



>BUSINESS MADE **SIMPLE**

NORTEL

Nortel Healthcare Solution
Mobile Device Checkout Release 2.0.1

Mobile Device Checkout Release 2.0.1

Customer Preparation Guide

Document Date: April 12, 2010
Document Number: NN49010-102
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.

The Information is subject to change without notice.

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

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.

Table of Content

TABLE OF CONTENT	2
LIST OF FIGURES	4
LIST OF TABLES.....	6
1 WHAT'S NEW IN THIS RELEASE	8
2 INTRODUCTION	9
2.1 PURPOSE AND SCOPE.....	9
2.2 TARGET AUDIENCE	9
2.3 ASSUMPTIONS	9
2.4 EXCLUSIONS	10
3 SUMMARY OF REQUIRED INFORMATION FOR MDC SOLUTION DEPLOYMENT	11
3.1 HARDWARE AND SOFTWARE REQUIREMENTS FOR MDC	11
3.2 INFORMATION REQUIRED FOR INSTALLATION	11
3.2.1 <i>Required Information for RHEL Installation and Configuration.....</i>	<i>11</i>
3.2.2 <i>Required Information to verify RHEL O/S Installation and Configuration.....</i>	<i>12</i>
3.2.3 <i>Required Information for MDC Installation.....</i>	<i>13</i>
3.2.4 <i>Required Information for Zebra Application Installation.....</i>	<i>14</i>
3.2.5 <i>Required Information for Motorola RDM Installation</i>	<i>14</i>
3.2.6 <i>Required Information for Microsoft ActiveSync Installation</i>	<i>14</i>
3.3 INFORMATION REQUIRED FOR CONFIGURATION	15
3.3.1 <i>Required Information for Call Server Configuration for MDC</i>	<i>15</i>
3.3.1.1 Required Information for CS 1000 Configuration for MDC	15
3.3.1.2 Required Information for CS 2100 Configuration for MDC	19
3.3.1.3 Preparing for Bulk Loading Users and Phones into MDC	23
3.3.2 <i>Required Information for KRS.....</i>	<i>24</i>
3.3.3 <i>Required Information for Basic Configuration of MDC Server.....</i>	<i>25</i>
3.3.4 <i>Required Information for integrating MDC Server and Location Server.....</i>	<i>27</i>
3.3.5 <i>Required Information for Integrating MDC Server and Call Server</i>	<i>27</i>
3.3.6 <i>Required Information for Creating Roles on MDC Server</i>	<i>30</i>
3.3.7 <i>Required Information for MDC Station Configuration</i>	<i>31</i>
3.3.7.1 Required Information for MDC Station Configuration.....	31
3.3.7.2 Required Information for MK1200 & MK1250 MDC Station initialization.....	32
3.3.7.3 Required Information for KDT900 MDC Station initialization	34
3.3.7.4 Required Information for Remote MK1200 & MK1250 MDC Station Configuration and Reboot.....	35
4 COMMUNICATION SERVER 1000 CONFIGURATION FOR MDC	37
4.1 ROADMAP OVERVIEW OF CS 1000 CONFIGURATION FOR MDC	37
4.1.1 <i>Summary of CS 1000 Configuration for MDC Server.....</i>	<i>38</i>
4.1.2 <i>Summary of CS 1000 Configuration for MDC Users.....</i>	<i>40</i>
4.1.3 <i>Summary of CS 1000 Configuration for MDC Phone/Assets</i>	<i>41</i>
4.2 REQUIRED INFORMATION FOR CS 1000 CONFIGURATION FOR MDC	44
4.3 CS 1000 BASE CONFIGURATION	49
4.3.1 <i>Enable Insecure Shells for Rlogin.....</i>	<i>49</i>
4.3.2 <i>Create LAPW Password Account on CS 1000 Rel 5.x for MDC</i>	<i>49</i>
4.3.3 <i>Create Limited Access Password (LAPW) Role on CS 1000 Rel 6 for MDC.....</i>	<i>57</i>
4.3.4 <i>Backup of CS 1000 Element Manager</i>	<i>63</i>
4.3.5 <i>Logout of CS 1000 Element Manager</i>	<i>65</i>
4.4 TESTING CONNECTIVITY BETWEEN CS 1000 AND MDC	66
4.4.1 <i>Connectivity</i>	<i>66</i>

4.4.2	<i>Rlogin from MDC Server to CS 1000</i>	66
4.5	OPTIONS FOR CLI CONNECTION TO CS 1000 FOR USERS AND PHONE CONFIGURATION	68
4.5.1	<i>Terminal Emulation/Putty Session from MDC Server via ELAN</i>	68
4.5.2	<i>Virtual Terminal from CEM GUI</i>	69
4.6	CREATING PSEUDO TERMINALS (PTY) FOR MDC	73
4.7	ENABLE MULTIPLE USER LOGIN	74
4.8	USER AND ROLE TERMINAL NUMBER, DIRECTORY NUMBER AND CLS CONFIGURATION	75
4.8.1	<i>Permit Multiple Loop Dial Number</i>	77
4.8.2	<i>Creating New Users</i>	78
4.8.2.1	Creating New Users in Dual Terminal Number (TN) Deployment.....	78
4.8.2.2	Creating New Users in Shared Terminal Number (TN) Deployment.....	79
4.8.3	<i>Print using Terminal Number</i>	81
4.8.3.1	Print Dual TN user	82
4.8.3.2	Print Shared TN user	84
4.8.4	<i>Print Using Directory Number</i>	86
4.8.5	<i>Add New Name using LD 11</i>	87
4.8.6	<i>Changing Existing Name using LD 11</i>	87
4.8.7	<i>Add New Name using LD 95</i>	88
4.8.8	<i>Changing Existing Name using LD 95</i>	88
4.8.9	<i>Delete Existing Name using LD 95</i>	88
4.8.10	<i>Changing Calling Name Display Denied (CNDD) using LD 11</i>	89
4.8.11	<i>Change SCR to MCR by deleting KEY 0 using LD 11</i>	89
4.8.12	<i>Printing MAC using LD 20</i>	89
4.8.13	<i>Backup</i>	90
4.8.14	<i>Useful Commands</i>	90
4.8.14.1	Who	90
4.8.14.2	Exit from Overlay or Command.....	90
4.8.14.3	Display Information on Error Code.....	90
4.9	CS 1000 WLAN PHONE CONFIGURATION	91
4.9.1	<i>Enable MCR/SCR on Mobile phones</i>	92
4.9.2	<i>Permit Multiple Loop Dial Number</i>	93
4.9.3	<i>Enable Location tracking</i>	93
5	COMMUNICATION SERVER 2100 CONFIGURATION FOR MDC	94
5.1	ROADMAP OVERVIEW OF CS 2100 CONFIGURATION FOR MDC	94
5.1.1	<i>Summary of CS 2100 Configuration for MDC Server</i>	95
5.1.2	<i>Summary of CS 2100 Configuration for MDC Users</i>	96
5.1.3	<i>Summary of CS 2100 Configuration for MDC Phone/Assets</i>	97
5.2	REQUIRED INFORMATION FOR CS 2100 CONFIGURATION FOR MDC	99
6	REFERENCES	104
7	ACRONYMS AND DEFINITIONS	105
8	APPENDICES	107
	END OF DOCUMENT	107



List of Figures

Figure 1: Overview of CS 1000 Configuration	44
Figure 2: CS 1000 Element Manager Security Submenu	49
Figure 3: CS 1000 Element Manager Security Submenu	50
Figure 4: CS 1000 Element Manager System Passwords	50
Figure 5: CEM Password Basic Parameters	51
Figure 6: CEM Edit Password Basic Parameters	51
Figure 7: CEM: Select Limited Password Account	52
Figure 8: CEM Limited Access Password Account	52
Figure 9: CEM Limited Access Password Account for MDC (Part 1)	54
Figure 10: CEM Limited Access Password Account for MDC (Part 2)	55
Figure 11: CEM Confirm Changes Message and Request Backup	55
Figure 12: CEM Call Server Backup	56
Figure 13: CEM Call Server Backup in Progress	56
Figure 14: CEM Call Server Backup Successful (Part 1)	57
Figure 15: CEM Call Server Backup Successful (Part 2)	57
Figure 16: UCM Log In Screen	58
Figure 17: UCM Role Screen	58
Figure 18: UCM Add New Role Screen	59
Figure 19: UCM Select Element and/or Network Service for Role	59
Figure 20: UCM Permission Mapping for Role	60
Figure 21: UCM Role Details	60
Figure 22: UCM User Services	61
Figure 23: UCM Administrative Users	61
Figure 24: UCM Add New Administrative User	62
Figure 25: UCM	62
Figure 26: CEM Call Server Backup	63
Figure 27: CEM Call Server Backup in Progress	64
Figure 28: CEM Call Server Backup Successful (Part 1)	64
Figure 29: CEM Call Server Backup Successful (Part 2)	65
Figure 30: CS 1000 Element Manager Home – System Overview Screen	65
Figure 31: CS 1000 Element Manager Logon Screen	66
Figure 32: Ping from MDC Server to CS 1000 ELAN	66
Figure 33: Rlogin from MDC to CS 1000	67
Figure 34: Rlogin from MDC to CS 1000	69
Figure 35: Virtual Terminal Security Warning	70

Figure 36: Virtual Terminal Screen.....	70
Figure 37: Remote Login with Virtual Terminal	71
Figure 38: Prompt with Virtual Terminal	71
Figure 39: Login with Virtual Terminal.....	72
Figure 40: Disconnect Confirmation Dialog.....	72
Figure 41: Disconnected Virtual Terminal	73



List of Tables

Table 1: Required Information for RHEL O/S Installation and Configuration	11
Table 2: Required Information to Verify RHEL O/S Installation and Configuration	12
Table 3: Required Information for MDC Installation	13
Table 4: Required Information for Zebra Application Installation	14
Table 5: Required Information for Motorola RDM Installation	14
Table 6: Required Information for Microsoft ActiveSync Installation	15
Table 7: Required Information for CS1000 Configuration for MDC.....	15
Table 8: Required CS 1000 Information for Dual TN User Information.....	18
Table 9: Required CS 1000 Information for Shared TN user information	18
Table 10: Required CS 1000 Information for WLAN Handset.....	18
Table 11: Required CS 1000 Information for Dual TN Role Information [Optional]	19
Table 12: Required CS 1000 Information for Shared TN Role information [Optional]	19
Table 13: Required Information for CS2100 Configuration for MDC.....	19
Table 14: Required CS 2100 Information for Dual TN User Information.....	21
Table 15: Required CS 2100 Information for Shared TN user information	22
Table 16: Required CS 2100 Information for WLAN Handset.....	22
Table 17: Required CS 2100 Information for Dual TN Role Information [Optional]	22
Table 18: Required Information for Shared TN Role information [Optional]	22
Table 19: Required Information for KRS Configuration.....	24
Table 20: Required Information for Basic MDC Server Configuration	25
Table 21: Required Information for Integrating MDC Server and Location Server	27
Table 22: Required Information for Integrating MDC Server and Call Server.....	27
Table 23: Required Information for MDC Station Screen Customization.....	31
Table 24: Required Information for MDC Station Initialization	32
Table 25: Required Information for MDC Station Initialization	34
Table 26: Required Information for Remote MDC Station Configuration and Reboot	35
Table 27: Required Information for CS1000 Configuration for MDC.....	45
Table 28: Required CS 1000 Information for Dual TN User Information.....	47
Table 29: Required CS 1000 Information for Shared TN user information	48
Table 30: Required CS 1000 Information for WLAN Handset.....	48
Table 31: Required CS 1000 Information for Dual TN Role Information [Optional]	48
Table 32: Required CS 1000 Information for Shared TN Role information [Optional]	48
Table 33: Required Information for CS2100 Configuration for MDC.....	99
Table 34: Required CS 2100 Information for Dual TN User Information.....	102

Table 35: Required CS 2100 Information for Shared TN user information	102
Table 36: Required CS 2100 Information for WLAN Handset.....	102
Table 37: Required CS 2100 Information for Dual TN Role Information [Optional]	102
Table 38: Required Information for Shared TN Role information [Optional]	103



1 What's New in This Release

This is a high level summary of changes to the Mobile Device Checkout Customer Preparation Guide as a result of new functionality and enhancements in Mobile Device Checkout (MDC) Release 2.0:

- Updated Summary of Required Information for MDC Solution Deployment to reflect new features and enhancements in MDC Release 2.0
- Updated Communication Server 1000 Configuration for MDC, including:
 - Support for Communication Server 1000 Release 6.0
 - Support for SCR call type for users and handsets in addition MCR. Note: All users and phone must have the same call type.
 - When optional role feature is licensed on MDC:
 - Configuration of Roles on CS 1000
 - Configuration of two lines on WLAN handset when both role and personal phone number assignment will be used.
 - Restrictions on the inclusion of specific text as part of user names and handset names
- Introducing support for Communication Server 2100 as a call server in the MDC Solution

For further details on MDC Release 2.0, refer to the Mobile Device Checkout Solution Overview and other sections of NN49010-600 Nortel Healthcare Solutions MDC Administration Guide.

2 Introduction

This document provides customer preparation information for the Mobile Device Checkout Solution. The intent is to describe the actions which can be performed in advance by customers. These customer preparations steps can facilitate the deployment of the Mobile Device Checkout (MDC) Solution when these steps are performed in advance of the deployment. This document describes the preparation procedures in generic terms. It is not the intention of this document to provide customer-specific information.

A full description of the Mobile Device Checkout Solution can be found in NN49010-600 Nortel Healthcare Solutions MDC Administration Guide.

The description of the deployment of the Mobile Device Checkout Solution can be found in NN49010-501 Nortel Healthcare Solutions MDC Deployment Guide. This includes the solution engineering, hardware and software requirements for the Mobile Device Checkout Solution.

A complete list of documentation on Mobile Device Checkout Solution is listed in NN49010-100 Nortel Healthcare Solutions MDC Documentation Roadmap.

2.1 Purpose and Scope

The customer preparatory information for the Mobile Device Checkout Solution is organized into the following distinct sections:

- Summary of the required information needed for the installation, configuration and integration of Mobile Device Checkout Solution:

This section describes the network and component information which must be gathered before starting the deployment of a Mobile Device Checkout Solution. The summary of required information starts in Section 3 of this document. This information is taken from the NN49010-501 Nortel Healthcare Solutions MDC Deployment Guide.
- Communication Server 1000 Configuration for Mobile Device Checkout Solution:

This section describes the Communication Server 1000 configuration specific for the Mobile Device Checkout Solution. The expectations are the customer will execute this provisioning in advance of the deployment of MDC Solution. The Communication Server 1000 configuration procedures start in Section 4 of this document.
- Communication Server 2100 Configuration for Mobile Device Checkout Solution:

This section describes the Communication Server 2100 configuration specific for the Mobile Device Checkout Solution. The expectations are the customer will execute this provisioning in advance of the deployment of MDC Solution. The Communication Server 2100 configuration procedures start in Section 5 of this document.

2.2 Target Audience

This manual is intended for the Solution Engineers (e.g. network engineers, integration engineers, support engineers) responsible for the deployment of the MDC Solution. These engineers should have an understanding of MDC, CS 1000, CS 2100, Asset Tracking Management System, WLAN networks, TCP/IP networks, and computer hardware and networks services.

2.3 Assumptions

Communication Server 1000 (CS 1000) or Communication Server 2100 (CS 2100) is assumed to be installed, configured and operational. The MDC Solution integrates with CS 1000 Releases 5.0, 5.5, and 6.0 only and CICM 10.1 MR2 load (which is compatible with SE10, SE11, and SE13) for CS 2100.

WLAN 2300 is assumed to be installed, configured and operational for telephony, including the TM2245, 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 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 document:

- The detailed steps for the physical installation of the server's hardware for MDC Server and MDC Management Station. Refer to the manufacturer's documentation for details.
- This document does not cover detailed steps for the physical installation of the PC hardware or installing the base operating system on the MDC Management Station.
- Comprehensive CS 1000 and CS 2100 configuration is not covered in this document except where related to the CS 1000 configuration for MDC.
- Complete WLAN 2300 configuration is not covered in this document except where related to the WLAN configuration for MDC.
- Nortel Asset Tracking and Management Solution installation and configuration is not covered in this document.

3 Summary of Required Information for MDC Solution Deployment

This section summarizes the required information needed prior to starting the installation, configuration and integration of Mobile Device Checkout Solution. This is the network and component information which must be gathered before starting the deployment of a Mobile Device Checkout Solution.

3.1 Hardware and Software Requirements for MDC

The description of the solution engineering, hardware and software requirements for the Mobile Device Checkout Solution is in NN49010-501 Nortel Healthcare Solutions MDC Deployment Guide.

3.2 Information Required for Installation

3.2.1 Required Information for RHEL Installation and Configuration

Prior to starting RHEL installation, you should have this required information for the installation:

Table 1: Required Information for RHEL O/S Installation and Configuration

	Required Information for RHEL Installation	
1	Access to RHEL Release 5.0 or later Release 5.x installation media	
2	Installation key or licenses for RHEL	
3	Language for installation (default language for OS)	
4	Language for keyboard	
	For disk partitions:	
5	amount of RAM on your server	
6	amount of hard drive space on your server	
	For Ethernet interface 0	
7	used for TLAN or ELAN/CS-LAN? (TLAN recommended for dual NIC server) (must be both for single NIC server)	
8	IP address (DHCP not recommended)	
9	netmask	
	For Ethernet interface 1	
10	used for TLAN or ELAN/CS-LAN? (ELAN/CS-LAN recommended for dual NIC server) (Ethernet i/f 1 is not needed for single NIC server)	
11	IP address (DHCP not recommended)	
12	netmask	
13	Hostname for MDC server (otherwise defaults to localhost)	

14	Domain name for organization (format host.domain.com)	
	For network configuration	
15	gateway IP address	
16	IP address of Primary DNS	
17	IP address of Secondary DNS (if applicable)	
18	Time zone	
19	NTP server IP address	
20	Root password for MDC Server (due to OS hardening, a non-root username and password is needed to login into MDC Server and then su - root)	
20a	Non-root username and password for MDC Server	
21	Red Hat login (username and password) or installation number to register subscription.	
22	MDC Server has Internet access	

3.2.2 Required Information to verify RHEL O/S Installation and Configuration

Prior to verifying RHEL installation, you should have this required information:

Table 2: Required Information to Verify RHEL O/S Installation and Configuration

	Required Information to verify RHEL Installation and Configuration	
	For disk partitions:	
1	amount of RAM on your server	
2	amount of hard drive space on your server	
	For Ethernet interface 0	
3	used for TLAN or ELAN/CS-LAN? (TLAN recommended for dual NIC server) (must be both for single NIC server)	
4	IP address (DHCP not recommended)	
5	netmask	
	For Ethernet interface 1	
6	used for TLAN or ELAN/CS-LAN? (ELAN recommended for dual NIC server) (Ethernet i/f 1 not needed for single NIC server)	
7	IP address (DHCP not recommended)	
8	netmask	
9	Hostname for MDC server (otherwise defaults to localhost)	
10	Domain name for organization (format host.domain.com)	
	For network configuration	
11	gateway IP address	

12	IP address of Primary DNS	
13	IP address of Secondary DNS (if applicable)	
14	IP address of MDC Server	
15	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))	
15a	Non-root username and password for MDC Server	
16	Red Hat login (username and password) or installation number to register subscription	
17	MDC Server has Internet access	

3.2.3 Required Information for MDC Installation

This is the required information for MDC application installation that you should have prior to starting the installation:

Table 3: Required Information for MDC Installation

	Required Information for MDC Installation	
1	IP address of MDC Server	
2	Root password for MDC Server to run the installation (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))	
2a	Non-root username and password for MDC Server	
3	Customer userid and password credentials for www.nortel.com	
4	Directory on MDC Server to place MDC installation media	
5	Credentials (user name, password) for an existing administration account to access MySQL	
6	Credentials (user name, password) for an account to access MySQL for MDC application. This account may be shared with other EBS applications.	
7	IP address of the MDC Server Ethernet port connected to call server.	
8	MDC Server has Internet access	



3.2.4 Required Information for Zebra Application Installation

Requirements before installing ZebraDesigner software:

Table 4: Required Information for Zebra Application Installation

	Required Information for Zebra Application Installation	
1	Registered userid on Zebra website www.zebra.com to permit download of manuals and software. Click the Login at the top of the page to initiate the registration process.	
2	Userid with Administrator rights on the MDC Management Station PC to perform the installation.	
3	Closure of all software application during installation on MDC Management Station.	
4	Zebra GK420t Printer MUST use thermal transfer media	
5	Directory on MDC Management Station to store the barcode label file. The default directory is My Document\My Labels\Labels.	
6	Internet Access	

3.2.5 Required Information for Motorola RDM Installation

Requirements before installing Motorola RDM software (RDM is only needed if MK1200 or MK1250 Micro-kiosks will be deployed):

Table 5: Required Information for Motorola RDM Installation

	Required Information for Motorola RDM Installation	
1	Userid with Administrator rights on the MDC Management Station PC to perform the installation.	
2	Internet Access	

3.2.6 Required Information for Microsoft ActiveSync Installation

Requirements before installing Microsoft ActiveSync software:

Table 6: Required Information for Microsoft ActiveSync Installation

	Required Information for Microsoft ActiveSync Installation	
1	Userid with Administrator rights on the MDC Management Station PC to perform the installation.	
2	Internet Access	

