not the recommended procedure but may be used if unavoidable. Using the delete procedure requires someone to be present at the MDC Station location to complete the registration process when the MDC Station is put back into use.

Required information:

- MDC Station MAC address or hostname or IP address to relocate
- Description of the future location of the MDC Station

13.13.1 Relocating an MDC Station when Future Location is Known

Note: If this is a new location with a new SSID for wireless MDC Stations, there may be additional steps needed to update the MDC Station configuration wireless profile for a new SSID. See document NN49010-501 Nortel Healthcare Solutions MDC Deployment Guide for further details on configuring MDC Stations.

When an MDC Station has to be physically relocated and the future location is known, the recommended procedure is:

1. If the future location is a new location for the MDC Station, add the description of the future location to the list of available station locations using the procedure in Section 13.6 *Insert Station Location*. Otherwise, a description of the station location should already exist in the MDC Administration GUI.
2. When the station is ready to be relocated, change the location of the MDC Station to its known future location in the MDC Administration GUI using the procedure in Section 13.9 *Update MDC Station Information*.
3. Power off the station and physically relocate the station per manufacturer's instructions. This will cause the status for the MDC Station to go red in the MDC Administration GUI because of the loss of communication between the MDC Server and the MDC Station.
4. Power on the MDC Station in its new location. At this point, if there are available station licenses, the MDC Station will automatically complete the registration process with its new location and the status of the MDC Station will change from red to green in the View Station screen on the MDC Administration GUI.
5. The main checkout screen should appear on the MDC Station. The station is now operational.

13.13.2 Relocating an MDC Station when Future Location is Not Known

Note: If this is a new location with a new SSID for wireless MDC Stations, there may be additional steps needed to update the MDC Station configuration wireless profile for a new SSID. See document NN49010-501 Nortel Healthcare Solutions MDC Deployment Guide for further details on configuring MDC Stations.

When an MDC Station has to be physically relocated and the future location is not known, the recommended procedure is:

1. When the station is ready to be decommissioned at its old location, first change the location of the MDC Station to **ADMIN TEST** from the MDC Administration GUI. See procedure in Section 13.9 *Update MDC Station Information*. This will force the MDC Station to go through the station registration process when it is rebooted in its new location, permitting the station location to be updated.
2. Power off the station and physically remove the station. This will cause the status for the MDC Station to go red because of the loss of communication between the MDC Server and the MDC Station.
3. When the future location is known, add the description of the future location to the list of available station locations if this is a new location for the MDC Stations. Use the procedure in Section 13.6 *Insert Station Location*. Otherwise, a description of the station location should already exist in the MDC Administration GUI before the station is powered on in its new location.
4. [Optional Step] Change the location of the MDC Station to its future location in the MDC Administration GUI using the procedure in Section 13.9 *Update MDC Station Information*. This is recommended (but not mandatory) as it will allow the MDC Station to be automatically registered if there are sufficient licenses.
5. Physically relocate the station in the future location per the manufacturer's instructions.
6. Power on the MDC Station in its new location.

   If the new location has not already been updated in the MDC Administration GUI, the MDC Station will go through the station registration process, where a station location can be selected from the station screen. Alternatively, the administrator can change the location of the MDC station on the View Station screen of the MDC Administration GUI using the procedure Section 13.9 *Update MDC Station Information*.

   Once the location has been selected, if there are available station licenses, the status of the MDC Station will change from red to green in the View Station screen of MDC Administration GUI.

   Note: Any new station locations added after the MDC Station has connected to the network will not automatically appear on the MDC Station registration page. Reboot the MDC Station to refresh the list of station locations on the registration page.
7. The main checkout screen should appear on the station. The station is now operational.

14 Using MDC Station

This section provides a brief overview of the using the MDC Station to check out and return phones. For additional information on using the MDC Station refer to these documents:

- NN49010-101 Nortel Healthcare Solutions MDC Station User Quick Reference Guide for CS 1000
- NN49010-103 Nortel Healthcare Solutions MDC Station with Roles User Quick Reference Guide for CS 1000
- NN49010-104 Nortel Healthcare Solutions MDC Station User Quick Reference Guide for CS 2100
- NN49010-105 Nortel Healthcare Solutions MDC Station with Roles User Quick Reference Guide for CS 2100

There must be at least one phone and user configured on MDC. See Section 10.2 *Insert New Asset* for the description of the steps to add an asset and Section 11.1 *Insert New Users* for the description of the steps to add a user. There must be an MDC Station configured and operational.

Optional, if roles are licensed, there can be a role template defined and deployed on the MDC Station.

This section describes:

- Check out a phone to a user at an MDC Station
- Return a phone at an MDC Station
- Presentation Conventions on MDC Station
- [Optional]Check out a phone to a location-tracked user
- [Optional] Return a phone assigned to a location tracked user
- Re-Assign a Phone from a User to another User at any MDC Station
- Assign a Phone from a User and Assign another phone to same User at any MDC Station

Ensure the phone has a fully charged battery and is powered on prior to attempting any of the above procedures.

14.1 Check out a phone to a user at an MDC Station

At the MDC Station, follow these steps to check out a phone to a user:

a. Press the **Checkout** button on the MDC Station screen.



Figure 197: Main MDC Station Screen

b. Scan the phone barcode as instructed.



Figure 198: Scan Device Barcode on MDC Station Screen

c. Scan the user barcode as instructed.

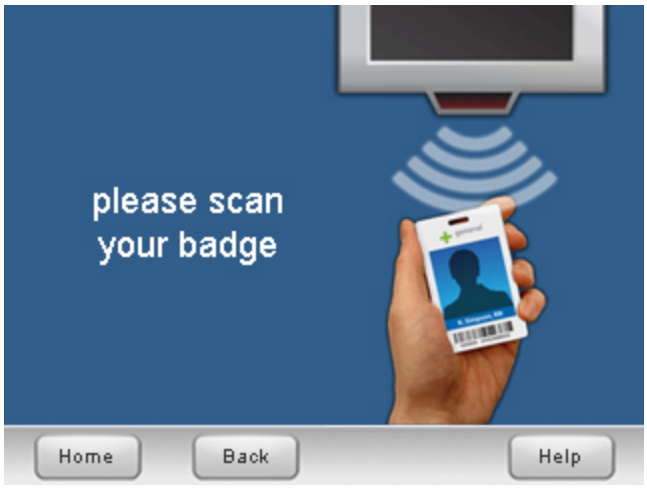


Figure 199: Scan Employee Badge on MDC Station Screen

d. [Optional] If roles are configured on MDC Station:

i. Select the **role category** for the role being assigned to you this shift, if categories are presented:

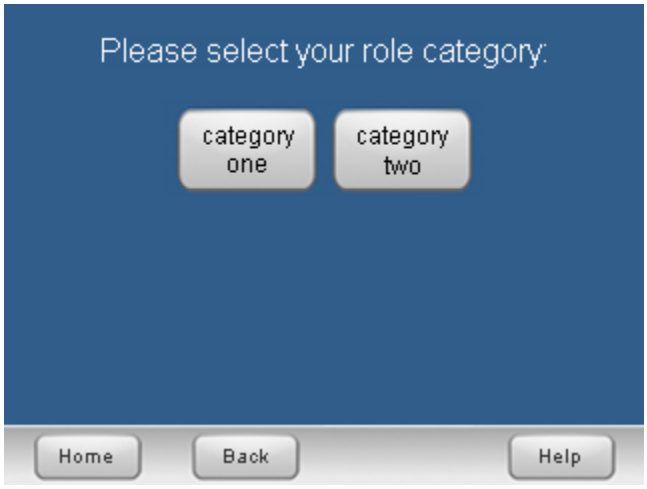


Figure 200: Select Role Category on MDC Station Screen

ii. Find and select the **role** being assigned to you this shift. You may need to use the **More Role** or **Back** buttons to see other available roles. If you do not have an assign role for this shift, location and select **no role** button if available:

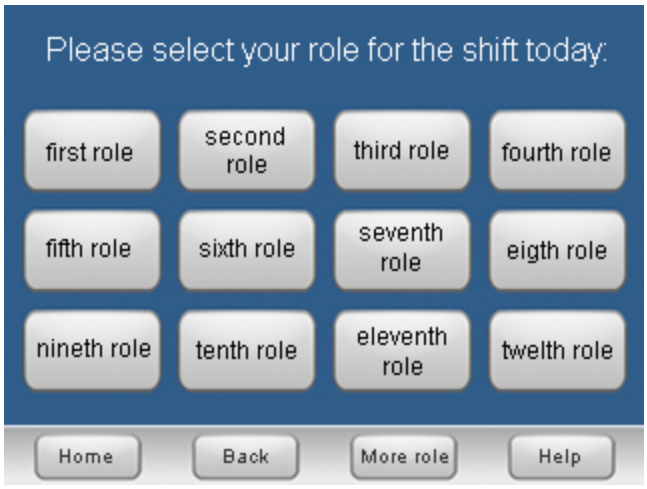


Figure 201: Select Role on MDC Station Screen

iii. Confirm the role selection.

e. Wait for a confirmation message of successful phone assignment on the MDC Station screen.

f. It is recommended the user confirm the checkout:

- With CS 1000 call server, the phone number on the handset changes to the user's phone number within 10 seconds typically (or within 3.5 minutes under heavy traffic load) after a successful phone checkout.
- With CS 2100 call server, the phone will have dial tone within 10 seconds typically (or within 3.5 minutes under heavy traffic load) after a successful phone checkout. The users must check for dial tone by pressing their off hook key. For situations when both role and personal phone numbers are assigned, the user should press the Line button (and select appropriate line 1 or 2) and verify that dial tone is available on both lines.

If the above does not occur, the user should check out the phone again.

At the MDC Admin GUI, you should see the association of the phone to the user in both the Users and Asset screens. See Section 10.4 *View Owner of Assets* and Section 11.3 *View Assets Assigned to User* for more details.

14.2 Return a phone at an MDC Station

At the MDC Station, use these steps to return the phone:

a. Press the **Return** button on the MDC Station screen. This can be any MDC Station, not necessarily the MDC Station where the phone was checked out.

b. Scan the phone barcode as instructed.

c. Wait for the confirmation message of successful phone return.

d. [Optional]To confirm the return:

- With CS 1000 call servers, confirm the phone number on the handset changes from the user's phone number back to the default number of the handset within 10 seconds typically (or within 3.5 minutes under heavy traffic load) after a successful phone return.
- With CS 2100 call servers, confirm there is no dial tone on the phone lines within 10 seconds typically (or within 3.5 minutes under heavy traffic load) after a successful phone return.

At the MDC Admin GUI, you should see the disassociation of the phone to the user in both the Users and Asset screens. See Section 10.4 *View Owner of Assets* and Section 11.3 *View Assets Assigned to User* for more details.

14.3 Presentation Conventions on MDC Station Screen

These are presentation conventions on the MDC Station Screen:

- Press the **Help** button on the lower right corner of the MDC Station screen to view the help number.
- Press the **Home** button on the lower left corner of MDC Station screen to return to the main Checkout and Return screen.
- Press the **Back** button to return to the previous screen.
- [Only applies if roles are enabled on MDC Stations and more then twelve roles exist] Press the **More Roles** button to see additional roles.

14.4 Check out a phone to a location-tracked user

This test is optional. It only applies if location tracking is being used with MDC.

Select both a location-tracking-enabled user and a location-tracking-enabled phone. At the MDC Station, use these steps to check out the phone to this user:

a. Press the **Checkout** button on the MDC Station screen.

b. Scan the phone barcode as instructed.

c. Scan the User barcode as instructed.

d. [Optional only if roles are enabled on MDC Station] Select and confirm role as instructed.

e. Wait for a confirmation message of successful phone assignment with location tracking.

f. It is recommended the user confirm the checkout:

- With CS 1000 call server, the phone number on the handset changes to the user's phone number within 10 seconds typically (or within 3.5 minutes under heavy traffic load) after a successful phone checkout.
- With CS 2100 call server, the phone will have dial tone within 10 seconds typically (or within 3.5 minutes under heavy traffic load) after a successful phone checkout. The users must check for dial tone by pressing their off hook key. For situations when both role and personal phone numbers are assigned, the user should press the Line button (and select appropriate line 1 or 2) and verify that dial tone is available on both lines.

If the above does not occur, the user should check out the phone again.

At the MDC Admin GUI, you should see the association of the phone to the user in both the Users and Asset screens with tracking enabled. Location tracking should be shown as being active. See Section 10.4 *View Owner of Assets* and Section 11.3 *View Assets Assigned to User* for more details.

Refer to Section 8 *Integrate MDC and Location Service* for more information on managing location services with MDC.