3.3 Information Required for Configuration

This is the summary of the required information needed prior to starting the configuration and integration of the MDC Solution. The information has been grouped into lists which the data applies to the configuration or integration of the components of the MDC Solution:

3.3.1 Required Information for Call Server Configuration for MDC

3.3.1.1 Required Information for CS 1000 Configuration for MDC

The following information is needed prior to starting to configure the CS 1000 for the MDC Solution:

Table 7: Required Information for CS1000 Configuration for MDC

	Required Information for CS1000 Configuration for MDC	
1	IP address of the CS 1000 Element Manager	
2	CS 1000 Element Manager Login information	
3	CS 1000 UCM Login information (for CS 1000 Release 6.0 or later releases)	
4	User ID and password for the CS 1000 administration user name. For most tasks, admin-level1 privileges will be sufficient. However, admin2-level privileges are required for the creation of a limited access user account for the MDC application.	
5	IP address of the CS 1000 Call Server (for virtual terminal sessions)	
6	Customer Group for phones and users	

7	Failed Log in Threshold used by customer for password basic parameters	
8	Port Lockout duration used by customer for password basic parameters	
9	Inactivity Timeout for password basic parameters (minimum of 20 minutes or longer recommended)	
10	Parameters for Limited Access Password account (in CS 1000 Release 5 and 5.5): <ul style="list-style-type: none"> ○ User Name ○ Password 	
11	For Limited Access Password Account Role (in CS 1000 Release 6 or later) <ul style="list-style-type: none"> ○ Role Name ○ Role Description 	
12	Parameters for Limited Access Password Account (in CS 1000 Release 6.0 or later) <ul style="list-style-type: none"> ○ User ID ○ Full Name ○ Temporary Password ○ Permanent Password 	
13	IP address for MDC Server	
14	Root password for MDC Server	
15	Non-root username and password for MDC Server (due to OS security hardening, root account cannot be used to log into MDC Server)	
16	Multiple Call Arrangement with Ring (MCR) or Single Call Ringing (SCR)	This call type must be the same for all phones, users and roles used with MDC.
17	To provision each user for dual TN (Terminal Number) deployment: <ul style="list-style-type: none"> ○ Terminal number (TN) ○ Directory number (DN) ○ Phone type or terminal type ○ Name of employee (first & last) ○ Description ○ QoS Zone 	See table below to capture dual TN user information

18	<p>To provision users for shared TN (Terminal Number) deployment:</p> <ul style="list-style-type: none"> ○ Shared Terminal number (TN) ○ Phone type or terminal type ○ Description ○ QoS Zone ○ Number of Key Extension Modules (KEM) <p>To provision each users in this shared TN (Terminal Number) deployment:</p> <ul style="list-style-type: none"> ○ Key number ○ Directory number (DN) ○ Name of employee (first & last) 	See table below to capture shared TN user information
19	<p>To provision each mobile WLAN phones for MDC:</p> <ul style="list-style-type: none"> ○ Terminal number (TN) ○ Directory number (DN) – key 0 ○ [optional] Directory number (DN) – key 1 ○ Description 	<p>See table below to capture phone information.</p> <p>Key 1 is only required if the optional MDC role feature will be used in the mode where both the user's personal phone number and the role phone number will be assigned to the handset during checkout</p>
20	<p>[Optional] To enable location tracking on the WLAN phone (only if the phone will be location tracked):</p> <ul style="list-style-type: none"> ○ IP address of EPE (Ekahau Positioning Engine) ○ ELP (Ekahau Location Port) number 	This information is only needed if optional MDC location tracking feature will be used.
21	<p>[Optional] To provision each role for dual TN (Terminal Number) deployment:</p> <ul style="list-style-type: none"> ○ Terminal number (TN) ○ Directory number (DN) ○ Phone type or terminal type ○ Display Name of role ○ Description ○ QoS Zone 	<p>Only required if the optional MDC role feature will be used.</p> <p>See table below to capture dual TN role information</p>

22	<p>[Optional] To provision roles for shared TN (Terminal Number) deployment:</p> <ul style="list-style-type: none"> ○ Shared Terminal number (TN) ○ Phone type or terminal type ○ Description ○ QoS Zone ○ Number of Key Extension Modules (KEM) <p>To provision each role in this shared TN (Terminal Number) deployment:</p> <ul style="list-style-type: none"> ○ Key number ○ Directory number (DN) ○ Display name of role 	<p>Only required if the optional MDC role feature will be used.</p> <p>See table below to capture shared TN role information</p>
----	---	--

Table 8: Required CS 1000 Information for Dual TN User Information

Terminal number (TN)	Directory number (DN)	Phone type or terminal type	Name of employee (first & last)	Description	QoS Zone

Table 9: Required CS 1000 Information for Shared TN user information

Shared Terminal number (TN)	Phone type or terminal type	Description	QoS Zone	Key number	Directory number (DN)	Name of employee (first & last)

Table 10: Required CS 1000 Information for WLAN Handset

Terminal number (TN)	Directory number (DN) – key 0	[Optional] Directory Number (DN)-key 1	Description

--	--	--	--

Table 11: Required CS 1000 Information for Dual TN Role Information [Optional]

Terminal number (TN)	Directory number (DN)	Phone type or terminal type	Name of Role	Description	QoS Zone

Table 12: Required CS 1000 Information for Shared TN Role information [Optional]

Shared Terminal number (TN)	Phone type or terminal type	Description	QoS Zone	Key number	Directory number (DN)	Name of Role

3.3.1.2 Required Information for CS 2100 Configuration for MDC

The following information is needed prior to starting to configure the CS 2100 for the MDC Solution:

Table 13: Required Information for CS2100 Configuration for MDC

	Required Information for CS2100 Configuration for MDC	
1	SESM Server IP Address	This is the same as PTM IP Address
2	user name and password to login to SESM Server	
3	Root password for SESM Server	
4	SESM account for MDC: <ul style="list-style-type: none"> Userid Password 	
5	OSSGATE port number on SESM	The port number is provisionable on the SESM
6	IP address for MDC Server	

7	Non-root username and password for MDC Server (due to OS security hardening, root account cannot be used to log into MDC Server)	
8	Root password for MDC Server	
9	Multiple Call Arrangement (MCA) or Single Call Arrangement (SCA)	This call type must be the same for all users and roles used with MDC.
10	<p>These values are the same of all users, phones and roles with MDC:</p> <ul style="list-style-type: none"> • Customer Group for phones and users • Customer Subgroup • Network Class of Service • Local Access and Transport Area (LATA) 	
11	<p>To provision each user for dual TN (Terminal Number) deployment:</p> <ul style="list-style-type: none"> • LEN (used as Terminal number (TN)) • Directory number (DN) • Phone type or terminal type • Name of employee (first & last) 	See table below to capture dual TN user information
12	<p>To provision users for shared TN (Terminal Number) deployment:</p> <ul style="list-style-type: none"> • Shared LEN (used as Terminal number (TN)) • Phone type or terminal type <p>To provision each users in this shared TN (Terminal Number) deployment:</p> <ul style="list-style-type: none"> • Key number • Directory number (DN) • Name of employee (first & last) 	See table below to capture shared TN user information
13	CICM Profile for handset	<p>Profile should define Key 1 and optionally Key 2. Key 2 is only required if the optional MDC role feature will be used in the mode where both the user's personal phone number and the role phone number will be assigned to the handset during checkout</p> <p>The CICM handset profile must permit autologin.</p>

14	Distinct user names for each WLAN handset	This is the parameter entered under the USERID option when the phone is provisioned. The USERID is typically part or all of the default DN. This username is needed to log the phone in.
15	Common password to be used on all WLAN handsets user names.	This parameter is entered when the phone is provisioned. This information is needed to log the phone in.
16	To provision each mobile WLAN phones for MDC: <ul style="list-style-type: none"> • LEN (used as Terminal number (TN)) • Directory number (DN) – key 1 	See table below to capture phone information.
17	[Optional] To enable location tracking on the WLAN phone (only if the phone will be location tracked): <ul style="list-style-type: none"> • IP address of EPE (Ekahau Positioning Engine) • ELP (Ekahau Location Port) number 	This information is only needed if optional MDC location tracking feature will be used.
18	[Optional] To provision each role for dual TN (Terminal Number) deployment: <ul style="list-style-type: none"> • LEN (used as Terminal number (TN)) • Directory number (DN) • Phone type or terminal type • Display Name of role 	Only required if the optional MDC role feature will be used. See table below to capture dual TN role information
19	[Optional] To provision roles for shared TN (Terminal Number) deployment: <ul style="list-style-type: none"> • Shared LEN (used as Terminal number (TN)) • Phone type or terminal type To provision each role in this shared TN (Terminal Number) deployment: <ul style="list-style-type: none"> • Key number • Directory number (DN) • Display name of role 	Only required if the optional MDC role feature will be used. See table below to capture shared TN role information

Table 14: Required CS 2100 Information for Dual TN User Information

Line Equipment Number (LEN)	Directory number (DN)	Phone type or terminal type	Name of employee (first & last)

Table 15: Required CS 2100 Information for Shared TN user information

Shared Line Equipment Number (LEN)	Phone type or terminal type	Key number	Directory number (DN)	Name of employee (first & last)

Table 16: Required CS 2100 Information for WLAN Handset

Line Equipment Number (LEN)	Directory number (DN) – key 1

Table 17: Required CS 2100 Information for Dual TN Role Information [Optional]

Line Equipment Number (LEN)	Directory number (DN)	Phone type or terminal type	Name of role

Table 18: Required Information for Shared TN Role information [Optional]

Shared Line Equipment Number (LEN)	Phone type or terminal type	Key number	Directory number (DN)	Name of role

3.3.1.3 Preparing for Bulk Loading Users and Phones into MDC

[Optional] Use the following format to capture information into input files for bulk loading of users into MDC. The use of bulk loading files is optional. Alternatively, the user and phone information can be entered individually through the MDC Admin GUI:

- The input files used with the bulk loading scripts should be derived from a primary data source used to drive CS 1000 configuration, such as LDAP. The information on the MDC must exactly match the configuration on the CS 1000 and it must remain synchronized. Any mismatch of information will impair service.
- 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.
- A CS 1000 terminal number (TN) must have the format **aaa b cc dd** where:
 - aaa** is the loop number. A single or double digit number may have leading zeros. For example, the number eight may be shown as 8, 08 or 008.
 - b** is the shelf number (either 0 or 1)
 - cc** is card number (number from 1-4 or 7-10). A single digit number may have leading zeros. For example, the number eight may be shown as 8 or 08.
 - dd** is the line number (number from 0 to 31). A single digit number may have leading zeros. For example, the number eight may be shown as 8 or 08.
- 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
- For CS 2100, the DN specified must be the full 10 digit DN, even if extension dialing is supported.
- The fields of the user input file are fixed as shown below for CS 1000. The General Description field is optional:

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 fields of the phone asset input file are fixed as shown below for CS 1000. 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

- A sample asset input file for CS 2100 call server is shown below. 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

3.3.2 Required Information for KRS

The following information is needed prior to starting to configure of KRS for the MDC Solution:

Table 19: Required Information for KRS Configuration

	Required Information for KRS Configuration	
1	User name and password to access KRS. Note: It may take up to 5 business days to validate registration and provide access to KRS.	
2	Site name for this specific MDC system. Blanks spaces are not allowed within the site name	
3	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	
4	Electronic authorization codes for purchased MDC license features can be one of the following: <ul style="list-style-type: none"> SAP Sale Order Number/ Nortel Order Number (COEO) Customer PO Number SAP Non Stock PO Number 	

	<ul style="list-style-type: none"> Numeric Authorization Code 	
5	Number of MDC Stations (kiosks) licenses are to be allocated for this specific MDC	
6	Number of assets (phones) licenses are to be allocated for this specific MDC	
7	[Optional] Number of location-tracking-enabled users licenses are to be allocated for this specific MDC, if location tracking is being used.	
8	[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.	
9	Folder on the local computer to place copy of the MDC keycode license file	
10	IP address for this specific MDC Server	
11	Root password for this specific 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))	
11a	Non-root username and password for MDC Server	

3.3.3 Required Information for Basic Configuration of MDC Server

The following information is needed prior to starting of basic configuration of MDC Server for the MDC Solution:

Table 20: Required Information for Basic MDC Server Configuration

	Required Information for Basic MDC Server Configuration	
1	IP address of the MDC Server	
2	New password for the default admin user	
3	Email address for default admin user	
4	First name and last name for default admin user	
5	Language for MDC Admin GUI. Only English is	

	supported in Release 2.0	
6	<p>Backup Server:</p> <ul style="list-style-type: none">• IP address of the backup server• Port used for SFTP with backup Server. Default port for SFTP is 22• Userid and password to log in to SFTP on the backup server• Backup server directory where MDC backup images will be stored	
7	<p>Backup Schedule:</p> <ul style="list-style-type: none">• Day of week (or All) to schedule backups• Hour of day and minute of hour to initiate backup• [Optional] Descriptive comment for each automatic backup scheduled	
8	<p>Email Settings for Event Notification digests:</p> <ul style="list-style-type: none">• Email address of recipient• Email address of sender• Name of sender• Hostname of SMTP Server• SMTP port number. The default SMTP port is 25• Number of days to retain event notification digest emails. Default value is 7 days. Maximum value is 30 days.	
9	<p>Asset Notification Alarms:</p> <ul style="list-style-type: none">• [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	
10	<p>[Optional] Configuration for each administration users:</p> <ul style="list-style-type: none">• First name and last name of the administrative user• User name and password for the administrative user• Email address of the administrator	

	user	
--	------	--

3.3.4 Required Information for integrating MDC Server and Location Server

The following information is needed prior to integrating MDC Server and Location Server for the MDC Solution. This information is optional as it only applies if location tracking will be used.

Table 21: Required Information for Integrating MDC Server and Location Server

	Required Information for Integrating MDC Server and Location Server	
1	Location service product (Ekahau or SynTrack)	
2	IP address of Location Server	
3	Port to communicate with Location Server. The default port for SynTrack is 443. The default port for Ekahau is 8550.	
4	User name and password to communicate with Location Server	
5	If using SynTrack for Healthcare for location tracking, the following additional information is needed: <ul style="list-style-type: none"> IP address of SynTrack Admin GUI User name and password for SynTrack Admin GUI 	
6	IP address of the MDC Server	
7	Administrative username and password for MDC Admin GUI	

3.3.5 Required Information for Integrating MDC Server and Call Server

The following information is needed prior to integrating MDC Server and Call Server for the MDC Solution:

Table 22: Required Information for Integrating MDC Server and Call Server

	Required Information for Integrating MDC Server and Call Server	
1a	For CS 1000 connection: <ul style="list-style-type: none"> Release version of the CS 1000 IP address of the CS 1000 Call Server 	

	<p>on E-LAN</p> <ul style="list-style-type: none"> • User name and password for limited-access user account for MDC to use to login into CS 1000 • Customer Number for phones and users • Rlogin Session Timeout (the inactivity timeout for passwords on the 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 users and phones (and roles if applicable) on this call server • Whether to disable return phones 	
1b	<p>For CS 2100 connection:</p> <ul style="list-style-type: none"> • 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 users (and roles if applicable) on this call server • Whether phones should be disabled (from making calls) when they are returned. For CS 2100, phones must 	

	always be disabled when not checked out.	
2	For barcode labels: <ul style="list-style-type: none"> • Unique starting number of barcode labels for phones • Number of phone labels to print • Unique starting number for barcode labels for users (if needed) • Number of user labels to print 	
3	For each asset(phone) added to MDC: <ul style="list-style-type: none"> • Barcode labels of phones • Tag type • Default DN • Phone type • Terminal number • MAC address • Whether asset is tracking enabled • [Optional] Description of asset 	
4	For each user added to MDC: <ul style="list-style-type: none"> • Barcode labels of user • Tag type • Phone number/ DN • Display name • First name • Last name • Whether user is tracking enabled • [Optional] Description of user 	
5	Optional: data file for bulk loading of assets can be used.	
6	Optional: data file for bulk loading of users can be used.	
7	UNIX root user password for the MDC Server if using bulk loading files will be used (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))	
7a	Non-root username and password for MDC	

	Server	
8	IP address of the MDC Server	
9	Administrative username and password for MDC Admin GUI	

3.3.6 Required Information for Creating Roles on MDC Server

The following information is needed prior to creating roles on MDC Server:

	Required Information for creating roles on MDC Server	
1	IP address of the MDC Server	
2	Username and password for MDC Admin GUI	
3	<p>For each Role:</p> <ul style="list-style-type: none"> • 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. • 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. This field is optional. • 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 	
4	<p>For each Role Category:</p> <ul style="list-style-type: none"> • 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. • 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. <ul style="list-style-type: none"> Brief text description of the role category List of roles associated with this role category 	
5	For each Role Templates: <ul style="list-style-type: none"> 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 	
6	Username and password for MDC Admin GUI	

3.3.7 Required Information for MDC Station Configuration

Ensure that you have the information in the following sections prior to starting to configure MDC Stations:

3.3.7.1 Required Information for MDC Station Configuration

The following information is optional and is only required for MDC Station configuration:

Table 23: Required Information for MDC Station Screen Customization

	Required Information for Integrating MDC Server and Location Server	
1	IP address of the MDC Server	
2	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))	
2a	Non-root username and password for MDC Server	
4	Username and password for MDC Admin GUI	
3	[Optional]: logo gif file (must be 320 x 50 pixels) only needed if the customer wants to	

	have their logo appear on the MDC Station screen.	
4	Help Desk number	
5	Language on MDC Station <ul style="list-style-type: none"> Languages to be used on MDC Station Order of these languages on the MDC Station 	
6	For each Station Location: <ul style="list-style-type: none"> 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. 	

3.3.7.2 Required Information for MK1200 & MK1250 MDC Station initialization

The following information is needed prior to starting the configuration and initialization of the MK1250 & MK1250 MDC Stations:

Table 24: Required Information for MDC Station Initialization

	Required Information for MDC Station Initialization	
1	IP address of MDC Server	
2	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))	
2a	non-root username and password for MDC Server	
4	IP address scheme for MDC Stations: dynamic or static:	

	<ul style="list-style-type: none"> Static IP addresses for each MDC Station if static IP addresses are used DHCP Options [optional] and DHCP Server [optional] if dynamic IP addresses are used 	
5	<p>Wireless LAN information (only if MK1250 Wireless Microkiosks are used):</p> <ul style="list-style-type: none"> WLAN SSIDs for local AP and the APs for locations where MDC Stations will be permanently installed. It is recommended a separate SSID be used for the wireless MDC Stations. Authentication used by AP: Choice of none, Kerberos, LEAP, EAP-TLS, and PEAP. Additional information may be needed depending on authentication used, such as certificates. Encryption used by AP. Choice of Open System, WEP, Keyguard-MCM, and TKIP (WPA). TKIP(WPA) is the recommended encryption. A shared passkey is needed. 	
6	<p>Network information (only needed if static IP addresses are being used):</p> <ul style="list-style-type: none"> Subnet mask Default gateway 	
7	<p>[Optional] MDC Station configuration customer customization information:</p> <ul style="list-style-type: none"> Password for reboot [optional] FTP user authentication server [optional] Time zone [optional] Daylight Savings Time [optional] if in effect and automatic Time service server [optional] as fully qualified domain name 	
8	Working directory on MDC Management Station to copy configuration files to and customize them.	
9	Username and password for MDC Admin GUI	

3.3.7.3 Required Information for KDT900 MDC Station initialization

The following information is needed prior to starting the configuration and initialization of the KDT900 MDC Stations:

Table 25: Required Information for MDC Station Initialization

	Required Information for MDC Station Initialization	
1	IP address of MDC Server	
2	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))	
2a	non-root username and password for MDC Server	
3	[Optional] list of usernames and passwords for ftp/telnet access to MDC Station	
4	IP address scheme for MDC Stations: dynamic or static: <ul style="list-style-type: none"> Static IP addresses for each MDC Station if static IP addresses are used DHCP Options [optional] and DHCP Server [optional] if dynamic IP addresses are used 	
5	Wireless LAN information (only if KDT900 Wireless scanners are used): <ul style="list-style-type: none"> WLAN SSIDs for local AP and the APs for locations where MDC Stations will be permanently installed. It is recommended a separate SSID be used for the wireless MDC Stations. Authentication used by AP: Choice of none, Kerberos, LEAP, EAP-TLS, and PEAP. Additional information may be needed depending on authentication used, such as certificates. Encryption used by AP. Choice of Open System, WEP, Keyguard-MCM, and TKIP (WPA). TKIP(WPA) is the recommended encryption. A shared passkey is needed. 	
6	Network information (only needed if static IP addresses are being used): <ul style="list-style-type: none"> Subnet mask 	

	<ul style="list-style-type: none"> • Default gateway 	
7	[Optional] MDC Station configuration customer customization information: <ul style="list-style-type: none"> • Time zone [optional] • Daylight Savings Time [optional] if in effect and automatic • Time service server [optional] as fully qualified domain name 	
8	Working directory on MDC Management Station to copy configuration files to and customize them.	
9	Username and password for MDC Admin GUI	
10	Whether POE will be used at final installation site	

3.3.7.4 Required Information for Remote MK1200 & MK1250 MDC Station Configuration and Reboot

To use Motorola RDM with MK1250 and MK1200 MDC Stations, ensure that you have the following information prior to starting:

Table 26: Required Information for Remote MDC Station Configuration and Reboot

	Required Information Remote MDC Station Configuration and Reboot	
1	Access to MDC Management Station	
2	Windows username and password for MDC Management Station	
3	Windows username and password for MDC Management Station with administrative privileges (optional: only if Motorola RDM application needs to be installed)	
4	Internet Access (optional: only if Motorola RDM application needs to be installed)	
5	IP address of MDC Server	
6	Username and password for MDC Admin GUI	

7	IP addresses and MAC addresses of MDC Stations (from the MDC Admin GUI)	
8	mkconfig.reg file (optional: only if this MDC Station configuration file needs to be updated)	

4 Communication Server 1000 Configuration for MDC

This section provides an overview of the required Communication Server (CS) 1000 configuration steps that precede integration with the rest of the MDC Solution and a list of the required information. The MDC Solution integrates with CS 1000 Releases 5.0, 5.5 and 6.0.