14.5 Return a phone assigned to a location tracked user

This test is optional. It only applies if location tracking is being used with MDC.

Select a location-tracking-enabled phone which has been checked out to a location-tracking-enabled user. At the MDC Station, use these steps to return the phone:

a. Press the **Return** button on the MDC Station screen. This can be any MDC Station, not necessarily the MDC station where the phone was checked out.

b. Scan the phone barcode as instructed.

c. Wait for a confirmation message of successful phone return and location tracking being disabled.

d. [Optional]To confirm the return:

    a. With CS 1000 call servers, confirm the phone number on the handset changes from the user's phone number back to the default number of the handset within 10 seconds typically (or within 3.5 minutes under heavy traffic load) after a successful phone return.

    b. With CS 2100 call servers, confirm there is no dial tone on the phone lines within 10 seconds typically (or within 3.5 minutes under heavy traffic load) after a successful phone return.

At the MDC Admin GUI, you should see the disassociation of the phone to the user in both the Users and Asset screens. Location tracking should be shown as not being active. See Section 10.4 *View Owner of Assets* and Section 11.3 *View Assets Assigned to User* for more details.

Refer to Section 8 *Integrate MDC and Location Service* for more information on managing location services with MDC

14.6 Re-Assign a Phone from a User to another User at any MDC Station

Select a phone which has been checked out to user A. At the MDC Station, using user B's barcode, use these steps to attempt to check out the phone:

a. Press the **Checkout** button on the MDC station screen.

b. Scan the phone barcode as instructed.

c. Scan the User B barcode as instructed.

d. Wait for a confirmation message of successful phone assignment.

e. Confirm the phone is checked out to user B within 10 seconds typically (or within 3.5 minutes under heavy traffic load) after a successful phone assignment:

- With CS 1000 call server, confirm the phone number on the handset changes to the user **B**'s phone number.
- With CS 2100 call server, confirm there is dial tone and any phone call made from the phone are seen as originating from user B's phone number.

At the MDC Admin GUI, you should see an automatic disassociation of the phone from first user A and an association of the phone to second user B. Any role or location tracking assigned to user A will also be disassociated. See Section 10.4 *View Owner of Assets* and Section 11.3 *View Assets Assigned to User* for more details.

14.7 Assign a Phone from a User and Assign another phone to same User at any MDC Station

Select phone A which has been checked out to a user. At the MDC Station, using phone B's barcode, use these steps to attempt to check out the phone B:

a. Press the **Checkout** button on the MDC Station screen.

b. Scan the phone B barcode as instructed.

c. Scan the User barcode as instructed.

d. [Optional if roles are enabled on MDC Station] Select and confirm role as instructed.

e. Wait for a confirmation message of successful phone assignment.

f. Confirm phone B is checked out to the user within 10 seconds typically (or within 3.5 minutes under heavy traffic load) after a successful phone assignment:

- With CS 1000 call server, confirm the phone number on phone B changes to the user's phone number [and role phone number if applicable].
- With CS 2100 call server, confirm there is dial tone and any phone calls made from phone B are seen as originating from user's phone number [or the user's role phone number if applicable]. [For situations when both role and personal phone numbers are assigned, the user should press the Line button (and select appropriate line 1 or 2) and verify that dial tone is available on both lines. Calls should be originated from both lines as well]

e. Confirm phone A is automatically returned to the default handset setting within 10 seconds typically (or within 3.5 minutes under heavy traffic load) of the successful checkout of phone B. To confirm the return:

- With CS 1000 call servers, confirm the phone number on phone A changes from the user's phone number back to the default number of the handset within 10 seconds typically (or within 3.5 minutes under heavy traffic load).
- With CS 2100 call servers, confirm there is no dial tone on the phone A's lines within 10 seconds typically (or within 3.5 minutes under heavy traffic load).

At the MDC Admin GUI, you should see an automatic disassociation of phone A from the user and an association of phone B to the user. Any role or location tracking assigned to the user with phone A will also be disassociated. See Section 10.4 *View Owner of Assets* and Section 11.3 *View Assets Assigned to User* for more details.

15 Additional Help

To access documentation, software and technical bulletins on MDC:

1. Open a new web browser window.
2. Go to the Nortel Website at http://www.nortel.com
3. Under the **SUPPORT & TRAINING** menu, select **TECHNICAL DOCUMENTATION**.
4. In the **DOCUMENTATION, SOFTWARE, AND BULLETINS** area, click **SOLUTIONS.**
5. Click **Healthcare Solutions.**
6. The technical support page for Healthcare Solutions will appear. There are sections for **DOCUMENTATION**, **SOFTWARE** and **BULLETINS**.

For technical support on MDC:

1. Open a new web browser window.
2. Go to the Nortel Global Support Contact page at http://www.nortel.com/cgi-bin/comments/comments.cgi?key=techsupport_cu.
3. The Nortel Technical Support screen will appear. On the right side of the screen will be a list titled **CALL US.**
4. Call the support number for your region.

16 References

1. Nortel Healthcare Solutions MDC Documentation Roadmap NN49010-100
2. Nortel Healthcare Solutions MDC Customer Preparation Guide NN49010-102
3. Nortel Healthcare Solutions MDC Deployment Guide NN49010-501
4. Nortel Healthcare Solutions MDC Station User Quick Reference Guide for CS 1000 NN49010-101
5. Nortel Healthcare Solutions MDC Station with Roles User Quick Reference Guide for CS 1000 NN49010-103
6. Nortel Healthcare Solutions MDC Station User Quick Reference Guide for CS 2100 NN49010-104
7. Nortel Healthcare Solutions MDC Station with Roles User Quick Reference Guide for CS 2100 NN49010-105
8. Nortel Healthcare Solutions MDC Application Troubleshooting Guide NN49010-700
9. Nortel Healthcare Solution Asset Tracking Management Documentation Suite
10. KRS User Guide for MDC is available from KRS. Within KRS, select **Product Control > Documentation, Forms & USER GUIDES.**

17 Acronyms and Definitions

ATM	Asset Tracking Management
CEM	CS 1000 Element Manager
CLI	Command Line Interface
CS 1000	Communication Server 1000
CS 2100	Communication Server 2100
ELAN	Embedded LAN
ELP	Ekahau Location Port
EPE	Ekahau Positioning Engine
GUI	Graphical User Interface
IP	Internet Protocol
HTTP	HyperText Transport Protocol
HTTPS	HyperText Transport Protocol Secure
IP	Internet Protocol
KRS	Keycode Retrieval System
LDAP	Lightweight Directory Access Protocol
MCA	Multiple Call Arrangement
MCR	Multiple Call Arrangement with Ringing
MDC	Mobile Device Checkout
NRS	Network Routing Service
PTY	Pseudo Terminal
RDM	Remote Device Manager
RTLS	Real Time Location System
SCA	Single Call Arrangement
SCR	Single Call Arrangement with Ringing
SIP	Session Initiation Protocol

TCP	Transmission Control Protocol
TLAN	Telephony LAN
TN	Terminal Number
WLAN	Wireless Local Area Network

18 Appendix: List of MDC Logs

The following table lists all the MDC logs with descriptions and resolution where available.