WARNING: It is strongly recommended that the CS 1000 configuration steps should only be performed by a qualified CS 1000 Administrator who has detailed knowledge and understanding of the CS 1000 Element Manager and Unified Communication Manager.

If needed, the CS 1000 Product documentation should be used as reference for the detailed steps for the procedures. Remember to use the documentation specific to the release of CS 1000 being used. There are variations in the CEM navigation menu and screens between Releases 5.0, 5.5 and 6.0 so your system may differ from the screen captures in this document. There may also be variations based on whether the CS 1000 is running on VxWorks or Linux operating system.

The following manuals are useful. Use the appropriate version based on the CS 1000 release being used:

- Nortel Communication Server 1000 System Management Reference NN43001-600 Standard Release 5.5
- Nortel Communication Server 1000 Software Input Output Reference – Administration NN43001-611
- Nortel Communication Server 1000 Element Manager System Reference – Administration NN43001-632
- Nortel Communication Server 1000 Network Routing Service Installation and Commissioning NN43001-564
- Nortel Communication Server 1000 Unified Communications Management Common Services Fundamentals NN43001-116
- Nortel Communication Server 1000 Security Management Fundamental NN43001-604
- Nortel Communication Server 1000 IP Phones Description, Installation and Operations
- Nortel WLAN Handset Fundamentals NN43001-505
- Nortel IP Line Fundamentals NN43100-500
- Nortel WLAN IP Telephony Installation and Commissioning NN43001-504
- Nortel WLAN Handset 6120 and WLAN Handset 6140 User Guide NN43150-100
- Nortel WLAN Handset 2210 User Guide NN10300-077
- Nortel WLAN Handset 2211 User Guide NN10300-078
- Nortel WLAN Handset 2212 User Guide NN10300-071

4.1 Roadmap Overview of CS 1000 Configuration for MDC

It is intended that these preparatory steps for CS 1000 can be performed in advance of the deployment of the MDC Solution. The CS 1000 configuration for MDC Solution consists of the following sequence of steps:

1. Verify you have the information needed prior to starting to configure the CS 1000 for the MDC Solution. The required information is listed in Section 4.2 *Required Information for CS 1000 Configuration for MDC*.
2. Execute basic CS 1000 configuration to enable the MDC application to communicate with the CS 1000. These details are summarized in Section 4.1.1 *Summary of CS 1000 Configuration for MDC Server*.

3. Validate the basic network connectivity and communication between CS 1000 and MDC Server if the operating system has been installed on MDC Server. These procedures are described in Section 4.4 *Testing connectivity between CS 1000 and MDC*.
4. Create new employee configuration on the CS 1000 or verify existing employee configuration to ensure these are compatible with the MDC Solution. The employee configuration will be used as the basis for users on the MDC Solution. The details are summarized in Section 4.1.2 *Summary of CS 1000 Configuration for MDC Users*.
5. Create new WLAN handset configuration on the CS 1000 or verify existing WLAN handset configuration to ensure these are compatible with the MDC Solution. The WLAN handset configuration will be used as the basis for phone asset on the MDC Solution. The details are summarized in Section 4.1.3 *Summary of CS 1000 Configuration for MDC Phone/Assets*.
6. If the optional role feature is licensed on MDC, create new role configuration on the CS 1000 or verify existing role configuration to ensure these are compatible with the MDC Solution. The role configuration will be used as the basis for roles on the MDC Solution. The configuration of roles is similar to the configuration of employees except roles are associated with functions (such as Doctor on call) rather than people. For further guidelines on configuring roles, refer to Section 4.1.2 *Summary of CS 1000 Configuration for MDC 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 for all the phones, roles and users on the call server.

7. Backup the CS 1000 configuration to preserve any configuration changes made for the MDC Solution. The detailed procedure is described in Section 4.3.4 *Backup of CS 1000 Element Manager* for CEM or Section 4.8.13 *Backup* from the command line.

WARNING: In addition, it is recommended to coordinate the following CS 1000 activities to avoid impacting MDC operations:

- It is recommended to avoid CS 1000 maintenance activities when adding/updating phones, users and roles on MDC Administration GUI as some maintenance activities may impact the MDC's ability to automatically retrieve data from CS 1000 call server. In particular, the use of backup should be avoided during MDC provisioning of users and roles to prevent an overlay conflict. If this condition cannot be avoided, the MDC administrator has the option to manually enter data when the MDC is unable to automatically retrieve information from CS 1000 call server.
- It is recommended to avoid scheduling CS 1000 maintenance activities (such as backup, restore, restarts, reboots or upgrades) during shift changes or periods of high MDC Station usage (i.e. checkout or returns). Any CS 1000 activities which prevent the ability to make CS 1000 provisioning changes will adversely affect MDC checkout or returns.

4.1.1 Summary of CS 1000 Configuration for MDC Server

Perform the following CS 1000 configuration to enable the MDC application to communicate with the CS 1000.

Verify you have the information needed prior to starting to configure the CS 1000 for the MDC Solution. The required information is listed in Section 4.2 *Required Information for CS 1000 Configuration for MDC*.

1. Verify there are at least three pseudo terminals (PTY) when a CS 1000 is used with MDC. See Section 4.6 *Creating Pseudo Terminals (PTY) for MDC* for the detailed procedure if needed.
2. Enable multiple user logins. See Section 4.7 *Enable Multiple User Login* for the detailed procedure if needed.
3. Enable multiple loop dial number so the same phone number can be used across different phone loops. See Section 4.8.1 *Permit Multiple Loop Dial Number* for the detailed procedure if needed.

4. Login into the CS 1000 Element Manager (CEM). Refer to Section 4.3 *CS 1000 Base Configuration* if additional details are needed on the login procedure or any of the following CEM procedures.
5. Enable Insecure Shells for rlogin. Refer to Section 4.3.1 *Enable Insecure Shells for Rlogin* if additional details are needed.
6. To assist with integration testing, it is recommended to temporarily increase the failed login threshold and temporarily shorten the port lockout duration until connectivity between MDC and CS 1000 is tested and established.
7. For CS 1000 Release 5.x, create a limited access password account for MDC specifying the:
 - User Name
 - Password
 - Overlay(OVLY) for the Password Access Type (PWTP)
 - Enable Host Mode Log In (HOST)
 - Enable OTM or MAT Log In (MAT)
 - Permit Allowed Overlay List (OVLA) for:
 - Overlay 10,
 - Overlay 11,
 - Overlay 20,
 - Overlay 22,
 - Overlay 32,
 - Overlay 95
 - Customer group under Accessible Customer (CUST)
 - Allow Configuration Prompts for Overlay Options (OPT)

Refer to Section 4.3.2 *Create LAPW Password Account on CS 1000 Rel 5.x for MDC* if additional details are needed.

8. For CS 1000 Release 6.0, log in to UCM and create an administrative role with:
 - Default CS1000 Permissions
 - Specified OAM privileges, specified customers
 - No Diagnostics
 - With the following Specified OAM Privileges (LAPW):
 - Telephony Manager (MAT)
 - Customer Group number under the Customer and Tenant section
 - Select the following under Specified Services and Features:
 - (10) Analog Sets Administration
 - (11) Digital Sets Administration
 - (20) Print Routine 1
 - (22) Print Routine 3
 - (32) Network and Peripheral Equipment Diagnostics
 - (95) Calling Party Name Display

Create an administrative user account for MDC based on this limited privilege role. Change the password to create the permanent password for this administrative user account for MDC to access CS 1000.

Refer to Section 4.3.3 *Create Limited Access Password (LAPW) Role on CS 1000 Rel 6 for MDC* if additional details are needed.

9. Perform a backup.

4.1.2 Summary of CS 1000 Configuration for MDC Users

Create new employee configuration on the CS 1000 or verify existing employee configuration to ensure these are compatible with the MDC Solution. The employee terminal number and directory number configured on the CS 1000 are used as the user information provisioned on the MDC Administration GUI. The user information on MDC must match exactly what is provisioned on the CS 1000. This is facilitated by loading information for the user from the CS 1000 when provisioning users at the MDC Administration GUI.

Verify you have the information needed prior to starting to configure the CS 1000 for the MDC Solution. The required information is listed in Section 4.2 *Required Information for CS 1000 Configuration for MDC*.

Refer to Section 4.8 *User and Role Terminal Number, Directory Number and CLS Configuration* if further details are required on the procedures including identifying the basic commands to add, query and change users on the CS 1000. Unfortunately, there can potentially be a great deal of variation in the CS 1000 configuration, depending on many factors, including the setup of customer groups, type of phones, feature sets in use, etc. It is assumed that the CS 1000 administrator has already configured these aspects of the CS 1000.

There are two deployments for users:

- Dual TN
- Shared TN

The important information to provision the employee is:

- Terminal number (TN)
- Key number (especially relevant for user in a shared TN deployment)
- Directory number (DN)
- Phone type or terminal type
- Name of employee

MDC supports the use of Multiple Call Ringing (MCR) or Single Call Ringing (SCR) however all phone, users and roles (if used) must be the same call type.

- Note: the use of Multiple Call Ringing (MCR) can be advantageous over Single Call Ringing (SCR). When multiple phones are assigned with the same phone number (for example, a desk phone and a mobile handset), MCR will permit the other phones to ring when a new call is received even when one of the phone is busy with an earlier call. In this instance, MCR must be enabled on the user's phones AND the MDC handsets. Note: MCR is incompatible with certain call features such as call waiting.
- If roles are used with MDC, this is another situation where multiple phones can be assigned the same phone number. This can occur when 2 or more users to select the same role. MCR should be used if multiple people will have the same role (even when the overlapping time period is short) so when one phone is in use the other phones will still ring.

Use the following checklist which highlights the key CS 1000 provisioning compatibilities for MDC users:

- All employee must have the same call type configured, either all MCR or all SCR.
 - All WLAN mobile phones and roles must have the same call type feature configured as well.
- If the user has an analogue or digital phone there is no key 0 entry. In this instance, ensure that the CLS line is defined as either MCRA if the user is MCR or MCNR, SCN if the user is SCR.
- Permit multiple-loop dial number on CS 1000. This will enable the CS 1000 to allow for the same phone number to be used across different loops.
- For all users it is recommended to assign names via CPND (Calling Party Name Display), if permitted, to make re-assignment of assets easier to validate. Users can have their employee name.
 - The following substrings cannot be part of the user's name:
 - SCH<one or more digits> e.g. SCH8
 - NPR705
 - OVL429
- For all users and phones, CLID is recommended. It's helpful to enable the CNDA (Calling Name Display Access) feature if permitted. This might mean changing CNDD (Calling Name Display Denied) temporarily to test MDC functionality.
- If the user has features on any key other than Key 0 (the primary DN), these feature do not get transferred to the WLAN handsets when the user checks out their phone using MDC.
- The mapping of certain phone types within the CS 1000 may be different. For example, the 6140/6120 phone type is shown as 2210.
- The configuration for any existing users of CS 1000 who will be using MDC should be reviewed to ensure that it is compatible with MDC.

Remember to do a backup after entering all configuration changes.

Tip: Retain the user information provisioned on CS 1000 for provisioning users on MDC Administration GUI. Refer to Section 3.3.1.3 *Preparing for Bulk Loading Users and Phones into MDC* if bulk loading will be used.

4.1.3 Summary of CS 1000 Configuration for MDC Phone/Assets

Create new WLAN handset configuration on the CS 1000 or verify existing WLAN handset configuration to ensure these are compatible with the MDC Solution. The WLAN phone configuration on the CS 1000 is used as the asset phone information provisioned on the MDC Administration GUI. The asset information on MDC must match exactly what is provisioned on the CS 1000. This is facilitated by being able to load information for the asset from the CS 1000 when adding new assets at the MDC Administration GUI.

Verify you have the information needed prior to starting to configure the CS 1000 for the MDC Solution. The required information is listed in Section 4.2 *Required Information for CS 1000 Configuration for MDC*.

Refer to Section 4.9 *CS 1000 WLAN Phone Configuration* and Section 4.8 *User and Role Terminal Number, Directory Number and CLS Configuration* if further details are required on the procedures including identifying the basic commands to add, query and change users on the CS 1000. Unfortunately, there can potentially be a great deal of variation in the CS 1000 configuration, depending on many factors, including the setup of customer groups, type of phones, feature sets in use, etc. It is assumed that a CS 1000 administrator has already configured these aspects of the CS 1000.

MDC supports the use of Multiple Call Ringing (MCR) or Single Call Ringing (SCR) however all phone, users and roles (if used) must be the same call type.

- The use of Multiple Call Ringing (MCR) can be advantageous over Single Call Ringing (SCR). When multiple phones are assigned with the same phone number (for example, a desk phone and a mobile handset), MCR will permit the other phones to ring when a new call is received even when one of the phone is busy with an earlier call. In this instance, MCR must be enabled on the user's phones AND the MDC handsets. Note: MCR is incompatible with certain call features such as call waiting.
- If roles are used with MDC, this is another situation where multiple phones can be assigned the same phone number. This can occur when 2 or more users to select the same role. MCR should be used if multiple people will have the same role (even when the overlapping time period is short) so when one phone is in use the other phones will still ring.

Use the following checklist which highlights the key CS 1000 provisioning compatibilities for MDC WLAN phones:

- All WLAN phones should have default DNs. These DNs must be unique in the system and cannot be used with any other existing TN on the CS 1000.
- All WLAN mobile phones must have the same call type configured, either all MCR or all SCR.
 - All employees and roles must have the same call type feature configured as well.
- Permit multiple-loop dial number on CS 1000. This will enable the CS 1000 to allow for the same phone number to be used across different loops.
- Use CLID for all users and phones. It is helpful to enable the CNDA (Calling Name Display Access) feature if permitted. This might mean changing CNDD (Calling Name Display Denied) temporarily to testing MDC functionality.
- Default names on the WLAN phones are not needed. Existing names assigned to WLAN phones as CPND will be overwritten when the phones are checked out to users.
 - If default names are used, the following substrings cannot be part of the name:
 - SCH<one of more digits> e.g. SCH8
 - NPR705
 - OVL429
- If the optional role feature will be used on MDC with both personal phone number and role phone number assignment to the WLAN phone, ensure that all WLAN phones have two lines provisioned i.e. key 0 and key 1. The configuration of the second line must conform to all requirements identified earlier.
 - In situations where only some MDC Stations will be provisioned with checkout of both role and personal phone numbers, for easier deployment it is recommended that all WLAN phones have two lines provisioned unless the dual line WLAN phones can be easily distinguished.
- Any feature which requires a user specific number to be dialed should not be configured on the WLAN handsets used in the MDC solution. For example, the Dialed Intercom Group (DIG) feature should not be used on the WLAN handsets.
- Test all WLAN phones once they have been provisioned to ensure that they are operational. It is recommended to use the WLAN handset to make a phone call, and to receive a call by ringing the WLAN handset.
- Each WLAN phone must physically have a unique barcode label attached to the back of the handset or inside the battery compartment if using a protective silicon cover (e.g. zCover) on the WLAN handset. See NN49010-501 Nortel Healthcare Solutions MDC Deployment Guide for information on label generation.
- The mapping of certain phone types within the CS 1000 may be different. For example, the 6140/6120 phone type is shown as 2210.

- The configuration for an existing WLAN phone on the C1S 000 which will be using MDC should be reviewed to ensure that it is compatible with MDC.

Remember to do a backup after entering all configuration changes.

Tip: Retain the WLAN phone information provisioned on CS 1000 for provisioning phone (assets) on MDC Administration GUI. Refer to Section 3.3.1.3 *Preparing for Bulk Loading Users and Phones into MDC* if bulk loading will be used.

Location tracking is an optional feature of MDC. If location tracking is being used for WLAN phones, the following is required:

- A site survey must be done for 802.11 A/B/G for location tracking. RFid tags use 802.11 B/G whereas the phones use 802.11 A.
- There must be sufficient licenses on Ekahau Position Engines to track the location-enabled WLAN phones. See the Nortel Healthcare Solution Asset Tracking Management Documentation Suite or EPE Product documentation for more information.
- Each WLAN phone which will be location tracked must be physically configured on the handset to enable location tracking by configuring the following:
 - RTLS Enable
 - Transmit interval should be set to 1 minute.
 - Enter the IP address of the EPE as location service.
 - Set ELP (Ekahau Location Port) to default 8552.

The important information for provisioning the WLAN phones for MDC is:

- Terminal number (TN)
- Directory number (DN)
- Phone type or terminal type
- Optional (for location tracking only): IP address of EPE
- Optional (for location tracking only): ELP

The figure below summarizes the overview of the CS 1000 configuration for the MDC Solution.

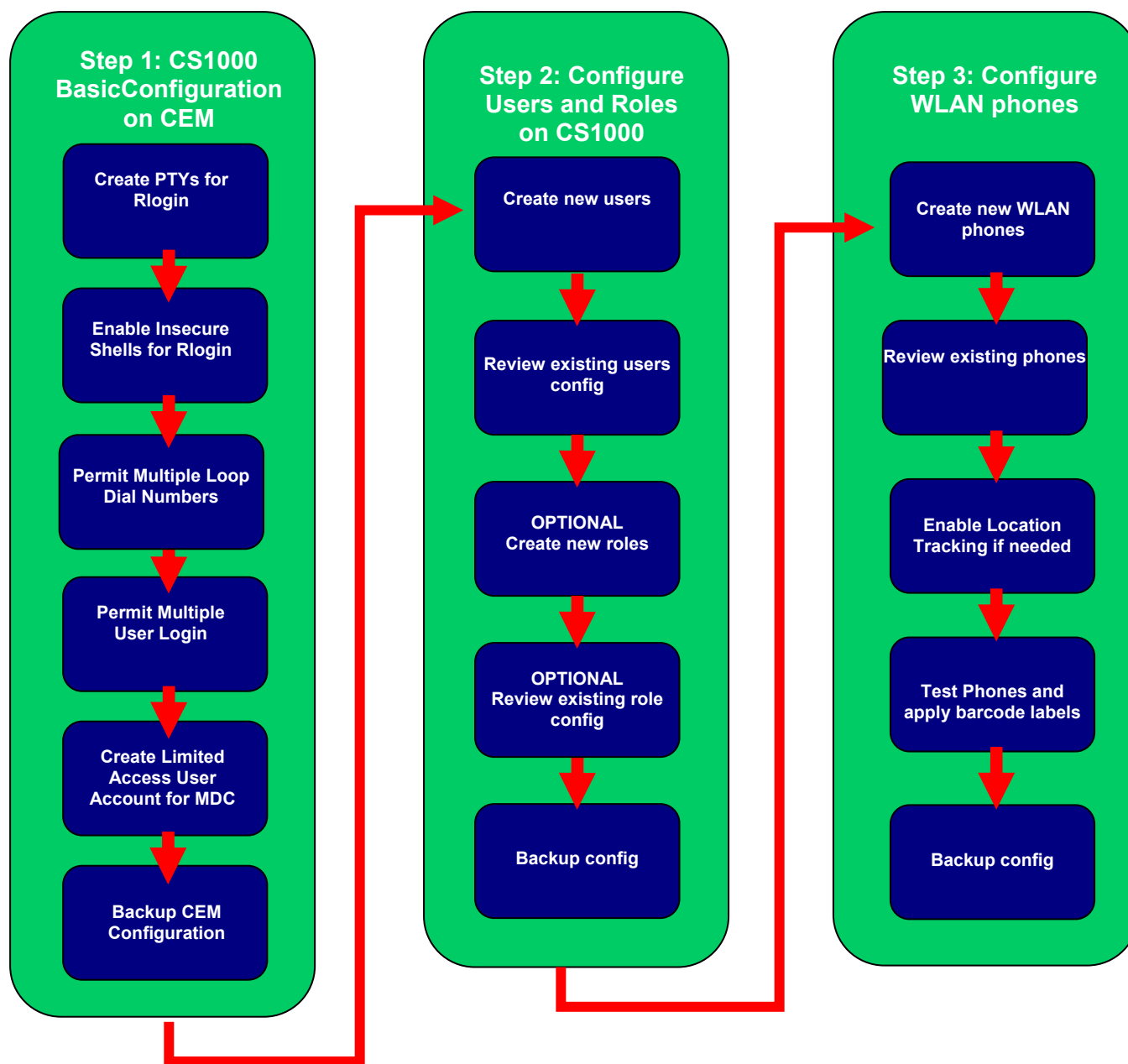


Figure 1: Overview of CS 1000 Configuration

4.2 Required Information for CS 1000 Configuration for MDC

The following information is needed prior to starting to configure the CS 1000 for the MDC Solution:

Table 27: Required Information for CS1000 Configuration for MDC

	Required Information for CS1000 Configuration for MDC	
1	IP address of the CS 1000 Element Manager	
2	CS 1000 Element Manager Login information	
3	CS 1000 UCM Login information (for CS 1000 Release 6.0 or later releases)	
4	User ID and password for the CS 1000 administration user name. For most tasks, admin-level1 privileges will be sufficient. However, admin2-level privileges are required for the creation of a limited access user account for the MDC application.	
5	IP address of the CS 1000 Call Server (for virtual terminal sessions)	
6	Customer Group for phones and users	
7	Failed Log in Threshold used by customer for password basic parameters	
8	Port Lockout duration used by customer for password basic parameters	
9	Inactivity Timeout for password basic parameters (minimum of 20 minutes or longer recommended)	
10	Parameters for Limited Access Password account (in CS 1000 Release 5 and 5.5): <ul style="list-style-type: none"> ○ User Name ○ Password 	
11	For Limited Access Password Account Role (in CS 1000 Release 6 or later) <ul style="list-style-type: none"> ○ Role Name ○ Role Description 	

12	Parameters for Limited Access Password Account (in CS 1000 Release 6.0 or later) <ul style="list-style-type: none"> ○ User ID ○ Full Name ○ Temporary Password ○ Permanent Password 	
13	IP address for MDC Server	
14	Root password for MDC Server	
15	Non-root username and password for MDC Server (due to OS security hardening, root account cannot be used to log into MDC Server)	
15	Multiple Call Arrangement with Ring (MCR) or Single Call Ringing (SCR)	This call type must be the same for all phones, users and roles used with MDC.
16	To provision each user for dual TN (Terminal Number) deployment: <ul style="list-style-type: none"> ○ Terminal number (TN) ○ Directory number (DN) ○ Phone type or terminal type ○ Name of employee (first & last) ○ Description ○ QoS Zone 	See table below to capture dual TN user information
17	To provision users for shared TN (Terminal Number) deployment: <ul style="list-style-type: none"> ○ Shared Terminal number (TN) ○ Phone type or terminal type ○ Description ○ QoS Zone ○ Number of Key Extension Modules (KEM) To provision each users in this shared TN (Terminal Number) deployment: <ul style="list-style-type: none"> ○ Key number ○ Directory number (DN) ○ Name of employee (first & last) 	See table below to capture shared TN user information

18	<p>To provision each mobile WLAN phones for MDC:</p> <ul style="list-style-type: none"> ○ Terminal number (TN) ○ Directory number (DN) – key 0 ○ [optional] Directory number (DN) – key 1 ○ Description 	<p>See table below to capture phone information.</p> <p>Key 1 is only required if the optional MDC role feature will be used in the mode where both the user's personal phone number and the role phone number will be assigned to the handset during checkout</p>
19	<p>[Optional] To enable location tracking on the WLAN phone (only if the phone will be location tracked):</p> <ul style="list-style-type: none"> ○ IP address of EPE (Ekahau Positioning Engine) ○ ELP (Ekahau Location Port) number 	<p>This information is only needed if optional MDC location tracking feature will be used.</p>
20	<p>[Optional] To provision each role for dual TN (Terminal Number) deployment:</p> <ul style="list-style-type: none"> ○ Terminal number (TN) ○ Directory number (DN) ○ Phone type or terminal type ○ Display Name of role ○ Description ○ QoS Zone 	<p>Only required if the optional MDC role feature will be used.</p> <p>See table below to capture dual TN role information</p>
21	<p>[Optional] To provision roles for shared TN (Terminal Number) deployment:</p> <ul style="list-style-type: none"> ○ Shared Terminal number (TN) ○ Phone type or terminal type ○ Description ○ QoS Zone ○ Number of Key Extension Modules (KEM) <p>To provision each role in this shared TN (Terminal Number) deployment:</p> <ul style="list-style-type: none"> ○ Key number ○ Directory number (DN) ○ Display name of role 	<p>Only required if the optional MDC role feature will be used.</p> <p>See table below to capture shared TN role information</p>

Table 28: Required CS 1000 Information for Dual TN User Information

Terminal	Directory	Phone type or	Name of	Description	QoS Zone
----------	-----------	---------------	---------	-------------	----------

number (TN)	number (DN)	terminal type	employee (first & last)		

Table 29: Required CS 1000 Information for Shared TN user information

Shared Terminal number (TN)	Phone type or terminal type	Description	QoS Zone	Key number	Directory number (DN)	Name of employee (first & last)

Table 30: Required CS 1000 Information for WLAN Handset

Terminal number (TN)	Directory number (DN) – key 0	[Optional] Directory Number (DN)-key 1	Description

Table 31: Required CS 1000 Information for Dual TN Role Information [Optional]

Terminal number (TN)	Directory number (DN)	Phone type or terminal type	Name of Role	Description	QoS Zone

Table 32: Required CS 1000 Information for Shared TN Role information [Optional]

Shared Terminal number (TN)	Phone type or terminal type	Description	QoS Zone	Key number	Directory number (DN)	Name of Role

4.3 CS 1000 Base Configuration

4.3.1 Enable Insecure Shells for Rlogin

1. Log in to CS 1000 Element Manager.
2. From the CS 1000 Element Manager, select **Security** from the left-hand navigation menu. The security submenu will be expanded.
3. Select **Login Options** from the security submenu on the left-hand navigation menu.
4. Select **Shell Login** from the Login Option submenu on the left-hand navigation menu.
5. The Shell Login screen will appear.

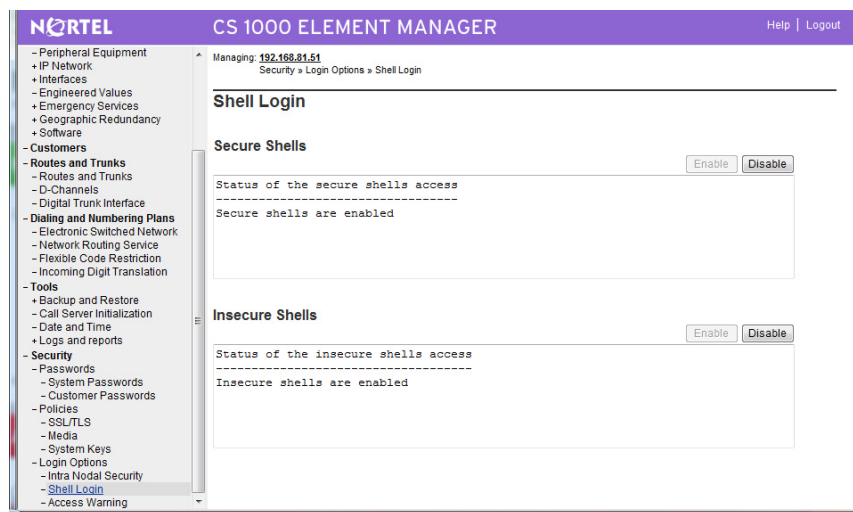


Figure 2: CS 1000 Element Manager Security Submenu

6. Under Insecure Shells, if insecure shells are not already enabled, select **Enable**.
7. The status of insecure shells access should change to enabled in the text message box under Insecure Shells.

4.3.2 Create LAPW Password Account on CS 1000 Rel 5.x for MDC

Tip: It is recommended that creating a password account on CS 1000 for MDC be done as the last configuration on CS 1000 Element Manager, as this action will automatically trigger a request to back up CEM data. Such a backup will save all the configuration changes made to the CEM so far.

1. From the CS 1000 Element Manager, select **Security** from the left-hand navigation menu. The security submenu will be expanded.

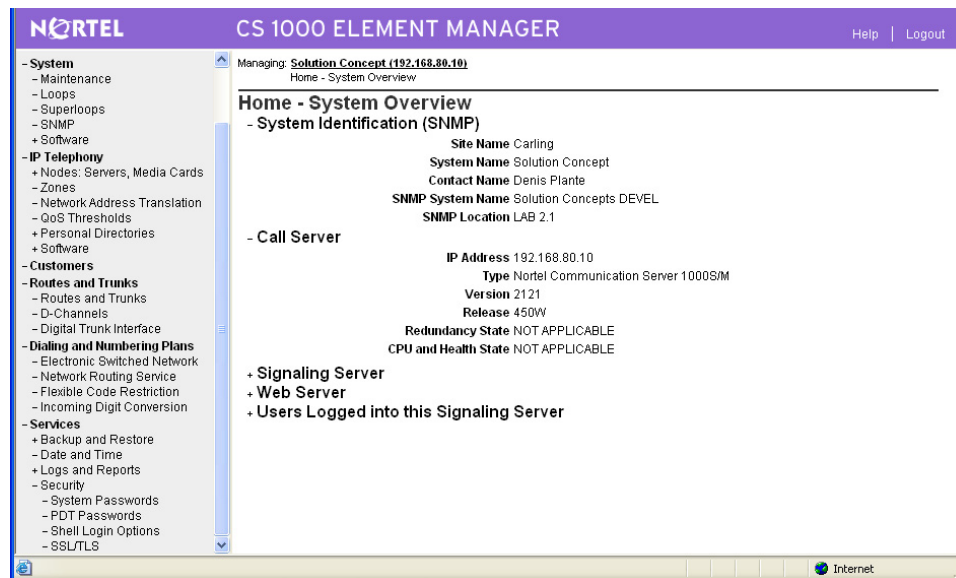


Figure 3: CS 1000 Element Manager Security Submenu

2. Select **System Passwords (Password then System Password in Release 5.5)** from the security submenu of the left-hand navigation menu. The Password Accounts List screen will appear.

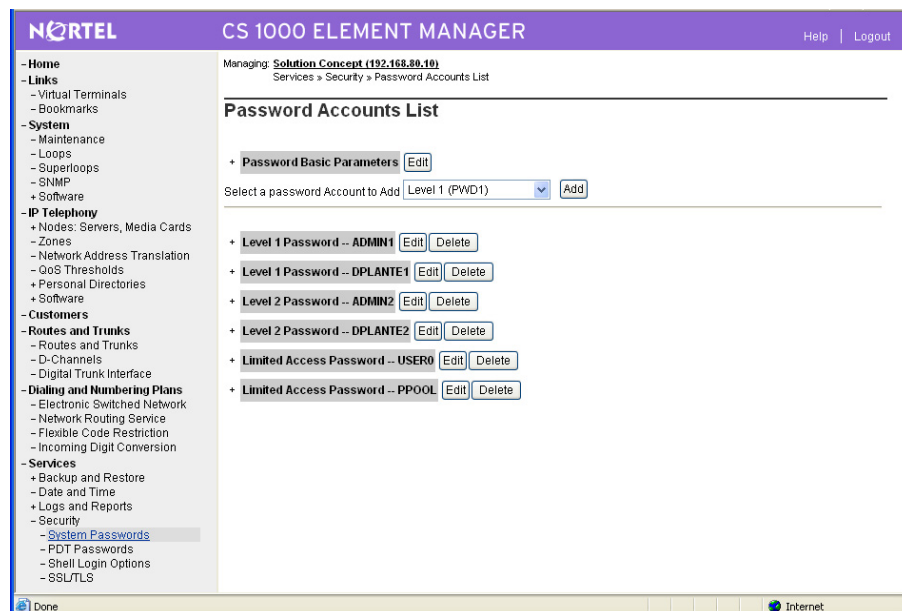


Figure 4: CS 1000 Element Manager System Passwords

3. To assist with integration testing, it is recommended that you temporarily change some of the password parameters if permitted by the customer. It is also recommended that you record the current Password Basic parameters settings.

Temporarily, the failed login threshold should be increased and port lockout duration should be shortened until connectivity between MDC and CS 1000 is tested and established.

- a. Click **Password Basic Parameters**. The details of the Password Basic Parameters will be displayed.

- b. Record the values displayed so the customer settings can be returned after connectivity between MDC and CS 1000 has been reliably established.

NORTEL CS 1000 ELEMENT MANAGER

Managing: **Solution Concept (192.168.88.10)**
Services > Security > Password Accounts List

Password Accounts List

Password Basic Parameters [Edit]

Password Complexity Check: OFF
 Inactivity Timeout: 20
 Failed Log In Threshold: 7
 Port Lockout Time in Minute After Failed Log In: 3
 Audit Trail for Password Usage: NO
 Initialize to Reset Locked-out Ports: NO

Select a password Account to Add: **Limited Access (LAPW)** [Add]

- Level 1 Password -- ADMIN1** [Edit] [Delete]
- Level 1 Password -- DPLANTE1** [Edit] [Delete]
- Level 2 Password -- ADMIN2** [Edit] [Delete]
- Level 2 Password -- DPLANTE2** [Edit] [Delete]
- Limited Access Password -- USER0** [Edit] [Delete]
- Limited Access Password -- PPOOL** [Edit] [Delete]
- Limited Access Password -- MTPC** [Edit] [Delete]

Figure 5: CEM Password Basic Parameters

- c. Click **Edit**.

NORTEL CS 1000 ELEMENT MANAGER

Managing: **Solution Concept (192.168.88.10)**
Services > Security > Password Accounts List > Password Basic Parameters

Password Basic Parameters

Input Description	Input Value
Force Password Change (FPC):	<input type="checkbox"/>
Failed Log In Threshold (FLTH):	7 Range: 1 to 7
Failed Log In Threshold Alarm (FLTA):	<input type="checkbox"/>
Port Lockout Time After Failed Log In (LOCK):	3 Range: 0 to 270 Minutes
Reset Locked-out Ports (INIT):	<input type="checkbox"/>
Password Complexity Check (PSWD_COMP):	OFF
Audit Trail for Password Usage (AUDT):	<input type="checkbox"/>
Last Log In Identification (LLID):	<input type="checkbox"/>
Inactivity Timeout (LOUT):	20 Range: 1 to 20 Minutes
Level 2 Password (LV2_PWD):	<input type="text"/>

[Submit] [Refresh] [Cancel]

(2) Microsoft Office Word

Figure 6: CEM Edit Password Basic Parameters

- d. Enter the temporary value for **Failed Log in Threshold (FLTH)**.
- e. Enter the temporary value for **Port Lockout Time After Failed In (LOCK)**.
- f. Change the value for **Inactivity Timeout (LOUT)** to a value of 10 minutes or longer.
- g. Click the **Submit** button to save the changes.

4. To create a password account, select **Limited Password (LAPW)** from the pulldown menu as the type of account to create.

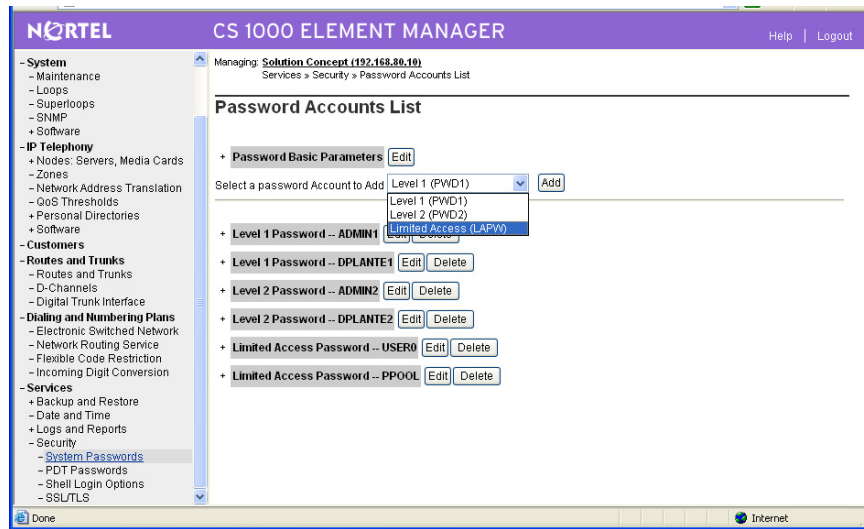


Figure 7: CEM: Select Limited Password Account

5. Click the **Add** button.
6. A Limited Access Password Account screen will appear:

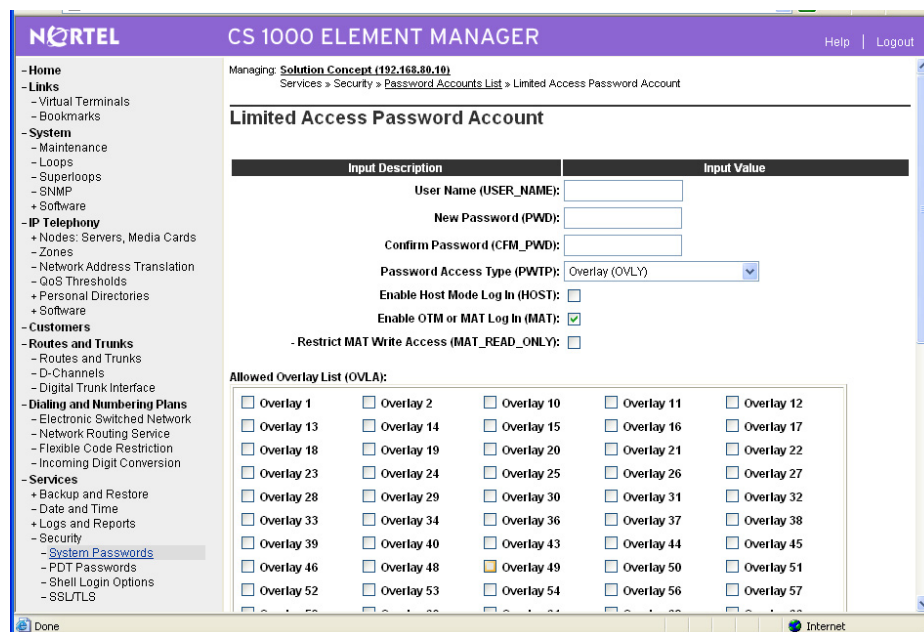


Figure 8: CEM Limited Access Password Account

7. Enter the following required information. You will need to scroll down to see the bottom fields:
 - a. **User Name (USER_NAME):** enter the user name of the administration account for the MDC application.
 - b. **New Password (PWD):** enter the password for the administration account for the MDC application.
 - c. **Confirm Password (CFM_PWD):** re-enter the password for the administration account for the MDC application.



- d. Select **Overlay (OVLY)** from the pulldown menu for Password Access Type (PWTP).
- e. Check the **Enable Host Mode Log In (HOST)** box.
- f. Check the **Enable OTM or MAT Log In (MAT)** box.
- g. Under Allowed Overlay List (OVLA), check the following boxes:
 - **Overlay 10,**
 - **Overlay 11,**
 - **Overlay 20,**
 - **Overlay 22,**
 - **Overlay 32,**
 - **Overlay 95**
- h. Under Accessible Customer (CUST), check the customer group which applies. If applicable, enter the Tenant. Tenant cannot be an empty field; if necessary enter a space.
- i. Under Overlay Options (OPT), check the **Allow Configuration Prompts** box.
- j. Click the **Submit** button.

NORTEL CS 1000 ELEMENT MANAGER Help | Logout

- Home
- Links
 - Virtual Terminals
 - Bookmarks
- System
 - + Alarms
 - Maintenance
 - + Core Equipment
 - Peripheral Equipment
 - + IP Network
 - + Interfaces
 - Engineered Values
 - + Emergency Services
 - + Geographic Redundancy
 - + Software
- Customers
- Routes and Trunks
 - Routes and Trunks
 - D-Channels
 - Digital Trunk Interface
- Dialing and Numbering Plans
 - Electronic Switched Network
 - Network Routing Service
 - Flexible Code Restriction
 - Incoming Digit Translation
- Tools
 - + Backup and Restore
 - Call Server Initialization
 - Date and Time
 - + Logs and reports
- Security
 - Passwords
 - **System Passwords**
 - Customer Passwords
 - Policies
 - SSL/TLS
 - Media
 - System Keys
 - Login Options
 - Intra Nodal Security
 - Shell Login
 - Access Warning

Overlay 13 Overlay 14 Overlay 15 Overlay 16 Overlay 17
 Overlay 18 Overlay 19 ☒ Overlay 20 Overlay 21 ☒ Overlay 22
 Overlay 23 Overlay 24 Overlay 25 Overlay 26 Overlay 27
 Overlay 28 Overlay 29 Overlay 30 Overlay 31 Overlay 32
 Overlay 33 Overlay 34 Overlay 36 Overlay 37 Overlay 38
 Overlay 39 Overlay 40 Overlay 43 Overlay 44 Overlay 45
 Overlay 46 Overlay 48 Overlay 49 Overlay 50 Overlay 51
 Overlay 52 Overlay 53 Overlay 54 Overlay 56 Overlay 57
 Overlay 58 Overlay 60 Overlay 61 Overlay 62 Overlay 66
 Overlay 73 Overlay 74 Overlay 75 Overlay 77 Overlay 79
 Overlay 80 Overlay 81 Overlay 82 Overlay 83 Overlay 84
 Overlay 86 Overlay 87 Overlay 88 Overlay 90 Overlay 92
 Overlay 93 Overlay 94 ☒ Overlay 95 Overlay 96 Overlay 97
 Overlay 117 Overlay 135 Overlay 137 Overlay 143

Select All De-Select

Accessible Customer (CUST):

☒ All Customers
☐ Customer 01
☐ Customer 02

Overlay Options (OPT):

☐ Allow Access to Resident Debug ☒ Allow Configuration Prompts
☒ Allow Force Command ☒ Allow Line Load Control
☒ Allow Loss Plan Customization ☒ Allow Monitor Command
☒ Allow Printing of Speed Call Lists ☐ Print Only

Submit Refresh Cancel

NORTEL CS 1000 ELEMENT MANAGER Help | Logout

Managing: [Solution Concept \(192.168.88.10\)](#)
 Services > Security > [Password Accounts List](#) > Limited Access Password Account

Limited Access Password Account

Input Description	Input Value
User Name (USER_NAME):	mtpc
New Password (PWD):	*****
Confirm Password (CFM_PWD):	*****
Password Access Type (PWTP):	Overlay (OVLY)
Enable Host Mode Log In (HOST):	<input checked="" type="checkbox"/>
Enable OTM or MAT Log In (MAT):	<input checked="" type="checkbox"/>
- Restrict MAT Write Access (MAT_READ_ONLY):	<input type="checkbox"/>

Allowed Overlay List (OVL):

Overlay 1 Overlay 2 ☒ Overlay 10 ☒ Overlay 11 Overlay 12
 Overlay 13 Overlay 14 Overlay 15 Overlay 16 Overlay 17
 Overlay 18 Overlay 19 ☒ Overlay 20 Overlay 21 ☒ Overlay 22
 Overlay 23 Overlay 24 Overlay 25 Overlay 26 Overlay 27
 Overlay 28 Overlay 29 Overlay 30 Overlay 31 Overlay 32
 Overlay 33 Overlay 34 Overlay 36 Overlay 37 Overlay 38
 Overlay 39 Overlay 40 Overlay 43 Overlay 44 Overlay 45
 Overlay 46 Overlay 48 Overlay 49 Overlay 50 Overlay 51
 Overlay 52 Overlay 53 Overlay 54 Overlay 56 Overlay 57

Figure 9: CEM Limited Access Password Account for MDC (Part 1)

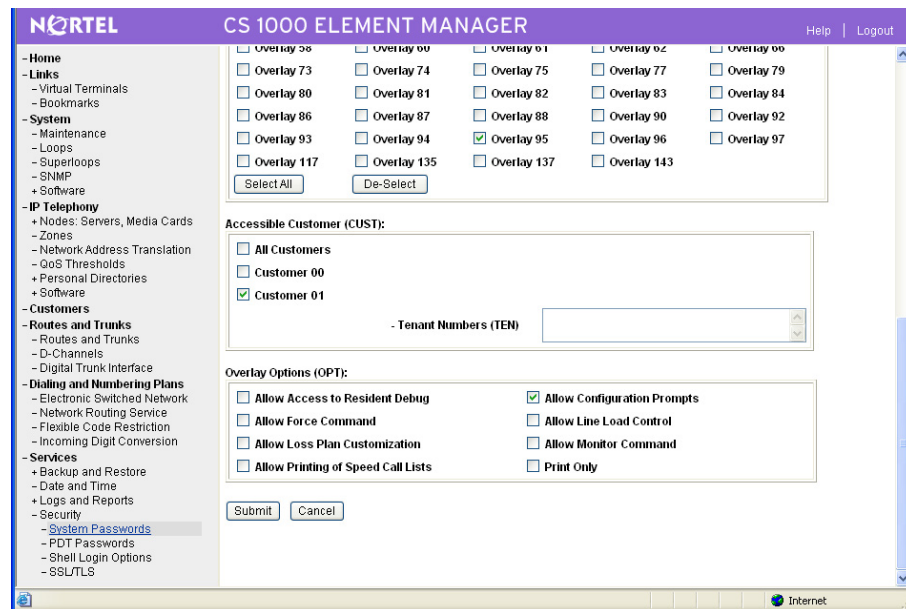


Figure 10: CEM Limited Access Password Account for MDC (Part 2)

8. A successful changes message will be displayed. You will be prompted to perform a backup. Click the **OK** button.

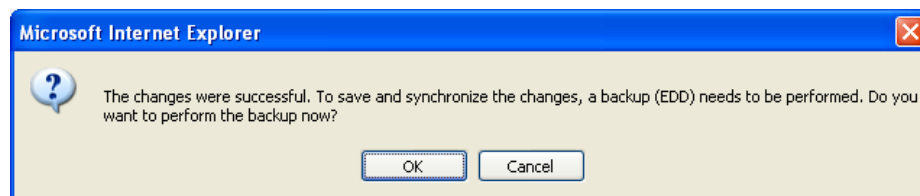


Figure 11: CEM Confirm Changes Message and Request Backup

9. A Call Server Backup screen will appear. Backup will be selected as the Action. Click the **Submit** button to initiate the backup.

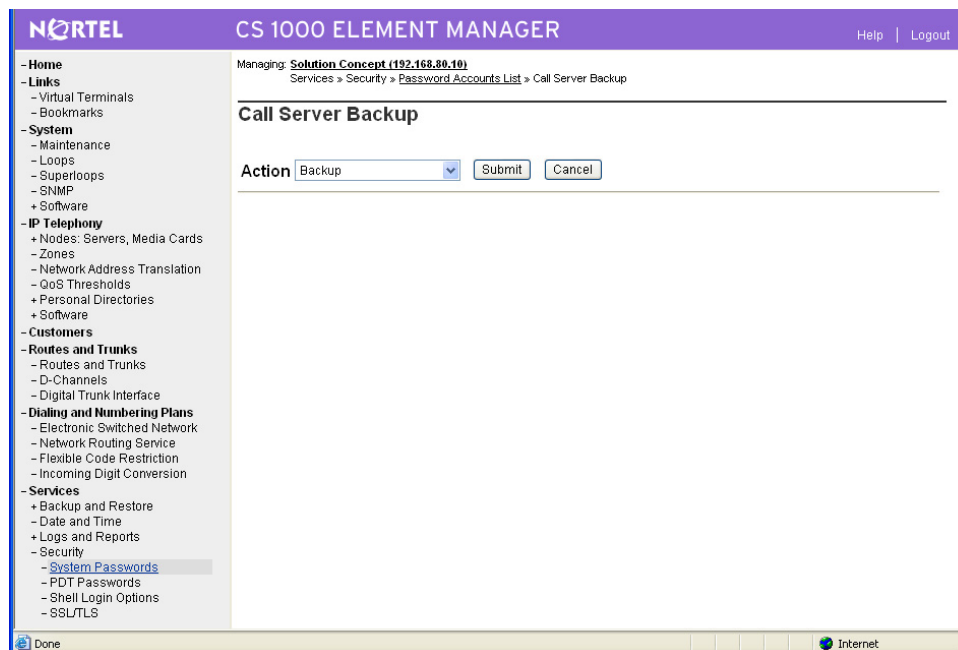


Figure 12: CEM Call Server Backup

10. A backup in progress message will appear. Wait for confirmation of successful backup.

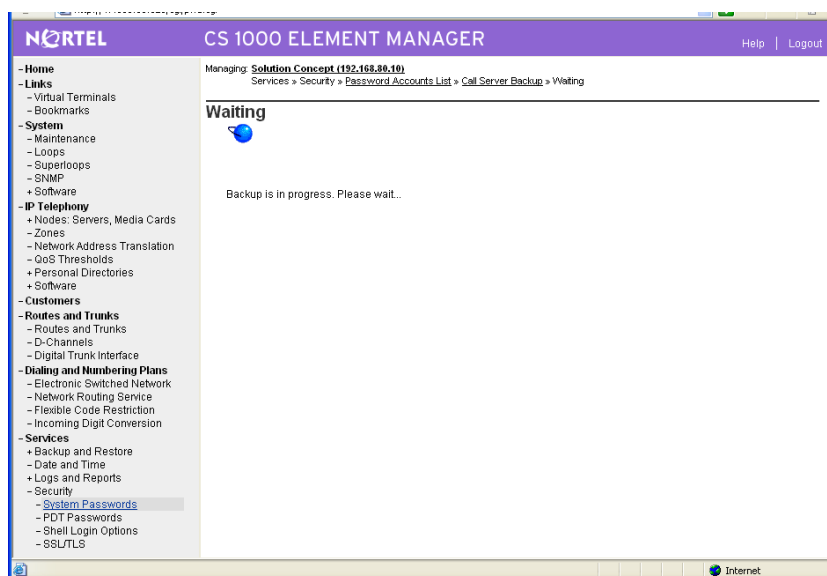


Figure 13: CEM Call Server Backup in Progress

11. A confirmation of successful backup will appear. You will need to scroll down to see the message.

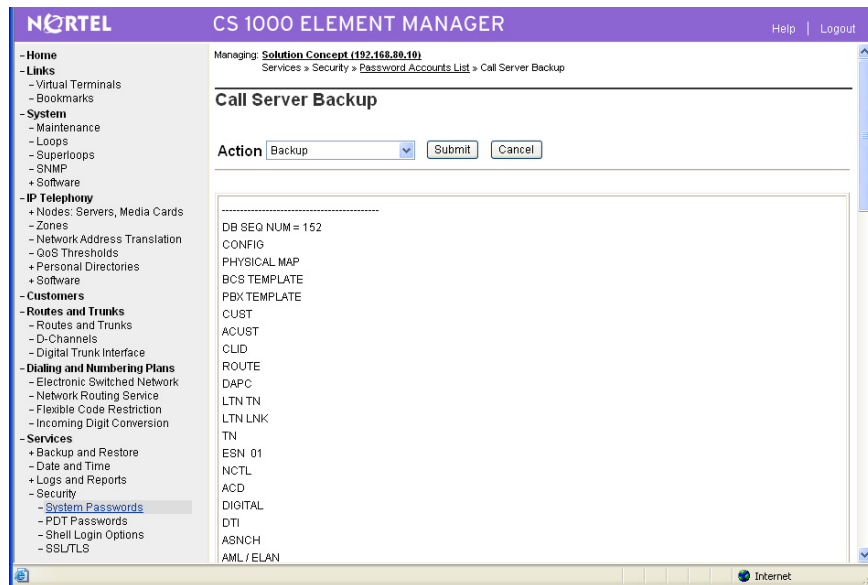


Figure 14: CEM Call Server Backup Successful (Part 1)

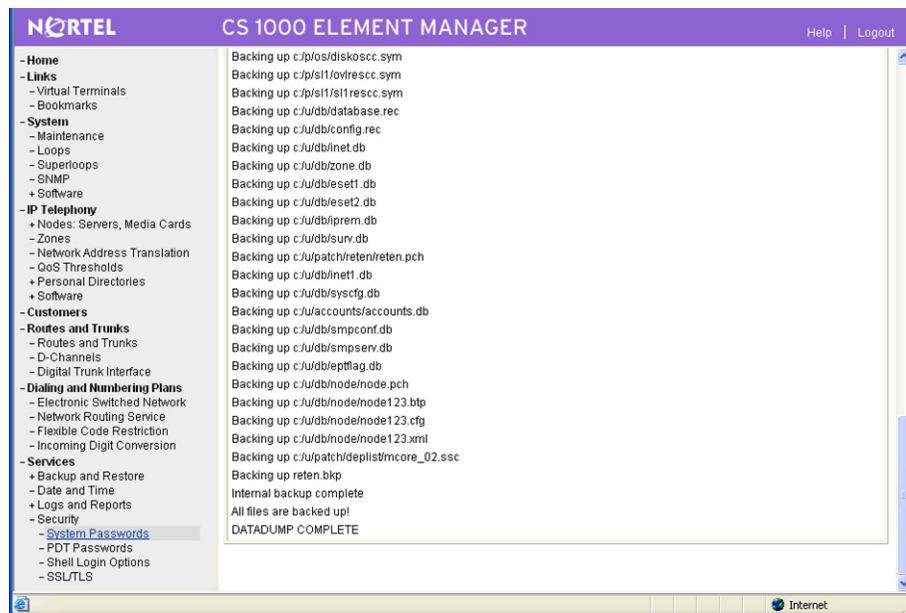
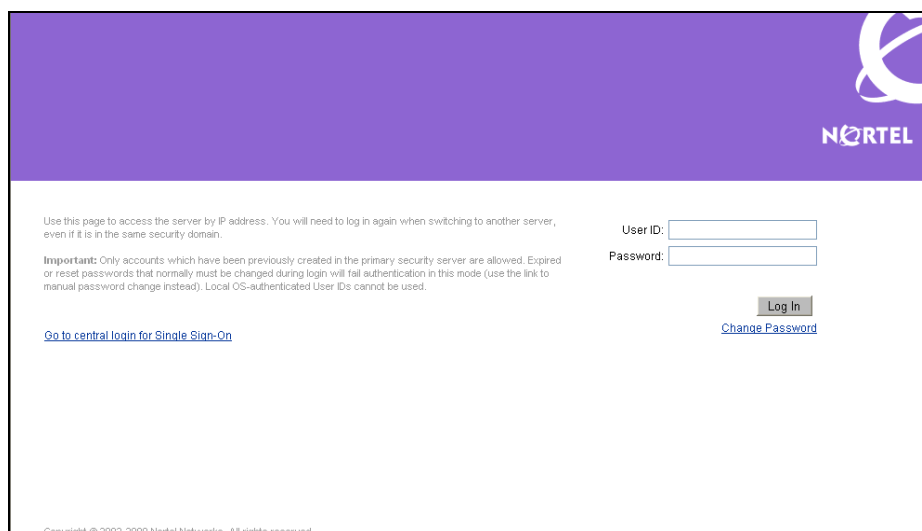


Figure 15: CEM Call Server Backup Successful (Part 2)

4.3.3 Create Limited Access Password (LAPW) Role on CS 1000 Rel 6 for MDC

CS 1000 Release 6.0 supports the concepts of user roles which permit group-based access to central management features, and are mapped to permissions on individual network elements. For elements of type CS 1000, there is a role template corresponding to a blank set of permissions for a CS 1000 administrative account "with specified OAM privileges". This UCM template corresponds to the previous CS 1000 system-level OAM account with "limited access to overlays password" (LAPW).

1. Log in to Unified Communication Manager.



Use this page to access the server by IP address. You will need to log in again when switching to another server, even if it is in the same security domain.

Important: Only accounts which have been previously created in the primary security server are allowed. Expired or reset passwords that normally must be changed during login will fail authentication in this mode (use the link to manual password change instead). Local OS-authenticated User IDs cannot be used.

User ID:

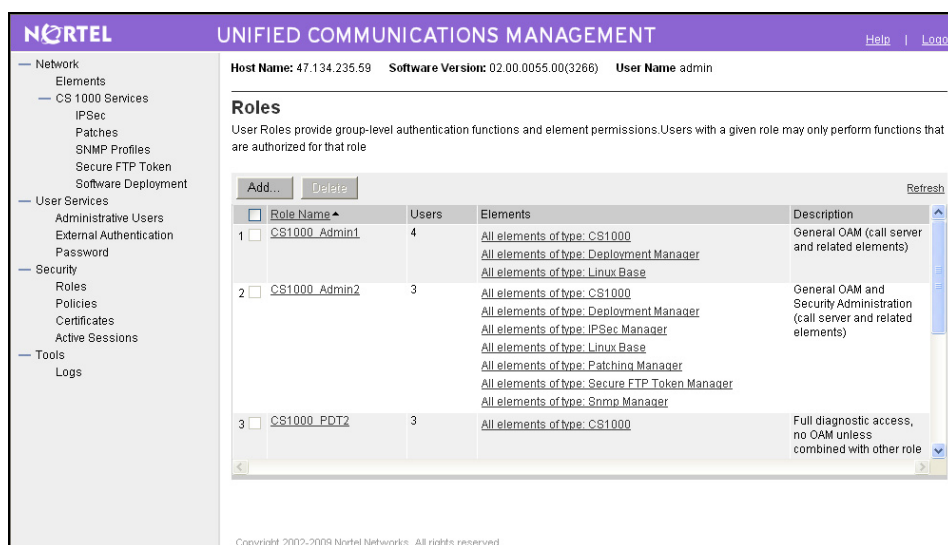
Password:

[Go to central login for Single Sign-On](#) [Change Password](#)

Copyright © 2002-2009 Nortel Networks. All rights reserved.

Figure 16: UCM Log In Screen

2. Within Unified Communications Management, select **Security** from the left-hand navigation menu. The security submenu will be expanded.
3. Select **Roles**.



NORTEL UNIFIED COMMUNICATIONS MANAGEMENT [Help](#) | [Logout](#)

Host Name: 47.134.235.59 Software Version: 02.00.0055.00(3266) User Name admin

Roles

User Roles provide group-level authentication functions and element permissions. Users with a given role may only perform functions that are authorized for that role.

<input type="checkbox"/>	Role Name	Users	Elements	Description
1 <input type="checkbox"/>	CS1000_Admin1	4	All elements of type: CS1000 All elements of type: Deployment Manager All elements of type: Linux Base	General OAM (call server and related elements)
2 <input type="checkbox"/>	CS1000_Admin2	3	All elements of type: CS1000 All elements of type: Deployment Manager All elements of type: IPsec Manager All elements of type: Linux Base All elements of type: Patching Manager All elements of type: Secure FTP Token Manager All elements of type: Snmp Manager	General OAM and Security Administration (call server and related elements)
3 <input type="checkbox"/>	CS1000_PDT2	3	All elements of type: CS1000	Full diagnostic access, no OAM unless combined with other role

Copyright 2002-2009 Nortel Networks. All rights reserved.

Figure 17: UCM Role Screen

4. Click **Add** button
5. Enter the following information:
 - a. **Role Name**
 - b. **Role Description**

NORTEL UNIFIED COMMUNICATIONS MANAGEMENT [Help](#) | [Logout](#)

Host Name: 47.134.235.59 Software Version: 02.00.0055.00(3266) User Name admin

Add New Role

Step 1: Identify the new role.
Enter a role name and description

Role Name: (1-26) (Allowed characters are a-z, A-Z, 0-9, - and _)

Role Description: 1-x characters

Note: The new role must be saved before you map element permissions.

[Save and Continue](#) [Cancel](#)

Copyright 2002-2009 Nortel Networks. All rights reserved.

Figure 18: UCM Add New Role Screen

6. Click **Save and Continue**
7. Click **Add Mapping** under Element/Service Permissions
8. Select **CS1000** from the pulldown menu and click **Next** button.

NORTEL UNIFIED COMMUNICATIONS MANAGEMENT [Help](#) | [Logout](#)

Host Name: 47.134.235.59 Software Version: 02.00.0055.00(3266) User Name admin

Select Element and/or Network Service to Map to Role (CS1000_LimitedAccess_MDC)

Element and/or Network Service Name:

[Next](#) [Cancel](#)

Copyright 2002-2009 Nortel Networks. All rights reserved.

Figure 19: UCM Select Element and/or Network Service for Role

9. Select the permissions for this role by:
 - a. Confirm **Default CS1000 Permissions** has been selected from the pulldown menu for Template for permission set.
 - b. Select **Specified OAM privileges, specified customers** under Administration (PWD)
 - c. Confirm **None** under Diagnostics (PDT)
 - d. Under Specified OAM Privileges (LAPW)

- i. Select **Telephony Manager (MAT)** under Account Options
- ii. Specify the Customer Group number under the Customer and Tenant section.
- iii. Select the following under Specified Services and Features:
 - (10) Analog Sets Administration
 - (11) Digital Sets Administration
 - (20) Print Routine 1
 - (22) Print Routine 3
 - (32) Network and Peripheral Equipment Diagnostics
 - (95) Calling Party Name Display

NORTEL UNIFIED COMMUNICATIONS MANAGEMENT

Host Name: 47.134.235.59 Software Version: 02.00.0055.00(3266) User Name admin

Permission Mapping (All elements of type: CS1000 for CS1000_LimitedAccess_MDC)

Users with this role will be authorized to perform all management functions associated with the selected permissions on the indicated element.

Template for permission set: Default CS1000 Permissions

Role: CS1000_LimitedAccess_MDC

Administration (PWD)

- ☐ None
- ☒ Specified OAM privileges, specified customers
Only those features explicitly enabled in the corresponding section below.
- ☐ General OAM, all customers
- ☐ General OAM, all customers, plus Security Administration

Diagnostic (PDT)

Diagnostic permissions may be combined with any of the above Admin permission sets.

- ☒ None
- ☐ PDT1
Limited diagnostic shell.

Save Cancel

Copyright 2002-2009 Nortel Networks. All rights reserved.

Figure 20: UCM Permission Mapping for Role

10. Click **Save**.

NORTEL UNIFIED COMMUNICATIONS MANAGEMENT

Host Name: 47.134.235.59 Software Version: 02.00.0055.00(3266) User Name admin

Role Details (CS1000_LimitedAccess_MDC)

Identification

Role Name: CS1000_LimitedAccess_MDC

Description: Limited Access for MDC 1-xx characters

Save Cancel

Element/Service Permissions Assigned Users

Add Mapping... Delete Mapping Copy All From...

Name	Permissions
1 <input type="checkbox"/> All elements of type: CS1000	All Customers, Config Prompts, CSO Am User, Enable Host Mode, Key Code Change, Telephony Manager (MAT), Root Access, (10) Analog Sets Administration, (95) Call Party Name Display, Specific Customer-Tenant access, (11) Digital Sets Administration, (32) Network and Peripheral Equipment Diagnostic, (20) Print Routine 1, (22) Print Routine 3

Save Cancel

Copyright 2002-2009 Nortel Networks. All rights reserved.