Additional information on logging can be found in the document NN49010-400 Nortel Healthcare Solutions MDC Application Troubleshooting Guide.

Table 1 – MDC logs

Event	Type	Description	Class	Severity	Resolution
QUEUE_SIZE	Processing	Current Queue Size	SERVICE	INFO	
SUCCESSFUL_ASSET_CHECKOUT	Processing	Asset has been checked out successfully	SERVICE	INFO	
SUCCESSFUL_ASSET_RETURN	Processing	Asset has been checked out successfully	SERVICE	INFO	
MULTIPLE_PHONE_CHECKOUT	Processing	More than one phone being checked out by the same user	SERVICE	WARNING	User must return phone to phone pool
PHONE_CHECKOUT_NO_RETURN	Processing	Phone checked out without being returned properly	SERVICE	WARNING	Remind the user to return phones after use
PHONE_CHECKOUT_FAILED	Processing	Phone checked out failed	SERVICE	WARNING	Phone must be checked out again
PHONE_RETURN_FAILED	Processing	Phone return failed	SERVICE	WARNING	Phone must be returned again via MDC Station
PHONE_SCANNED3_FAILED	Processing	Phone was scanned three times and failed to be recognized three times	SERVICE	WARNING	Phone needs be checked that it has a valid barcode
BADGE_SCANNED3_FAILED	Processing	Badge was scanned three times and failed to be recognized three times	SERVICE	WARNING	Badge needs be checked that it has a valid barcode
SUCCESSFUL_START_LOCATION_TRACK	Processing	User is being location tracked	SERVICE	INFO	
SUCCESSFUL_STOP_LOCATION_TRACK	Processing	User location tracking stopped	SERVICE	INFO	
FAILED_START_LOCATION_TRACK	Processing	Attempt to start user location tracking failed	SERVICE	WARNING	
FAILED_STOP_LOCATION_TRACK	Processing	Attempt to stop user location tracking failed	SERVICE	WARNING	
LOSS_OF_CONNECTION	Communications	Loss of connection	ADMIN	CRITICAL	

Event	Type	Description	Class	Severity	Resolution
FAILED_TO_CONNECT	Communications	Failed to establish connection	ADMIN	CRITICAL	Validate connection credentials and network connectivity
CONNECTION_ESTABLISHED	Communications	Connection established	ADMIN	CRITICAL	
LOGIN_SUCCESSFUL	Communications	Login to call server successful	ADMIN	CRITICAL	
LOGIN_FAILED	Communications	Login to call server failed	ADMIN	CRITICAL	Check Call Server Credentials and IP address
COMMUNICATION_ERROR	Communications	Connection error	FAULT	CRITICAL	
DEFAULT_CONFIGURATION_USED	Processing	Configuration retrieval error	ADMIN	WARNING	Provision Database
UNSUCCESSFUL_TAG_READ	Processing	Unsuccessful read of ID tag	ADMIN	WARNING	
UNAUTHORIZED_DEVICE_CONNECTION_ATTEMPT	Security	Unauthorized device Connection Attempted	ADMIN	WARNING	
USER_LOGIN	Processing	User login	ADMIN	INFO	
USER_LOGOUT	Processing	User logout	ADMIN	INFO	
INVALID_LOGIN_ATTEMPT	Security	Invalid login attempt	ADMIN	NOTICE	
LICENSE_LIMIT_REACHED	Security	License limits have been reached	ADMIN	NOTICE	
PROCESS_STOPPED	Processing	Process stopped	ADMIN	CRITICAL	
PROCESS_COMPLETED	Processing	Process has completed	ADMIN	INFO	
PROCESS_STARTED	Processing	Process stated	ADMIN	INFO	
PROCESS_FAILURE	Processing	Process has failed	ADMIN	CRITICAL	
FILE_SYSTEM_ERROR	Processing	File system error	ADMIN	NOTICE	
DATA_INTEGRITY_ERROR	Processing	Data integrity error	ADMIN	INFO	
FAILED_EXECUTE_COMMAND	Processing	Failed to execute request	FAULT	WARNING	
TRACKABLE_USER_LICENSES_EXPIRED	Processing	Licenses expired for trackable users	SERVICE	CRITICAL	
PHONE_LICENSES_EXPIRED	Processing	Licenses expired for phones	SERVICE	CRITICAL	
STATION_LICENSES_EXPIRED	Processing	Licenses expired for stations	SERVICE	CRITICAL	

Event	Type	Description	Class	Severity	Resolution
ROLE_LICENSES_EXPIRED	Processing	Licenses expired for roles. Roles will be disabled	SERVICE	CRITICAL	ROLE_LICENSES_EXPIRED
ROLE_LICENSES_INSUFFICIENT_OR_NON_EXISTANT	Processing	No role licenses or number of role licenses is less than the number of station licenses. Roles will be disabled	SERVICE	CRITICAL	
TRACKABLE_USER_LICENSE_LIMIT_REACHED	Processing	Reached license limit for trackable users	SERVICE	WARNING	
PHONE_LICENSE_LIMIT_REACHED	Processing	Reached license limit for phones	SERVICE	WARNING	
STATION_LICENSE_LIMIT_REACHED	Processing	Reached license limit for stations	SERVICE	WARNING	
STATION_REBOOT_SENT_SUCCESSFULLY	Processing	Reboot request sent to station successfully	SERVICE	WARNING	
FAILED_STATION_REBOOT	Processing	Failed to send reboot request to station	SERVICE	WARNING	
FAILED_AUTHENTICATION_ATTEMPT	Security	Failed to authenticate with provisioned credentials	ADMIN	CRITICAL	Please check the credentials and ensure that the userid-password combination is valid
FAILED_TO_SEND_NOTIFICATION	Security	Failed to send notification to application	SERVICE	CRITICAL	
ASSET_INACTIVE_OVERDUE_TIMEOUT	Processing	Asset has exceeded the specified inactive/overdue timeout period	ADMIN	WARNING	
DATABASE_RECORD_INSERTED	Processing	A record has been inserted into the database	ADMIN	INFO	
DATABASE_RECORD_UPDATED	Processing	A record has been updated in the database	ADMIN	INFO	
DATABASE_RECORD_DELETED	Processing	A record has been deleted from the database	ADMIN	INFO	

19 Appendix: Upgrade MDC Software

This procedure will upgrade the software of the MDC application from:

- Release 1.0.2 to Release 2.0.1
- Release 2.0 to Release 2.0.1

After a successful MDC upgrade, the MDC application will automatically be restarted.