Figure 21: UCM Role Details

11. Click **User Services**

The screenshot shows the Nortel Unified Communications Management (UCM) interface. The top navigation bar includes the Nortel logo, the title "UNIFIED COMMUNICATIONS MANAGEMENT", and links for "Help" and "Logout". Below the navigation bar, the page displays the "User Services" section. The left sidebar contains a tree view with categories: Network, CS 1000 Services, User Services, Security, and Tools. The "User Services" category is expanded, showing sub-items: Administrative Users, External Authentication, and Password. The main content area for "User Services" includes a description: "Manage the people who utilize network services as subscribers or as administrators." and three links: "Administrative Users", "External Authentication", and "Password". The "Administrative Users" link is highlighted. The page footer contains the copyright notice: "Copyright 2002-2009 Nortel Networks. All rights reserved."

Figure 22: UCM User Services

12. Click **Administrative Users**

The screenshot shows the Nortel Unified Communications Management (UCM) interface, specifically the "Administrative Users" page. The top navigation bar includes the Nortel logo, the title "UNIFIED COMMUNICATIONS MANAGEMENT", and links for "Help" and "Logout". Below the navigation bar, the page displays the "Administrative Users" section. The left sidebar contains a tree view with categories: Network, CS 1000 Services, User Services, Security, and Tools. The "User Services" category is expanded, showing sub-items: Administrative Users, External Authentication, and Password. The "Administrative Users" sub-item is selected. The main content area for "Administrative Users" includes a description: "Select a User ID to manage the properties and roles of local and externally authenticated users. Refer to password and authentication server policies for additional configuration requirements. Refer to [Active Sessions](#) for currently logged in users and session management functions." and a table of administrative users. The table has columns: User ID, Name, Roles, Type, and Account Status. The table lists four users: admin, admin2, mdclogin1, and mdclogin2. The "Add..." button is highlighted. The page footer contains the copyright notice: "Copyright 2002-2009 Nortel Networks. All rights reserved."

User ID	Name	Roles	Type	Account Status
1 admin	Default security administrator	NetworkAdministrator Patcher	Local	Enabled
2 admin2	admin two	CS1000_Admin1 CS1000_Admin2 CS1000_PDT2	Local	Enabled
3 mdclogin1	mdclogin1	CS1000_Admin1 CS1000_Admin2 CS1000_PDT2	Local	Enabled
4 mdclogin2	mdclogin2	CS1000_Admin1 CS1000_Admin2 CS1000_PDT2	Local	Enabled

Figure 23: UCM Administrative Users

13. Click **Add** to create a user ID for MDC

NORTEL UNIFIED COMMUNICATIONS MANAGEMENT Help | Logout

Host Name: 47.134.235.59 Software Version: 02.00.0055.00(3266) User Name admin

Add New Administrative User

Step 1: Identify the new user.
Enter the user's full name and select an authentication type and User ID. Locally authenticated users also required a temporary password.

User ID: (1-31) (Allowed characters are a-z, A-Z, 0-9, - and _)

Authentication Type: ☒ Local ☐ External

Full Name:

Temporary password:

Re-enter password:

The user will be required to change this password when logging in.

Allowed characters in the password are: a-zA-Z0-9()!@#\$%^&*~?\. The length of your password must be at least 4 characters.

Note: The new user must be saved before you may assign roles.

Save and Continue Cancel

Copyright 2002-2009 Nortel Networks. All rights reserved.

Figure 24: UCM Add New Administrative User

14. Enter the new administrative user information:

- User ID**
- Authentication Type:** Select **Local**
- Full Name**
- Temporary Password:** Give the password. Confirm the password in the **Re-enter password** field.

15. Click **Save and Continue** button.

16. Assign the role for the MDC Userid by selecting the limited access role created earlier.

17. Click **Finish** button.

NORTEL UNIFIED COMMUNICATIONS MANAGEMENT Help | Logout

Host Name: 47.134.235.59 Software Version: 02.00.0055.00(3266) User Name admin

Add New Administrative User

Step 2: Assign Role(s)
Selected roles authorize the user for associated features and element permissions.

Roles

Role	Description
<input checked="" type="checkbox"/> CS1000_LimitedAccess_MDC	All elements of type: Secure FTP Token Manager All elements of type: Snmp Manager Limited Access for MDC
<input type="checkbox"/> CS1000_PDT2	All elements of type: CS1000 Full diagnostic access, no OAM unless combined with other role(s).
<input type="checkbox"/> MemberRegistrar	All elements of type: IPsec Manager Member Registrar Role

Finish Cancel

Copyright 2002-2009 Nortel Networks. All rights reserved.

Figure 25: UCM

18. The newly created Userid will be listed in the table of Administrative Users.
19. **Logout** of UCM
20. **Log** back into UCM with the newly created MDC Userid and its temporary password. You will be automatically prompted to change the temporary password. Change the password by entering the new permanent password and confirming it.
21. **Logout** of UCM

This completes the creation of LAPW account for MDC.

4.3.4 Backup of CS 1000 Element Manager

This section is optional if you have already done a backup when creating a limited access password in the previous section.

1. On any screen of CS 1000 Element Manager, click **Backup and Restore** under Tools in the left-hand navigation menu.
2. The Backup and Restore submenu will be displayed. Click **Call Server** in the Backup and Restore submenu.
3. The Call Server Backup and Restore screen will be displayed. Click **Backup** in the main task working area.
4. The Call Server Backup screen will be displayed. Select **Backup** as Action from the pulldown menu.
5. Click **Submit** button to initiate backup.

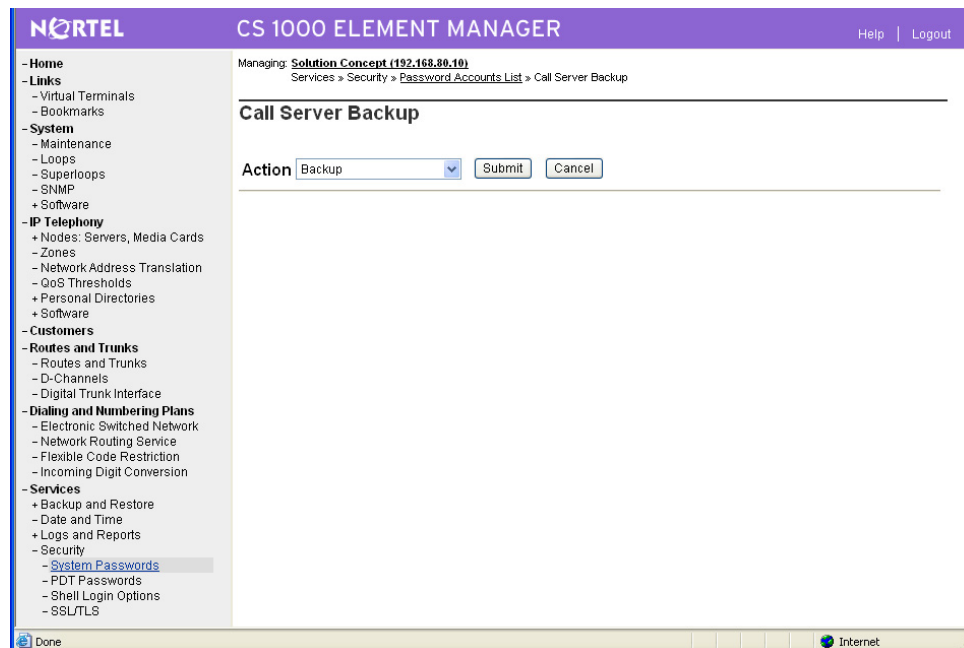


Figure 26: CEM Call Server Backup

6. A backup in progress message will appear. Wait for confirmation of successful backup.

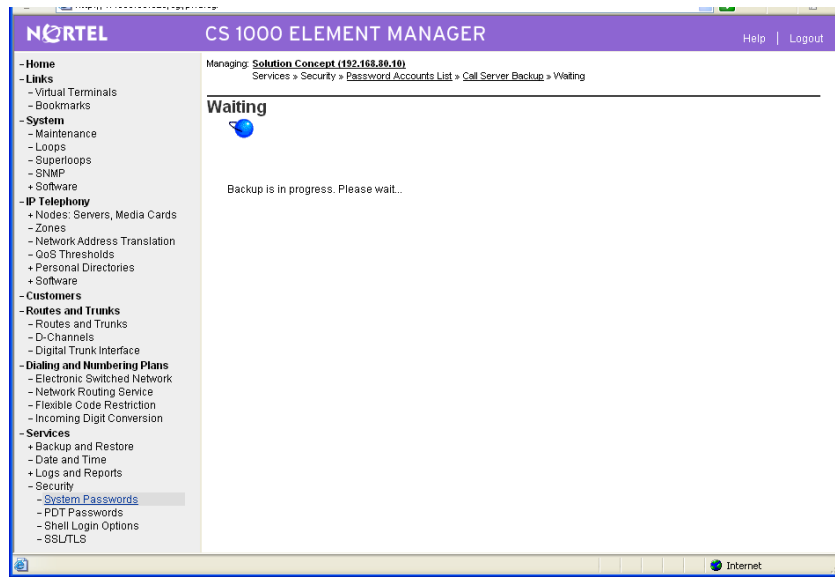


Figure 27: CEM Call Server Backup in Progress

7. A confirmation of successful backup will appear. You will need to scroll down to see the message.

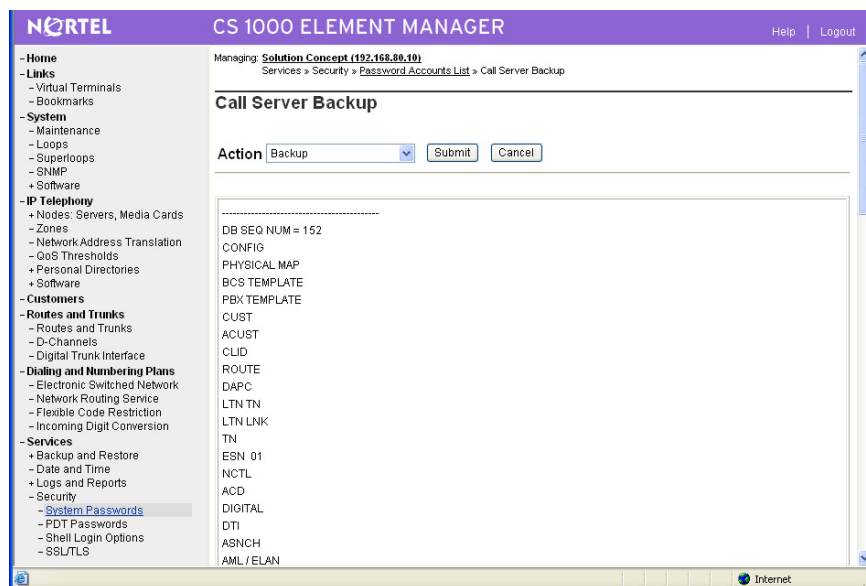


Figure 28: CEM Call Server Backup Successful (Part 1)

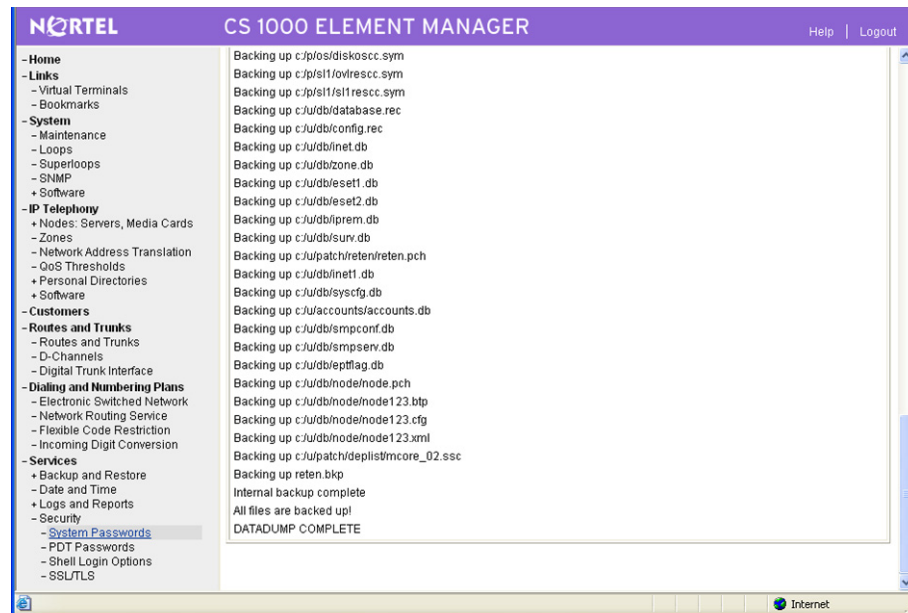


Figure 29: CEM Call Server Backup Successful (Part 2)

4.3.5 Logout of CS 1000 Element Manager

1. On any screen of CS 1000 Element Manager, click **Logout** on the right side of the CS 1000 Element Manager title bar.

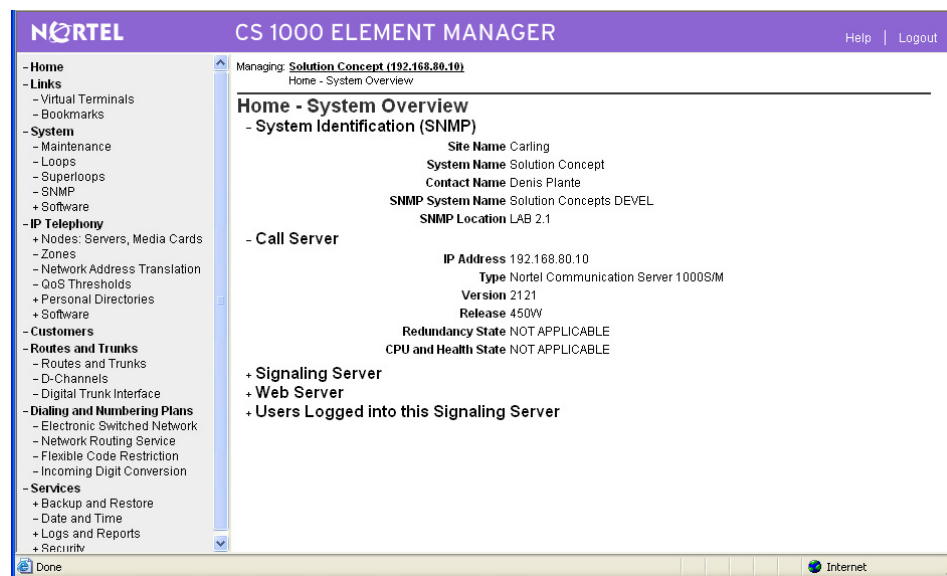


Figure 30: CS 1000 Element Manager Home – System Overview Screen

2. The CS 1000 Element Manager (CEM) login page will appear. You are now logged out of CEM.

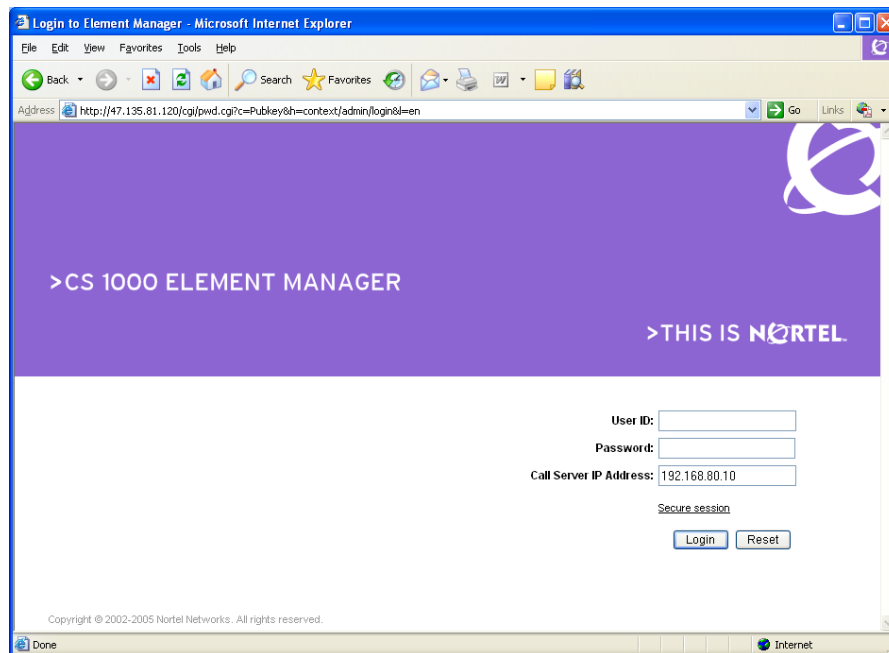


Figure 31: CS 1000 Element Manager Logon Screen

4.4 Testing connectivity between CS 1000 and MDC

4.4.1 Connectivity

Ping the CS 1000 Call server IP address from the MDC Server to test for network connectivity.

```
root@asrd127-9:~#  
[root@asrd127-9 ~]# ping 192.168.80.10  
PING 192.168.80.10 (192.168.80.10) 56(84) bytes of data.  
64 bytes from 192.168.80.10: icmp_seq=1 ttl=255 time=1.00 ms  
64 bytes from 192.168.80.10: icmp_seq=2 ttl=255 time=1.00 ms  
64 bytes from 192.168.80.10: icmp_seq=3 ttl=255 time=1.00 ms  
64 bytes from 192.168.80.10: icmp_seq=4 ttl=255 time=1.00 ms  
64 bytes from 192.168.80.10: icmp_seq=5 ttl=255 time=1.00 ms  
64 bytes from 192.168.80.10: icmp_seq=6 ttl=255 time=0.985 ms  
  
--- 192.168.80.10 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 4998ms  
rtt min/avg/max/mdev = 0.985/1.001/1.007/0.019 ms  
[root@asrd127-9 ~]#
```

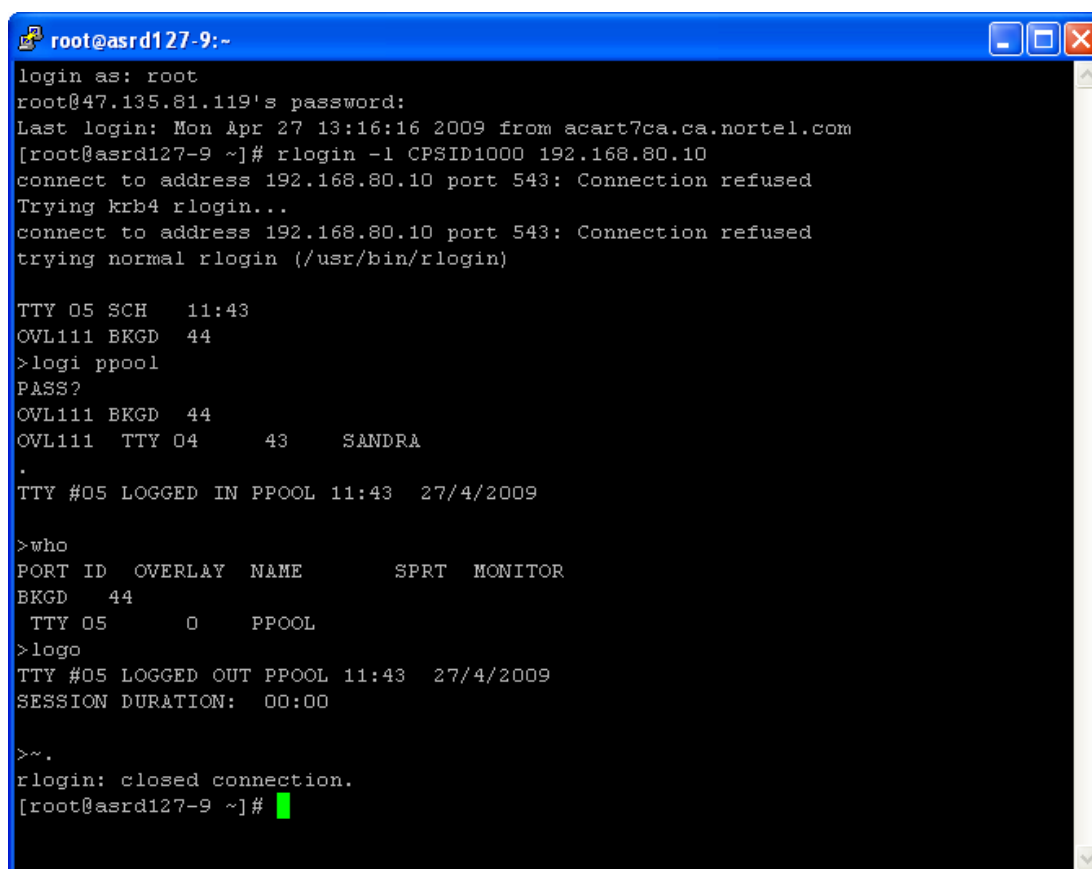
Figure 32: Ping from MDC Server to CS 1000 ELAN

4.4.2 Rlogin from MDC Server to CS 1000

Use rlogin to test whether insecure shell and limited access password have been set up correctly.

1. From a terminal emulator program (like putty), open a connection to the MDC Server IP address.

2. Log in to the MDC Server with **root** userid and password. Due to OS hardening, you may need to initially log in with a non-root userid and password and then change privileges to root (su – root),
3. Type **#rlogin -l CPSID1000 <ELAN IP address of call server >** to establish remote login session to CS 1000 Call Server via ELAN.
4. Press the **<Enter>** key a few times to get a prompt.
5. Type **logi <limited access user name for MDC application>** to log in with the administration account for the MDC application.
6. At the PASS? Prompt, type **<limited access password for MDC application>** to access the administration account for the MDC application.
7. You should see a confirmation message about being logged in.
8. Type **who** which will display the limited access user name for MDC to confirm connectivity.
9. Type **logo** to log out of the CS 1000.
10. Type **~.** to disconnect from rlogin.
11. Type **exit** to terminate the putty session or use the appropriate command to end the terminal emulation program.



```
root@asrd127-9:~  
login as: root  
root@47.135.81.119's password:  
Last login: Mon Apr 27 13:16:16 2009 from acart7ca.ca.nortel.com  
[root@asrd127-9 ~]# rlogin -l CPSID1000 192.168.80.10  
connect to address 192.168.80.10 port 543: Connection refused  
Trying krb4 rlogin...  
connect to address 192.168.80.10 port 543: Connection refused  
trying normal rlogin (/usr/bin/rlogin)  
  
TTY O5 SCH 11:43  
OVL111 BKGD 44  
>logi ppool  
PASS?  
OVL111 BKGD 44  
OVL111 TTY O4 43 SANDRA  
.  
TTY #05 LOGGED IN PPOOL 11:43 27/4/2009  
  
>who  
PORT ID OVERLAY NAME SPRT MONITOR  
BKGD 44  
TTY O5 0 PPOOL  
>logo  
TTY #05 LOGGED OUT PPOOL 11:43 27/4/2009  
SESSION DURATION: 00:00  
  
>~.  
rlogin: closed connection.  
[root@asrd127-9 ~]#
```

Figure 33: Rlogin from MDC to CS 1000

4.5 Options for CLI Connection to CS 1000 for Users and Phone Configuration

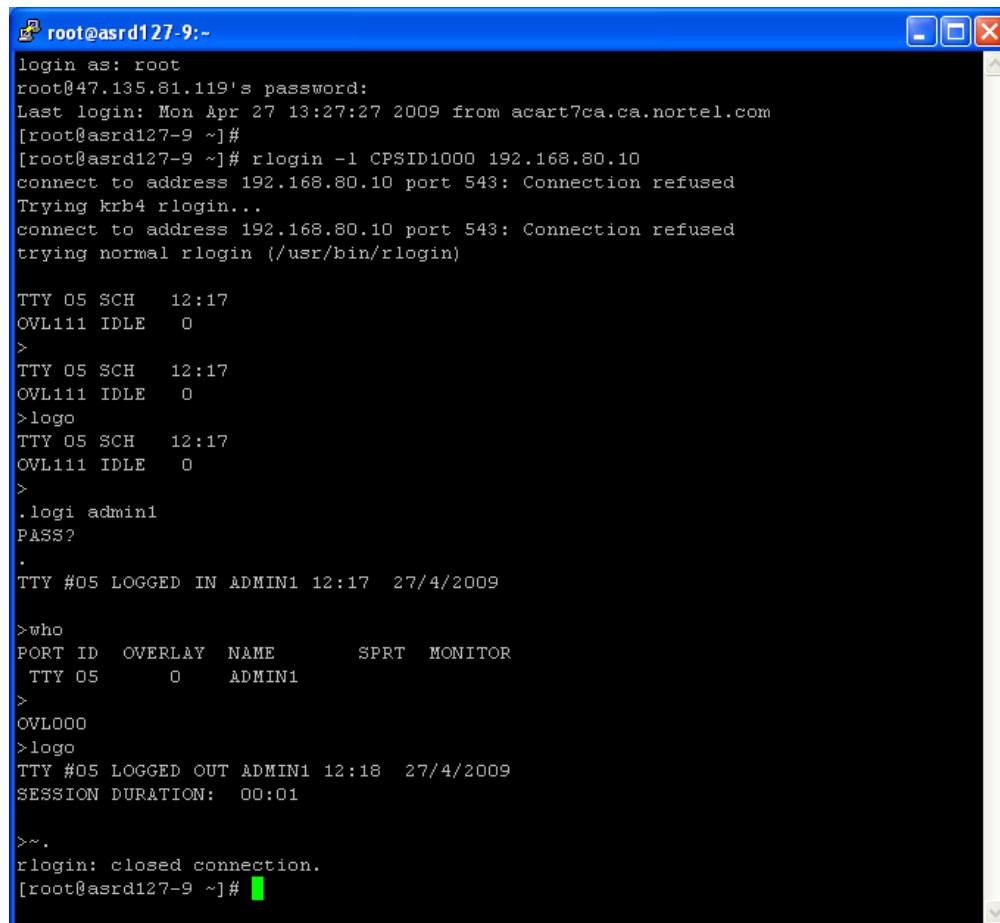
You will need access to the admin1 or higher-level userid for CS 1000 to be able administer users and phones. This document places emphasis on character-based interfaces, as these will work on multiple releases of CS 1000.

Here are four possible ways to connect to CS 1000 to do provisioning:

- rlogin via terminal emulator from the MDC Server to CS 1000 via ELAN
- Virtual Terminal from the CEM UI
- Phone GUI from CEM if CS 1000 is running on a Linux server. This graphical user interface is not available with earlier releases of CS 1000. This interface is not described in this document. Refer to CS 1000 documentation for further details on using this interface.
- Telephony Manager. This graphical user interface may not always be available. This interface is not described in this document. Refer to CS 1000 documentation for further details on using this interface.

4.5.1 Terminal Emulation/Putty Session from MDC Server via ELAN

1. From a terminal emulator program (like putty), open a connection to the MDC Server IP address.
2. Log in to the MDC Server with **root** userid and password. Due to OS hardening, you may need to initially log in with a non-root userid and password and then change privileges to root (su – root),
3. Type **#rlogin -l CPSID1000 <ELAN IP address of call server >** to establish a remote login session to the CS 1000 Call Server via ELAN.
4. Press the **<Enter>** key a few times to get a prompt.
5. Type **logi <admin1 or admin2 level userid>** to log in to CS 1000 with administration privileges.
6. At the PASS? Prompt, type **< password for administrative userid>**
7. You should see a confirmation message about being logged in.
8. Execute the configuration changes needed for users or phones using overlays. This is described in more detail in Section 4.8 *User and Role Terminal Number, Directory Number and CLS Configuration* and Section 4.9 *CS 1000 WLAN Phone Configuration*.
9. Perform a backup to save the configuration changes. This is described in more detail in Section 4.3.4 *Backup of CS 1000 Element Manager*.
10. Type **logo** to log out of the CS 1000 when you have finished.
11. Type **~.** to disconnect from rlogin.
12. Type **exit** to terminate the putty session or use the appropriate command to end the terminal emulation program.

A screenshot of a terminal window titled 'root@asrd127-9:~'. The terminal shows a login sequence where the user 'root' logs in from IP 47.135.81.119. The user then attempts to connect to 192.168.80.10 using 'rlogin -l CPSID1000'. The connection is refused, and the user tries 'krb4 rlogin' and 'normal rlogin', both of which are also refused. The terminal then displays system status for TTY 05, showing it is in 'SCH' state at 12:17. The user enters 'logo' and then '.logi admin1'. The system logs the user in as 'ADMIN1' at 12:17 on 27/4/2009. The user then enters 'who', and the system displays a table with columns 'PORT ID', 'OVERLAY', 'NAME', 'SPRT', and 'MONITOR'. The table shows 'TTY 05', '0', 'ADMIN1', and empty values for 'SPRT' and 'MONITOR'. The user enters 'OVLOOO' and 'logo' again. The system logs the user out as 'ADMIN1' at 12:18 on 27/4/2009, with a session duration of 00:01. The user enters '~.' and the terminal displays 'rlogin: closed connection.' and '[root@asrd127-9 ~]#'.

```
root@asrd127-9:~  
login as: root  
root@47.135.81.119's password:  
Last login: Mon Apr 27 13:27:27 2009 from acart7ca.ca.nortel.com  
[root@asrd127-9 ~]#  
[root@asrd127-9 ~]# rlogin -l CPSID1000 192.168.80.10  
connect to address 192.168.80.10 port 543: Connection refused  
Trying krb4 rlogin...  
connect to address 192.168.80.10 port 543: Connection refused  
trying normal rlogin (/usr/bin/rlogin)  
  
TTY 05 SCH 12:17  
OVL111 IDLE 0  
>  
TTY 05 SCH 12:17  
OVL111 IDLE 0  
>logo  
TTY 05 SCH 12:17  
OVL111 IDLE 0  
>  
.logi admin1  
PASS?  
.  
TTY #05 LOGGED IN ADMIN1 12:17 27/4/2009  
  
>who  
PORT ID OVERLAY NAME SPRT MONITOR  
TTY 05 0 ADMIN1  
>  
OVL000  
>logo  
TTY #05 LOGGED OUT ADMIN1 12:18 27/4/2009  
SESSION DURATION: 00:01  
  
>~.  
rlogin: closed connection.  
[root@asrd127-9 ~]#
```

Figure 34: Rlogin from MDC to CS 1000

4.5.2 Virtual Terminal from CEM GUI

Note: For CS 1000 Release 5.5 (and possibly 5.0), the Java Runtime Environment (JRE) version 1.5 must be installed for the Virtual Terminal Emulator to run properly. JRE version 1.5 is also known as JRE 5.0. It can be accessed from the Sun Microsystems website for the Sun Developer Network (<http://java.sun.com/products/archive/>).

1. From CS 1000 Element Manager, click **Links** in the left navigation menu to display the Link submenu.
2. Click **Virtual Terminal** from the Link submenu on the left navigation menu. The Virtual Terminal Sessions screen will appear.
3. To test the virtual terminal session connection, select the newly created (or any) virtual terminal session to the CS 1000 by clicking the name from the list of virtual terminals displayed.
4. A separate terminal emulation window will appear. It may take some time for the Java applet to initialize, especially the first time it runs. You may also have a security warning prompting for confirmation to run the application: "The application's digital signature cannot be verified. Do you want to run the application?" If so, click the **Run** button.

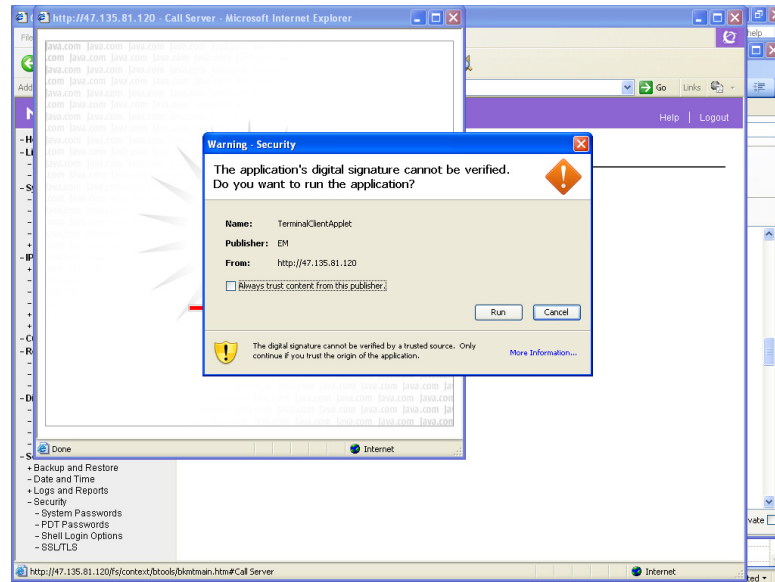


Figure 35: Virtual Terminal Security Warning

- When the Java applet initializes, the terminal emulation window will appear:

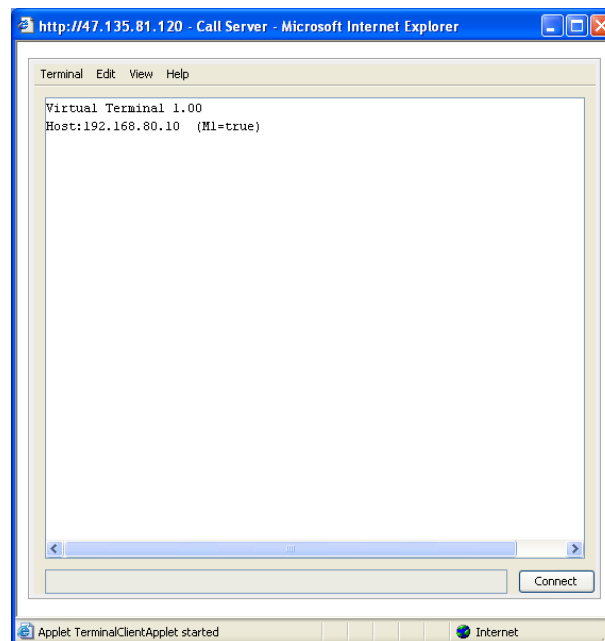


Figure 36: Virtual Terminal Screen

- Click the **Connect** button in the lower right corner of the virtual terminal emulator. Or you can select **Connect** from the **Terminal** menu in the menu bar at the top of the window.
- If successful, a message "Remote Login Server is connected" will appear in the terminal emulator screen.

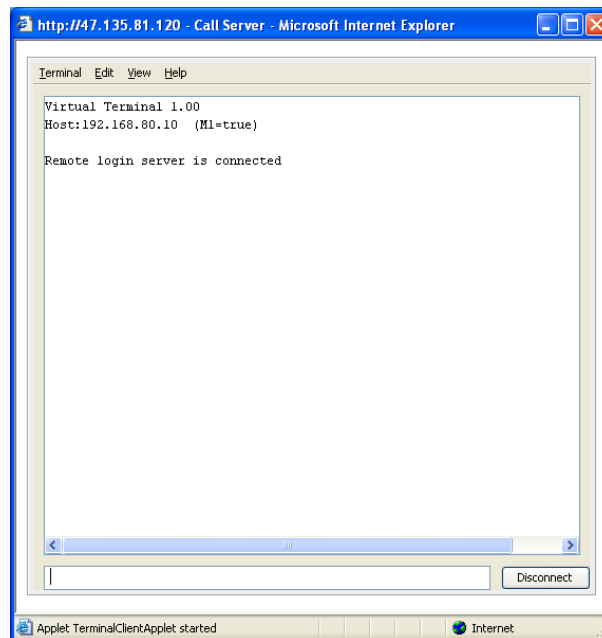


Figure 37: Remote Login with Virtual Terminal

8. Once a connection is established, the Connect button changes to Disconnect. The text box at the bottom of the screen (beside the Disconnect button) used to input text into the virtual terminal session becomes available. The user can type input to the virtual terminal session via this text box. Type **<CR>** several times to get the prompt.

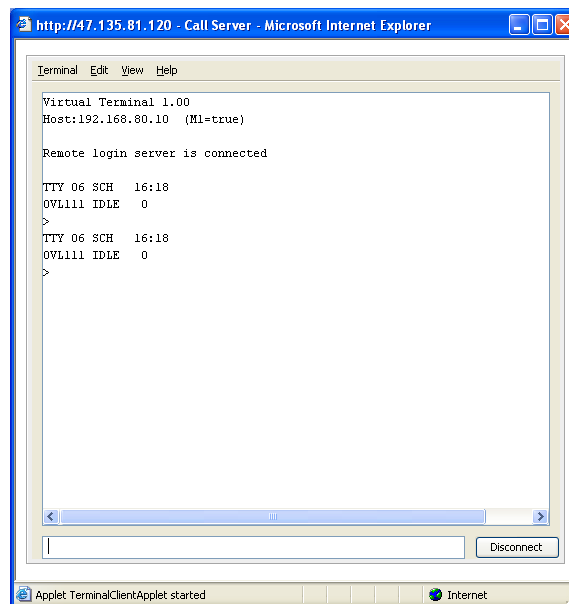


Figure 38: Prompt with Virtual Terminal

9. Type **logi <admin1 or admin2 level userid>** to log in to CS 1000 with administration privileges.
 - a. At the PASS? Prompt, type **< password for administrative userid>**
 - b. You should see a confirmation message about being logged in.

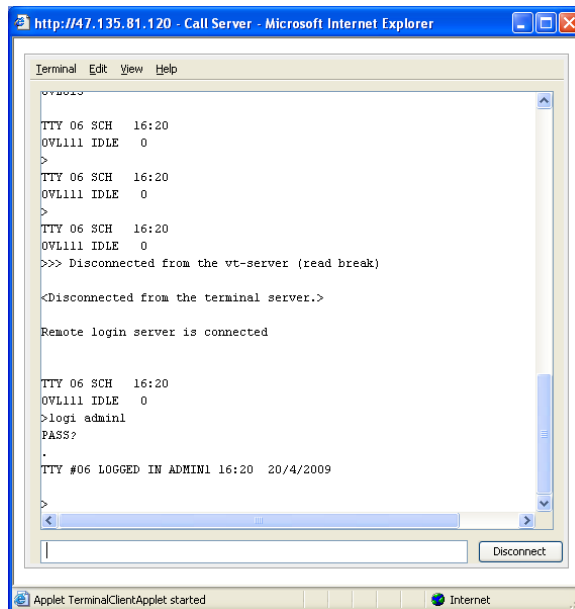


Figure 39: Login with Virtual Terminal

10. Execute the configuration changes needed for users or phones using overlays. This is described in more detail in Section 4.8 *User and Role Terminal Number, Directory Number and CLS Configuration* and Section 4.9 *CS 1000 WLAN Phone Configuration*.
11. Perform a backup to save the configuration changes. This is described in more detail in Section 4.3.4 *Backup of CS 1000 Element Manager*.
12. Type **logo** to log out of the CS 1000 when you have finished.
13. You should see a confirmation message about being logged out.
14. Click the **Disconnect** button in the lower right corner of the virtual terminal emulator. Or you can select **Disconnect** from the **Terminal** menu in the menu bar at the top of the window.
15. A popup dialog will ask you to confirm that you really want to disconnect. Click **Ok** at the prompt

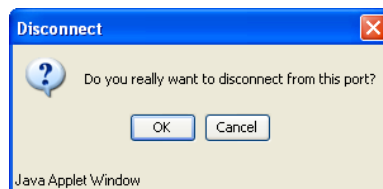


Figure 40: Disconnect Confirmation Dialog

16. A message "Disconnected from the terminal server" will appear.

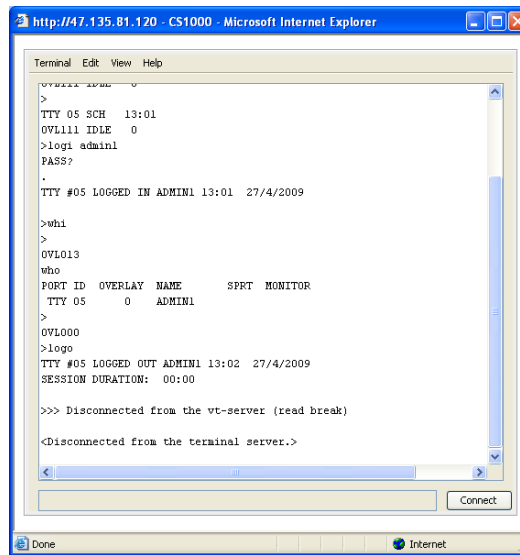


Figure 41: Disconnected Virtual Terminal

17. To close the virtual terminal down you can either:

- a. Select **Exit** from the Terminal menu in the menu bar at the top of the window or
- b. Click the Close window icon

4.6 Creating Pseudo Terminals (PTY) for MDC

Here is an important configuration to ensure that MDC can communicate to the CS 1000. MDC uses the same method as other applications, such as Element Manager or Telephony Manager, to communicate to the CS 1000. This is accomplished with a PTY (Pseudo Terminal), which utilizes rlogin. Rlogin is insecure, which means that u=insecure shells must be enabled. (This configuration has been covered earlier.)

There should be a least three PTYs created when a CS 1000 is being used with MDC.

There are may be restrictions on the number of PTYs supported depending on the CS 1000 Release. For example, a maximum of 4 PTYs are supported with CS 1000 Release 4.5.

The conventions used in this procedure are:

- The commands describe only the important prompts and their input. The user will use <CR> to skip input for the other prompts not described.
- It is assumed that the administrator has already connected and logged in to the CS 1000 Call Server using one of the methods described in Section 4.5 *Options for CLI Connection to CS 1000 for Users and Phone Configuration*

From a CLI prompt to the CS 1000, use these commands to verify whether enough terminals have been created:

```
>ld 37
IOD000
>.stat tty
TTY 0 : DSBL
TTY 1 : DSBL
TTY 2 : DSBL
TTY 3 : DSBL
TTY 4 : ENBL
TTY 5 : ENBL
```

TTY 6 : DSBL DES: pty6
TTY 7 : DSBL DES: pty7
TTY 8 : DSBL DES: pty8
TTY 9 : DSBL DES: pty9
TTY 10 : DSBL DES: pty10
TTY 11 : DSBL DES: pty11
TTY 12 : ENBL DES: pty12
TTY 13 : DSBL DES: pty13
TTY 14 : ENBL DES: pty14
TTY 15 : ENBL DES: pty15

This example shows that the commands to add a new terminal are:

```
>ld 17
CFN000
MEM AVAIL: (U/P): 99051668  USED U P: 5116719 84026  TOT: 104252413
DISK SPACE NEEDED: 126 KBYTES
DCH          AVAIL: 254  USED:  1  TOT: 255
AML          AVAIL:  14  USED:  2  TOT:  16
>REQ chg
TYPE cfn
ADAN new tty 6
  CTYP pty
  PORT 6
  DNUM 06
  DES pty 6
  FLOW no
  USER sch
  TTYLOG no
  BANR no

MEM AVAIL: (U/P): 99051885  USED U P: 5116615 83913  TOT: 104252413
DISK SPACE NEEDED: 126 KBYTES
DCH          AVAIL: 254  USED:  1  TOT: 255
AML          AVAIL:  14  USED:  2  TOT:  16

ADAN DATA SAVED
```

There is a maximum of 16 terminals on a CS 1000, from 0 to 15. In this example, because MDC is using rlogin, this could be from PTY6 to PTY 15. There are 10 PTY terminals defined. ENBL means that they are in use and DSBL means that they are available for use. In the above example, there are 7 available terminals.