WARNING: This procedure is service affecting. The MDC Server processes and cklt processes will be stopped during the upgrade process. As a result, there will be a period of time when MDC service will be unavailable during the upgrade when software is upgraded and data is converted if needed. It is recommended that this procedure be performed during a period of low activity, such as a maintenance window, or in-between shift changes, to minimize the impact.

WARNING: As part of upgrading from MDC Release 1.0.2 to MDC Release 2.0.1, it is recommended SE Linux enforcement is enabled during the upgrade process using the instructions provided in the upgrade procedure below. Enabling SE Linux will require a reboot of the MDC server.

WARNING: If custom station graphic have been used in MDC Release 1.0.2, this customization will not be automatically preserved over the upgrade. Instructions are provided in the upgrade procedure below to manually re-install the custom station graphics.

Manual actions are described in the upgraded procedure to backup these files prior to the upgrade and then re-install these custom station graphics in MDC Release 2.0.1. See the document NN49010-501 Nortel Healthcare Solutions MDC Deployment Guide for further details on configuring the MDC Stations

WARNING: After the installation of the upgraded software, the MDC application will be returned to service but it will NOT be fully operational. The upgrade must be completed as described below including a manual restart of all of the MDC Stations.

19.1 Information Needed to Upgrade MDC

It is recommended that the person performing the upgrade should be familiar with MDC Admin GUI.

The required information needed prior to starting the MDC upgrade is listed in the table below:

Table 2 – Required Information for MDC Upgrade

Description	Information
MDC Server must have Internet access	
Name of the most recent MDC backup performed prior to upgrade	
Back up of station graphic (only if customized)	
IP address of the MDC Server	
Root password for the MDC Server to run the upgrade (Due to OS security hardening, you may need to login with a non-root username and then switch	

user privileges to root (e.g. **su – root**))	
Non-root username and password for MDC Server	
Customer userid and password credentials for www.nortel.com to retrieve MDC installation media	
Directory on the MDC Server in which to place MDC installation media	
Username and password for MDC Administration GUI	
IP address of backup server which acts as repository for MDC backup files	
Port used for SFTP to backup server (22 is default port used for SFTP)	
Userid and password to log on to the backup server using SFTP utility	
Directory on the backup server where MDC backup files are stored	

19.2 Performing an Upgrade of MDC

NOTE: the latest MDC load will be a different version than what is shown in the examples of this section.

NOTE: Depending on the upgrade path being performed, the output from the upgrade may differ from what is shown in the examples.

These are the steps to upgrade MDC:

1. These pre-conditions were verified or configured as part of the MDC installation. These pre-conditions are assumed to still be in effect:
    a. RHEL version
    b. yum version
    c. Apache is installed and configured to automatically start
    d. MySQL is installed and configured to automatically start
    e. BIOS AC power recovery
    f. port usage
    g. Server run level
    h. mdc and cklt RPM were installed

    For further information on these pre-conditions, refer to the installation procedure in document NN49010-501 Nortel Healthcare Solutions MDC Deployment Guide.
2. Perform the pre-upgrade verification checks:

a. Confirm the MDC Server has internet access. Ping a well known hostname and confirm the ping is successful.

b. Confirm the MDC Server YUM repository access. Use the following commands to display the YUM repository configured. Verify that Red Hat Enterprise Linux repository for v5 is configured.

Example:

 # yum repolist

Loaded plugins: rhnplugin, security

rhel-i386-server-5 | 1.3 kB 00:00

repo id repo name status

rhel-i386-server-5 Red Hat Enterprise Linux (v. 5 for 32-bi enabled : 5,223

repolist: 5,223

c. Perform an OS update. It is recommended that the OS be updated with the latest versions available. Use the following command to update all currently installed packages.

WARNING: This command may take a long time to complete. The duration of the command varies depending on the version of OS, the contents of the YUM repository, and network connectivity.

Example:

#yum update

If queried about importing GPG, confirm the installation of software packages with “y”.

3. Manually back up MDC (using MDC Administration GUI). See Section 5.12.3 *Manual Backup* for the detailed procedure.
4. Prior to upgrading the MDC software, log out of all MDC Admin GUI sessions and close their associated browser windows. For browsers which support tabs, the browser window must still be closed as exiting only the tab is insufficient to update the MDC Admin GUI over the upgrade.
5. Log on to the MDC Server with root privileges. Due to OS security hardening, you may need to login with a non-root username and then switch user privileges to root (e.g. **su – root**).
6. When upgrading from MDC Release 1.0.2 system, if a custom logo graphic is being used in MDC Release 1.0.2 *(i.e. phone_pool_init.txt has TEMPLATE = "custom"*), you need to manually backup /opt/nortel/ebs/mdc/templates/custom/images/logo.gif at this time as this file is not part of the MDC Release 1.0.2 backup.

   Following the upgrade from Release 1.0.2 to Release 2.0.1, there will be instructions on how to re-apply this customized station graphic file logo.gif on the MDC Release 2.0.1 system.
7. SE Linux enforcement is recommended for MDC Release 2.0.1. To enable SE Linux enforcement in preparation for upgrading from Release 1.0.2 to Release 2.0.1:

   a. Stop MDC processes and their automatic restart with the following commands:

      chkconfig mdc off

      chkconfig cklt off

      service mdc stop

      service cklt stop

   b. Edit the **/etc/selinux/config** file to set the SELinux status to enforcing:

cat /etc/selinux/config

This file controls the state of SELinux on the system.

SELINUX= can take one of these three values:

enforcing - SELinux security policy is enforced.

permissive - SELinux prints warnings instead of enforcing.

disabled - SELinux is fully disabled.

SELINUX=**enforcing**

SELINUXTYPE= type of policy in use. Possible values are:

targeted - Only targeted network daemons are protected.

strict - Full SELinux protection.

SELINUXTYPE=**targeted**

SETLOCALDEFS= Check local definition changes

SETLOCALDEFS=**0**

c. Re-label the filesystem with the command:

touch /.autorelabel

d. Type **reboot** to reboot the server.

e. On a terminal window, type **sestatus** to confirm the SELinux setting.

 # sestatus

SELinux status: **enabled**

SELinuxfs mount: /selinux

Current mode: **enforcing**

Mode from config file: **enforcing**

Policy version: 21

Policy from config file: **targeted**

8. Retrieve the MDC installation/upgrade media. The MDC installation media is obtained from Nortel's Technical Support Portal:

a. Open a new web browser window.

b. Go to the Nortel website at http://www.nortel.com.

c. Log in with the customer's username and password.

d. Under the **SUPPORT & TRAINING** menu, select **SOFTWARE DOWNLOADS**.

e. In the **DOCUMENTATION, SOFTWARE, AND BULLETINS** area, click **SOLUTIONS.**

f. Click **Healthcare Solutions.**

g. The technical support page for Healthcare Solutions will appear. There are sections for **DOCUMENTATION**, **SOFTWARE** and **BULLETINS**.

h. Click on **SOFTWARE** to access MDC media.

i. Select the software for MDC Release 2.0.1.

j. Download the MDC installation tar file onto the user-chosen directory on the MDC Server.

9. Extract the MDC install media and list contents.

- Type **tar xvfz <filename>**

  Example:

```
# tar xvfz mdc-2.0.0-1376-PKG.tar.gz
mdc-2.0.0/cklt-2.0.0-1376.el5.i386.rpm
mdc-2.0.0/ionCube-loader-3.1-1.el5.i386.rpm
mdc-2.0.0/libssh2-1.0-1.i386.rpm
mdc-2.0.0/log4php-ebs-2.0.0-1.el5.noarch.rpm
mdc-2.0.0/mdc-2.0.0-1376.el5.noarch.rpm
mdc-2.0.0/php-ssh2-0.11.0-1.el5.i386.rpm
mdc-2.0.0/createdb.sql
mdc-2.0.0/MigrateData1.01.sql
mdc-2.0.0/PopulateInitialData.sql
mdc-2.0.0/PostMigrate.sql
mdc-2.0.0/PreMigrate.sql
mdc-2.0.0/install_mdc
```

- Type **cd <directory with install media>**

  Example:

```
# cd mdc-2.0.0
```

10. Run **./install_mdc** to start the upgrade with the installation of the new release of MDC software.

    a. You will be asked to confirm that you have performed a backup of MDC server. Type "**y**" only if you have performed the backup.

    b. The script will determine the software packages required for MDC upgrade. You will be asked to confirm the installation of the software packages with "**y**".

    Note: Depending on the upgrade path, you may be asked to confirm a second installation of software packages with a "**y**". The first confirmation is needed to install new required base packages and the second confirmation is for the upgrade of MDC software packages.

    Note: The list of software packages to be installed will always include those packages contained in the MDC RPM. In addition, any required dependencies of the software in MDC RPM obtained from the YUM repository (if used) will also be included. The total of these two sources will be contained in the yum transaction summary and the total download size presented to the user with the request for confirmation.

    c. Wait for the confirmation that installing new software has been completed successfully.

    During this step, the MDC application will be taken out of service. At the end of this step, the MDC application will be running; however, it will have a new (empty) database. The MDC system will not be operational until the database is restored in the next step.

    Example:

```
# ./install_mdc
Welcome to Nortel Mobile Device Checkout (MDC) Installation.

Performing upgrade of MDC.

Confirmation Required:
```

```
It is recommended to perform a backup prior to running the MDC
Upgrade from release 1.0.1 or 1.0.2.
Has this backup been performed? [ y/N ]: y
Stopping mdc before modifying database.
                                                                [  OK  ]
Preparing database nortel_ebs_mdc for MDC upgrade
Recreating database nortel_ebs_mdc for MDC
Migrating the data in database nortel_ebs_mdc for MDC upgrade
Populating database nortel_ebs_mdc for MDC
Performing post-migration activities on database nortel_ebs_mdc for
MDC upgrade

Determining if any package needs to be installed before upgrading
the remaining packages.

ionCube-loader-3.1-1.el5
libssh2-1.0-1
php-ssh2-0.11.0-1.el5
package log4php-ebs is not installed
Package log4php-ebs will be installed now before upgrading other
packages.
Loaded plugins: rhnplugin, security
Setting up Local Package Process
Examining log4php-ebs-2.0.0-1.el5.noarch.rpm: log4php-ebs-2.0.0-
1.el5.noarch
Marking log4php-ebs-2.0.0-1.el5.noarch.rpm to be installed
Resolving Dependencies
There are unfinished transactions remaining. You might consider
running yum-complete-transaction first to finish them.
The program yum-complete-transaction is found in the yum-utils
package.
--> Running transaction check
---> Package log4php-ebs.noarch 0:2.0.0-1.el5 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package       Arch     Version         Repository
Size
================================================================================
Installing:
 log4php-ebs   noarch   2.0.0-1.el5     /log4php-ebs-2.0.0-
1.el5.noarch   270 k

Transaction Summary
================================================================================
Install      1 Package(s)
Update       0 Package(s)
Remove       0 Package(s)

Total size: 270 k
Is this ok [y/N]: y
Downloading Packages:
Running rpm_check_debug
```

```
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : log4php-ebs
1/1

Installed:
  log4php-ebs.noarch 0:2.0.0-1.el5

Complete!
cklt-1.0.2-1001.el5
mdc-1.0.2-1001.el5
Loaded plugins: rhnplugin, security
Setting up Local Package Process
Examining cklt-2.0.0-1313.el5.i386.rpm: cklt-2.0.0-1313.el5.i386
Marking cklt-2.0.0-1313.el5.i386.rpm as an update to cklt-1.0.2-
1001.el5.i386
Examining ionCube-loader-3.1-1.el5.i386.rpm: ionCube-loader-3.1-
1.el5.i386
ionCube-loader-3.1-1.el5.i386.rpm: does not update installed
package.
Examining libssh2-1.0-1.i386.rpm: libssh2-1.0-1.i386
libssh2-1.0-1.i386.rpm: does not update installed package.
Examining log4php-ebs-2.0.0-1.el5.noarch.rpm: log4php-ebs-2.0.0-
1.el5.noarch
log4php-ebs-2.0.0-1.el5.noarch.rpm: does not update installed
package.
Examining mdc-2.0.0-1313.el5.noarch.rpm: mdc-2.0.0-1313.el5.noarch
Marking mdc-2.0.0-1313.el5.noarch.rpm as an update to mdc-1.0.2-
1001.el5.noarch
Examining php-ssh2-0.11.0-1.el5.i386.rpm: php-ssh2-0.11.0-1.el5.i386
php-ssh2-0.11.0-1.el5.i386.rpm: does not update installed package.
Resolving Dependencies
There are unfinished transactions remaining. You might consider
running yum-complete-transaction first to finish them.
The program yum-complete-transaction is found in the yum-utils
package.
--> Running transaction check
---> Package cklt.i386 0:2.0.0-1313.el5 set to be updated
---> Package mdc.noarch 0:2.0.0-1313.el5 set to be updated
--> Processing Dependency: expect >= 5.43.0 for package: mdc
--> Processing Dependency: expectk >= 5.43.0 for package: mdc
--> Running transaction check
---> Package expect.i386 0:5.43.0-5.1 set to be updated
---> Package expectk.i386 0:5.43.0-5.1 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
============
 Package     Arch       Version            Repository
Size
================================================================================
============
Updating:
```

```
 cklt        i386       2.0.0-1313.el5     /cklt-2.0.0-1313.el5.i386
6.7 M
 mdc         noarch     2.0.0-1313.el5     /mdc-2.0.0-
1313.el5.noarch     2.4 M
Installing for dependencies:
 expect      i386       5.43.0-5.1         rhel-i386-server-5
158 k
 expectk     i386       5.43.0-5.1         rhel-i386-server-5
48 k

Transaction Summary
================================================================================
Install      2 Package(s)
Update       2 Package(s)
Remove       0 Package(s)

Total size: 9.3 M
Total download size: 206 k
Is this ok [y/N]: y
Downloading Packages:
(1/2): expectk-5.43.0-5.1.i386.rpm                       |  48 kB
00:00
(2/2): expect-5.43.0-5.1.i386.rpm                        | 158 kB
00:00
--------------------------------------------------------------------------------
Total                                            182 kB/s | 206 kB
00:01
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Updating       : cklt
1/6
Starting CKLT cfsserver:[  OK  ]
Starting CKLT ckltproxy:[  OK  ]
  Installing     : expect
2/6
  Installing     : expectk
3/6
  Updating       : mdc
4/6
Stopping httpd: [  OK  ]
Starting httpd: httpd: Could not reliably determine the server's
fully qualified domain name, using 127.0.0.1 for ServerName
[  OK  ]
# Save MDC messages also to mdc.log
local0.info
/var/log/mdc.log
# Save MDC debug messages to mdc_debug.log
local0.=debug
/var/log/mdc_debug.log
Shutting down kernel logger: [  OK  ]
Shutting down system logger: [  OK  ]
Starting system logger: [  OK  ]
Starting kernel logger: [  OK  ]
```

```
Reloading cron daemon configuration: [  OK  ]
/ /
/

SELinux is currently enabled. Installing the SELinux policy
necessary for MDC. This may take 30-45 seconds.
fs.mqueue.msg_max = 128
Starting MDC EventProcessor.php:[  OK  ]
Starting MDC BackupManager.php:[  OK  ]
Starting MDC ProcessingQueue.php:[  OK  ]
Starting MDC StationMonitor.php:[  OK  ]
Starting MDC WatchDog.php:[  OK  ]
Starting MDC KeepAliveCS1K.php:[  OK  ]
Starting MDC EventNotificationProcessor.php:[  OK  ]
warning: /opt/nortel/ebs/mdc/config/phone_pool_init.txt created as
/opt/nortel/ebs/mdc/config/phone_pool_init.txt.rpmnew
  Cleanup        : cklt
5/6
  Cleanup        : mdc
6/6
warning: /opt/nortel/ebs/mdc/templates/custom/images/logo.gif saved
as /opt/nortel/ebs/mdc/templates/custom/images/logo.gif.rpmsave
Stopping httpd: [  OK  ]
Starting httpd: httpd: Could not reliably determine the server's
fully qualified domain name, using 127.0.0.1 for ServerName
[  OK  ]

Dependency Installed:
  expect.i386 0:5.43.0-5.1              expectk.i386 0:5.43.0-5.1

Updated:
  cklt.i386 0:2.0.0-1313.el5            mdc.noarch 0:2.0.0-1313.el5

Complete!
MDC Upgrade has completed successfully.
MDC may now be used.
```

Proceed to the next section to verify the upgrade of MDC software.

19.3 Verifying Upgrade of MDC Software

1. Post-upgrade verification procedure:
   - Verify all the MDC processes are running:
     - Type **service mdc status**
   - Verify all the licensing processes are running:
     - Type **service cklt status**

Proceed to the next section to complete the upgrade of MDC software:

19.4 Completing the Upgrade of MDC

To complete the upgrade of MDC:

1. On the MDC admin GUI confirm the assets and users' data, etc., is present.
2. If there was a custom logo graphic saved from MDC Release 1.0.2 (see Step 6 above):
    a. Replace /**opt/nortel/ebs/mdc/templates/MK1250/custom/images/logo.gif** with the saved image.
    b. Replace **/opt/nortel/ebs/mdc/templates/KDT900/custom/images/logo.gif** with the saved image.
    c. Go to MDC Admin GUI > Configure > Stations > Locations. Change the station graphic templates to **custom for all locations**. See Section 13.7 *Modify Station Location* if further details are needed.
3. If location tracking is licensed on MDC and using SynTrack, update the location service port to **443**. See Section 8.2 *Integrating MDC Server and Location Service* for details if needed.
4. Confirm all the station locations are station type **MK1250**. See Section 13.7 *Modify Station Location* for details if needed.
5. To complete the upgrade, reboot the MDC Stations to update and align their content with the new MDC software load. See 13.11 *Reboot All MDC Stations* for detailed steps if needed.

    These actions complete the upgrade. The MDC application will be in service and operational upon the successful completion of this step.
6. If necessary, physically remove the MDC upgrade media from the server.
7. Clean up the extracted MDC installation media on the server.

You have successfully completed upgrading the MDC application.

20 Appendix: Uninstall MDC Software

WARNING: This action is service impacting.

The uninstall_mdc script will stop the MDC service and remove all MDC data from the database and configuration files from the server. This includes the /opt/nortel/ebs/mdc directory and its contents. However, the MDC logs and event mail digests will remain.

During uninstall of MDC, the user will be given the option to uninstall dependent software packages and delete accounts used by MDC. However, these accounts and software may also be used by other applications. The correct response will depend on whether other EBS applications and/or other software are deployed on the same server as MDC.

WARNING: Do a backup prior to uninstalling MDC if you intend to re-establish MDC with its current data.

20.1 Information Needed to Uninstall MDC Software

The following information is needed prior to attempting to uninstall MDC:

- Whether a recent MDC backup has been performed.
- Whether the cklt RPM package should be uninstalled. This package may be used for licensing by other EBS applications.
    - If cklt package is removed, the user will be prompted on whether all files related to licensing in directory /opt/nortel/ebs/cklt should be removed as well.
- Whether ionCube-loader, log4php-ebs, libssh2 and php-ssh2 should be uninstalled. These packages may be used by other applications.
- Whether to remove nortelebs UNIX account. This account may be used by other EBS applications.
- Whether to remove nortelebs mySQL account. This account may be used by other EBS applications.
- Whether to remove the MDC SELinux policy. This policy may be used by other EBS applications.
- Information required to perform an MDC backup is:
    - Username and password for MDC Administration GUI
    - If the backup server is not configured you will also need to know:
        - IP address of the backup server which will act as a repository for MDC backup files
        - Port used for SFTP
        - Userid and password to log on to backup server using ftp utility
        - Directory on backup server where backup files are stored

20.2 Performing an Uninstall of MDC Software

The steps for uninstall are:

1. Type **cd /opt/nortel/ebs/mdc**
2. Type **./uninstall_mdc** to run the uninstall of MDC.
    a. You will be reminded to perform a backup of MDC and prompted whether you want to continue. Type “**y**” if you have already performed the backup using the MDC Administration GUI. Otherwise, type “**n**” to exit the uninstall script so you can perform the MDC backup.
    b. If the server is only running the MDC application, type '**y**' when prompted for the removal of various packages, accounts, policies and directories.

        Example:

```
[root@sc-mdc-2 mdc]# ./uninstall_mdc
MDC Uninstall
This will uninstall the MDC software, including:
  - removing the nortel_ebs_mdc database,
  - uninstalling the mdc RPM package,
  - removing mdc configuration files.
Optionally, you may also choose to:
  - remove the cklt RPM package,
  - remove the ionCube-loader, log4php-ebs, libssh2 and php-ssh2 RPM
packages,
  - remove the nortelebs Linux account used for operating Nortel EBS
applications,
  - remove the mySQL account used for interacting with the
nortel_ebs_mdc database.
  - remove the SELinux policy module that was added for the MDC
software.


It is recommended to perform a MDC backup prior to the uninstall if
MDC may be used at a later time.

Would you like to continue? [ y/N ]: y


The cklt RPM package is installed with MDC but may be used for other
applications.
Would you like to remove cklt if not used by other applications? [
y/N ]: y

The ionCube-loader, log4php-ebs, libssh2 and php-ssh2 RPM packages
are installed with MDC but may be used for other applications.
Would you like to remove ionCube-loader, log4php-ebs, libssh2 and
php-ssh2 if not used by other applications? [ y/N ]: y

The nortelebs Linux account may be used for operating other Nortel
EBS applications.
Would you like to remove the nortelebs Linux account? [ y/N ]: y

The mySQL account nortelebs used for accessing nortel_ebs_mdc may be
used with other databases.
Would you like to remove the nortelebs mySQL account? [ y/N ]: y

The SELinux policy used with the MDC software interacts with the
Apache httpd server.
Would you like to remove the SELinux policy used with the MDC
software? [ y/N ]: y

Stopping MDC processes.
                                                           [  OK  ]
Deleting nortel_ebs_mdc database.
Dropping mySQL account nortelebs.
Uninstalling mdc RPM.
warning: /opt/nortel/ebs/mdc/config/phone_pool_init.txt saved as
/opt/nortel/ebs/mdc/config/phone_pool_init.txt.rpmsave
Stopping httpd: [  OK  ]
Starting httpd: [  OK  ]
Uninstalling cklt RPM.
no package requires cklt
```

```
Files remain in /opt/nortel/ebs/cklt after the removal of CKLT.
Do you want to completely remove this directory? y

Uninstalling ionCube-loader, log4php-ebs, libssh2 and php-ssh2 RPMs.
no package requires ionCube-loader
Stopping httpd: [  OK  ]
Starting httpd: [  OK  ]
no package requires log4php-ebs
no package requires php-ssh2
Reloading httpd: [  OK  ]
no package requires libssh2
/opt/nortel/ebs/mdc
Deleting nortelebs Linux account.

Removing the SELinux policy used with the MDC software. This may
take 30-45 seconds to complete.
```

c. There will be a confirmation that the uninstall completed successfully:

Example:

```
MDC Uninstall is now complete.
```

20.3 Verifying Uninstall of MDC Software

1. Exit the current directory by typing **cd ..**
2. Confirm that there are no remaining files by typing **cd /opt/nortel/ebs/mdc**; This directory should no longer exist once there are no users present in the directory.

You have successfully completed un-installing the MDC application.

21 Appendix: MDC RPM Dependencies

This appendix lists the software package dependencies for MDC RPM against which the MDC application has been tested. The administration should exercise caution when updating RHEL, as changes to the software release of any of the software packages listed below has the potential to impact MDC functionality.

Nortel intends to perform compatibility testing of the MDC application against updates of RHEL 5 at regular intervals. Any exceptions will be issued in Technical Bulletins.

This is a list of the dependencies for MDC Release 2.0 (mdc-2.0.0-1376.el5):

- cklt >= 0.8.0
- expect >= 5.43.0
- expectk >= 5.43.0
- httpd >= 2.0.52
- php >= 5.1.0
- php-mysql >= 5.0.0
- php-soap >= 5.1.6
- php-ssh2 >= 0.11.0
- php-xml >= 5.1.0
- php-snmp >= 5.1.6
- ionCube-loader >= 3.1
- mod_ssl >= 2.2.3
- log4php-ebs >= 2.0.0

On the MDC server, the command **rpm –q <software package name>** will display the release version of the specified software package rpm.

End of Document