4.7 Enable Multiple User Login

This procedure enables multiple user logins, which is needed by MDC. The user may still get a warning that the Overlay memory space is in use. This is only a warning to indicate that there may be a race condition if both parties are in the same overlay and if they are both making the exact same change; the last one to configure will win. This warning does not prevent the changes. If an administrator is in the Element Manager and tries to use an overlay in use, then a popup warning message will indicate this.

The conventions used in this section are:

- The commands describe only the important prompts and their input. The user will use <CR> to skip input for the other prompts not described.
- It is assumed that the administrator has already connected and logged in to the CS 1000 Call Server using one of the methods described in Section 4.5 *Options for CLI Connection to CS 1000 for Users and Phone Configuration*

From an rlogin session, execute these steps to enable the multi-user option:

1. From the rlogin prompt, enter the command **LD 17**
2. At the REQ prompt, enter **chg**
3. At the TYPE prompt, enter **ovly**
4. At the MULTI_USER prompt, enter **on**
5. At the REQ prompt, enter ******** to exit the overlay.

Example output:

```
>LD 17
CFN000
MEM AVAIL: (U/P): 1015918 USED U P: 138773 24956
TOT: 1179647
DISK RECS AVAIL: 486
TMDI D-CHANNELS AVAIL: 0 USED: 0 TOT: 0
DCH AVAIL: 80 USED: 0 TOT: 80
AML AVAIL: 15 USED: 1 TOT: 16
...
>REQ chg
...
>TYPE ovly
....
MULTI_USER on
MEM AVAIL: (U/P): 1015893 USED U P: 138773 24981
TOT: 1179647
DISK RECS AVAIL: 486
TMDI D-CHANNELS AVAIL: 0 USED: 0 TOT: 0
DCH AVAIL: 80 USED: 0 TOT: 80
AML AVAIL: 15 USED: 1 TOT: 16
...
>REQ ****
```

4.8 User and Role Terminal Number, Directory Number and CLS Configuration

Note: The following section describes the creation of MDC users on the CS 1000. These requirements and commands also apply to creating roles on the call server if the optional roles feature will be used in the MDC.

The user terminal number and directory number configured on the CS 1000 are used as the user information provisioned on the MDC Management Station. The user information on MDC must match exactly what is provisioned on the CS 1000. This is facilitated by loading information for the user from the CS 1000 when provisioning users at the MDC Administration GUI.

This section will identify the basic commands to add, query and change users on the CS 1000. Unfortunately, there can potentially be a great deal of variation in the CS 1000 configuration, depending on many factors, including the setup of customer groups, type of phones, feature sets in use, etc. It is assumed that the CS 1000 administrator has already configured these aspects of the CS 1000.

There are two deployments for users:

- Dual TN
- Shared TN

The important information to provision the employee is:

- Terminal number (TN)
- Key number (especially relevant for user in a shared TN deployment)
- Directory number (DN)
- Phone type or terminal type
- Name of employee

MDC supports the use of Multiple Call Ringing (MCR) or Single Call Ringing (SCR) however all phone, users and roles (if used) must be the same call type.

- Note: the use of Multiple Call Ringing (MCR) can be advantageous over Single Call Ringing (SCR). When multiple phones are assigned with the same phone number (for example, a desk phone and a mobile handset), MCR will permit the other phones to ring when a new call is received even when one of the phone is busy with an earlier call. In this instance, MCR must be enabled on the user's phones AND the MDC handsets. Note: MCR is incompatible with certain call features such as call waiting.
- If roles are used with MDC, this is another situation where multiple phones can be assigned the same phone number. This can occur when 2 or more users to select the same role. MCR should be used if multiple people will have the same role (even when the overlapping time period is short) so when one phone is in use the other phones will still ring.

The key highlights for MDC with respect to CS 1000 provisioning are:

- All users must have the same call type configured, either all MCR or all SCR.
 - All WLAN mobile phones and roles must have the same call type feature configured as well...
- If the user has an analogue or digital phone there is no key 0 entry. In this instance, ensure that the CLS line is defined as either MCRA if the user is MCR or MCNR, SCN if the user is SCR.
- Permit multiple-loop dial number on CS 1000. This will enable the CS 1000 to allow for the same phone number to be used across different loops.
- For all users it is recommended to assign names via CPND (Calling Party Name Display), if permitted, to make re-assignment of assets easier to validate. Users can have their employee name.
 - The following substrings cannot be part of the user's name:
 - SCH<one of more digits> e.g. SCH8
 - NPR705
 - OVL429

- For all users and phones, CLID is recommended. It's helpful to enable the CNDA (Calling Name Display Access) feature if permitted. This might mean changing CNDD (Calling Name Display Denied) temporarily to test MDC functionality.
- If the user has features on any key other than Key 0 (the primary DN), these feature do not get transferred to the WLAN handsets when the user checks out their phone using MDC.
- The mapping of certain phone types within the CS 1000 may be different. For example, the 6140/6120 phone type is shown as 2210.

The configuration for any existing users of CS 1000 who will be using MDC should be reviewed to ensure that it is compatible with MDC.

TIP: Remember to do a backup after entering all configuration changes.

The conventions used in this section are:

- The commands describe only the important prompts and their input. The user will use <CR> to skip input for the other prompts not described.
- It is assumed that the administrator has already connected and logged into the CS 1000 Call Server using one of the methods described in Section 4.5 *Options for CLI Connection to CS 1000 for Users and Phone Configuration*

Refer to Nortel Communication Server 1000 Software Input Output Reference – Administration NN43001-611 for additional information on using software input and output commands with the CS 1000.

4.8.1 Permit Multiple Loop Dial Number

Enable multiple-loop dial number, which permits the CS 1000 to allow for the same phone number to be used across different loops.

Note: Use <CR> to skip over a prompt not described.

1. Type ********
2. Type **LD 17**
3. At the REQ prompt, type **CHG**
4. At the TYPE prompt, type **PARM**
5. At the MLDN prompt, type **YES**
6. Type **<CR>** to skip all other prompts.

Example:

```
>ld 17
CHG
PARM
....
MLDN YES      (enter yes to MLDN enable multiple loop DN on the system)
.....
```



4.8.2 Creating New Users

4.8.2.1 Creating New Users in Dual Terminal Number (TN) Deployment

Use this procedure to add new users on the CS 1000 who will be using MDC in the dual terminal number (TN) deployment.

Note: MCR is shown but SCR can be used.

Note: If provisioning a role, the input for Name will be the role name (rather than <firstname>,<lastname>)

Note: Use <CR> to skip over a prompt not described.

1. Type ****
2. Type **LD 11**
3. At the REQ prompt, type **new**
4. At the TYPE prompt, type **<phone type>**
5. At the TN prompt, type **<terminal number>**
6. At the DES prompt, type **<text description>**
7. At the CUST prompt, type **<Customer group number>**
8. At the ZONE prompt, type **<QoS zone>**
9. At the CLS prompt, type **CNDA** (to enable calling name display access)
10. At the KEY prompt, type **0 MCR <DN>**
11. At the CPND prompt, type **new**
12. At the NAME prompt, type **<firstname>,<lastname>**
13. Type **<CR>** to skip all other prompts.
14. The information for the newly added phone/user will automatically be displayed.

Example:

```
>ld 11
SL1000
MEM AVAIL: (U/P): 50348167   USED U P: 1150132 114370   TOT: 51612669
DISK SPACE NEEDED: 129 KBYTES
TNS                AVAIL: 32454   USED: 313   TOT: 32767

REQ: new
TYPE: 1140
TN 156 0 2 16
DES USER
CUST 0
NUID
NHTN
KEM
ZONE 1
ERL
ECL
```

FDN
 TGAR
 LDN
 NCOS
 RNPG
 SSU
 SCPW
 SGRP
 SFLT
 CAC_MFC
 CLS **CNDA**
 HUNT
 SCI
 PLEV
 DANI
 AST
 IAPG
 MLWU_LANG
 MLNG
 DNDR
 KEY **0 MCR 1016**
 MARP
 CPND **new**
 CPND_LANG
 NAME **Darlene,Hiscock**
 XPLN
 DISPLAY_FMT
 VMB
 KEY

MGMT001 TNB NEW TYPE:1140 TN:156 0 2 16

MEM AVAIL: (U/P): 50347858 USED U P: 1150276 114535 TOT: 51612669
 DISK SPACE NEEDED: 130 KBYTES
 TNS AVAIL: 32453 USED: 314 TOT: 32767

4.8.2.2 Creating New Users in Shared Terminal Number (TN) Deployment

Use this procedure to add new users on the CS 1000 who will be using MDC with shared TN deployment.

There can be up to 3 Key Expansion Modules (KEM) supported.

The KEMs are supported for IP phone types 1120, 1140, 1150. The example below is for IP phone type 1140.

The key number range mapped to the Key Expansion Modules for IP phone is:

KEM Value	Range for KEY number
0	0-31
1	32-49
2	50-67

3	68-85
---	-------

Note: MCR is shown but SCR can be used.

Note: If provisioning a role, the input for Name will be the role name (rather than <firstname>,<lastname>)

Note: Use <CR> to skip over a prompt not described.

1. Type ****
2. Type **LD 11**
3. At the REQ prompt, type **new**
4. At the TYPE prompt, type **<phone type>**
5. At the TN prompt, type **<terminal number>** (this is the shared TN)
6. At the DES prompt, type **<text description>**
7. At the CUST prompt, type **<Customer group number>**
8. At the KEM prompt, type **<number of Key Expansion Modules (KEM) being used>**
9. At the ZONE prompt, type **<QoS zone>**
10. At the CLS prompt, type **KEM3 CNDA** (to enable key expansion modules and calling name display access)
11. For each user:
 - a. At the KEY prompt, type **<key number> MCR <DN>**
 - b. At the CPND prompt, type **new**
 - c. At the NAME prompt, type **<firstname>,<lastname>**
 - d. Type **<CR>** to skip all other prompts until the KEY prompt.

Example:

```

OVL000
>ld 11
SL1000
MEM AVAIL: (U/P): 97966505   USED U P: 5681738 604170   TOT: 104252413
DISK SPACE NEEDED: 1582 KBYTES
TNS           AVAIL: 29463   USED: 3304   TOT: 32767

REQ: new
TYPE: 1140
TN 80 0 0 1
DES user
CUST 1
NUID
NHTN
KEM 3
ZONE 1
ERL
ECL
FDN
TGAR
LDN

```

NCOS
RNPG
SSU
SCPW
SGRP
SFLT
CAC_MFC
CLS **kem3**
HUNT
SCI
PLEV
DANI
AST
IAPG
MLWU_LANG
MLNG
DNDR
KEY **32 mcr 8232**
MARP
CPND **new**
CPND_LANG
NAME **user,key32**
XPLN
DISPLAY_FMT
VMB
KEY **33 mcr 8233**
MARP
CPND **new**
CPND_LANG
NAME **user,key33**
XPLN
DISPLAY_FMT
VMB
KEY **50 mcr 8250**
MARP
CPND **new**
CPND_LANG
NAME **user,key50**
XPLN
DISPLAY_FMT
VMB
KEY
KEMOFST

MGMT001 TNB NEW TYPE:1140 TN:80 0 0 1

MEM AVAIL: (U/P): 97965459 USED U P: 5681984 604970 TOT: 104252413
DISK SPACE NEEDED: 1584 KBYTES
TNS AVAIL: 29462 USED: 3305 TOT: 32767

4.8.3 Print using Terminal Number

Use this procedure to review existing users on the CS 1000 who will be using MDC.

Note: Use <CR> to skip over a prompt not described.

1. Type ****

2. Type **LD 11**
3. At the REQ prompt, type **prt**
4. At the TYPE prompt, type **tnb**
5. At the CUST prompt, type **<Customer group number>**
6. At the TN prompt, type **<terminal number>**
7. Type **<CR>** to skip all other prompts.
8. The information for the terminal number will be displayed.

4.8.3.1 Print Dual TN user

Example for user in a dual TN deployment:

```
>ld 11
REQ: prt
TYPE: tnb
```

```
TN 156 0 2 16
DATE
PAGE
DES
```

```
DES USER
TN 156 0 02 16 VIRTUAL
TYPE 1140
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 001
CUR_ZONE 001
ERL 0
ECL 0
FDN
TGAR 1
LDN NO
NCOS 0
SGRP 0
RNPG 0
SCI 0
SSU
XLST
SCPW 1016
SFLT NO
CAC_MFC 0
CLS CTD FBD WTA LPR MTD FND HTD TDD HFD CRPD
MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD DSX VMD SLKD CCSD SWD LND CNDA
CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCB
```

ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDD CFXD ARHD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
UDI RCC HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXR0
USMD USRD ULAD CCBF RTDD RBDD RBHD PGND OCBF FLXD FTTC DNDY DNO3
MCBN
FDSD NOVD VOLA VOUD CDMR ICRD MCDD T87D KEM3 MSNV FRA PKCH
CPND_LANG ENG
HUNT
PLEV 02
DANI NO
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00 MCR 1016 0 MARP
CPND
CPND_LANG ROMAN
NAME Darlene Hiscock
XPLN 24
DISPLAY_FMT FIRST, LAST
01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 16
20 RGA
21 PRK
22 RNP
23
24 PRS
25 CHG
26 CPN

27
28
29
30
31
DATE 17 APR 2009

4.8.3.2 Print Shared TN user

Example for a user in a shared TN deployment:

>ld 11
REQ: prt
TYPE: tnb

TN 80 0 0 1
SPWD
DATE
PAGE
DES

DES USER
TN 080 0 00 01 VIRTUAL
TYPE 1140
CDEN 8D
CTYP XDLC
CUST 1
NUID
NHTN
KEM 3
CFG_ZONE 001
CUR_ZONE 001
ERL
ECL 0
FDN
TGAR 1
LDN NO
NCOS 0
SGRP 0
RNPG 0
SCI 0
SSU
XLST
SCPW 8232
SFLT NO
CAC_MFC 0
CLS CTD FBD WTA LPR MTD FND HTD TDD HFD CRPD
MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD DSX VMD SLKD CCSD SWD LND CNDD
CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDD CFXD ARHD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
UDI RCC HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXR0

USMD USRD ULAD CCBDD RTDD RBDD RBHD PGND FLXD FTTC DNDY DNO3 MCBN
FDSD NOVD VOLA VOUD CDMR ICRD MCDD T87D KEM3 MSNV FRA PKCH
CPND_LANG ENG
HUNT
PLEV 02
DANI NO
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00
01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 16
20 RGA
21 PRK
22 RNP
23
24 PRS
25 CHG
26 CPN
27
28
29
30
31
KEM 1 PAGE 0
32 MCR 8232 0 MARP
CPND
CPND_LANG ROMAN
NAME user key32
XPLN 13
DISPLAY_FMT FIRST, LAST
33 MCR 8233 0 MARP
CPND
CPND_LANG ROMAN
NAME user key33

```
XPLN 13
DISPLAY_FMT FIRST, LAST
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
KEM 2 PAGE 0
50 MCR 8250 0   MARP
   CPND
   CPND_LANG ROMAN
   NAME user key50
   XPLN 13
   DISPLAY_FMT FIRST, LAST
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
KEM 3 PAGE 0 : NO KEYS CONFIGURED
DATE 29 JUL 2009
```

4.8.4 Print Using Directory Number

This is an alternative procedure to review existing users on the CS 1000 who will be using MDC.

Note: Use <CR> to skip over a prompt not described.

1. Type ********
2. Type **LD 11**
3. At the REQ prompt, type **prt**



4. At the TYPE prompt, type **dnb**
5. At the CUST prompt, type **<Customer group number>**
6. At the DN prompt, type **<directory number>**
7. Type **<CR>** to skip all other prompts.
8. The information for the directory number will be displayed.

4.8.5 Add New Name using LD 11

It is recommended that users have names defined. Use this procedure to add names for existing users.

Note: SCR is shown but MCR can be used.

Note: If provisioning a role, the input for Name will be the role name (rather than <firstname>,<lastname>)

Note: Use <CR> to skip over a prompt not described.

1. Type ********
2. Type **LD 11**
3. At the REQ prompt, type **CHG**
4. At the TYPE prompt, type **<phone type>**
5. At the TN prompt, type **<terminal number>**
6. At the ECHG prompt, type **yes**
7. At the ITEM prompt, type **<key 0 information e.g. KEY 0 SCR 1021>**
8. At the CPND prompt, type **new**
9. At the NAME prompt, type **<firstname>,<lastname>**
10. Type **<CR>** to skip all other prompts.

4.8.6 Changing Existing Name using LD 11

It is recommended that users have names defined. Use this procedure to change names for existing users.

Note: SCR is shown but MCR can be used.

Note: If provisioning a role, the input for Name will be the role name (rather than <firstname>,<lastname>)

Note: Use <CR> to skip over a prompt not described.

1. Type ********
2. Type **LD 11**
3. At the REQ prompt, type **CHG**
4. At the TYPE prompt, type **<phone type>**
5. At the TN prompt, type **<terminal number>**
6. At the ECHG prompt, type **yes**
7. At the ITEM prompt, type **<key 0 information e.g. KEY 0 SCR 1021>**
8. At the CPND prompt, type **chg**
9. At the NAME prompt, type **<firstname>,<lastname>**
10. Type **<CR>** to skip all other prompts.



4.8.7 Add New Name using LD 95

It is recommended that users have names defined. This is an alternative procedure to add names for existing users.

Note: If provisioning a role, the input for Name will be the role name (rather than <firstname>,<lastname>)

Note: Use <CR> to skip over a prompt not described.

1. Type ********
2. Type **LD 95**
3. At the REQ prompt, type **new**
4. At the TYPE prompt, type **name**
5. At the CUST prompt, type **<Customer group number>**
6. At the DN prompt, type **<directory number>**
7. At the DES prompt, type **<text description>**
8. At the NAME prompt, type **<firstname>,<lastname>**
9. Type **<CR>** to skip all other prompts.

4.8.8 Changing Existing Name using LD 95

It is recommended that users have names defined. This is an alternative procedure to change names for existing users.

Note: If provisioning a role, the input for Name will be the role name (rather than <firstname>,<lastname>)

Note: Use <CR> to skip over a prompt not described.

1. Type **LD 95**
2. At the REQ prompt, type **chg**
3. At the TYPE prompt, type **name**
4. At the CUST prompt, type **<Customer group number>**
5. At the DN prompt, type **<directory number>**
6. At the DES prompt, type **<text description>**
7. At the NAME prompt, type **<firstname>,<lastname>**
8. Type **<CR>** to skip all other prompts.

4.8.9 Delete Existing Name using LD 95

This is a procedure to delete names for existing users.

Note: Use <CR> to skip over a prompt not described.

1. Type **LD 95**
2. At the REQ prompt, type **out**
3. At the TYPE prompt, type **name**
4. At the CUST prompt, type **<Customer group number>**



5. At the DN prompt, type **<directory number>**
6. Type **<CR>** to skip all other prompts.

4.8.10 Changing Calling Name Display Denied (CNDD) using LD 11

It is recommended that users have Calling Name Display defined.

Note: Use **<CR>** to skip over a prompt not described.

1. Type ********
2. Type **LD 11**
3. At the REQ prompt, type **CHG**
4. At the TYPE prompt, type **<phone type>**
5. At the TN prompt, type **<terminal number>**
6. At the ECHG prompt, type **yes**
7. At the ITEM prompt, type **CLS CNDD CNDA**
8. Type **<CR>** to skip all other prompts.

4.8.11 Change SCR to MCR by deleting KEY 0 using LD 11

The following commands will delete KEY 0 so it can be added again as MCR.

Note: The same command can be used to change MCR to SCR with the correct value substitution.

Note: Use **<CR>** to skip over a prompt not described.

1. Type ********
2. Type **LD 11**
3. At the REQ prompt, type **CHG**
4. At the TYPE prompt, type **<phone type>**
5. At the TN prompt, type **<terminal number>**
6. At the ECHG prompt, type **yes**
7. At the ITEM prompt, type **KEY 0 NUL**
8. Type **<CR>** to skip all other prompts until REQ.
9. At the REQ prompt, type **CHG**
10. At the TYPE prompt, type **<phone type>**
11. At the TN prompt, type **<terminal number>**
12. At the ECHG prompt, type **yes**
13. At the ITEM prompt, type **KEY 0 MCR <directory number>**
14. Type **<CR>** to skip all other prompts.

4.8.12 Printing MAC using LD 20

The following command will print the MAC address for a given terminal number. While this procedure is executing, the phone must be turn on and able to make & receive calls for this command to work.

1. Type ********
2. Type **LD 20**
3. At the REQ prompt, type **IDU <Terminal number>**
4. Type **<CR>** to skip all other prompts.

4.8.13 Backup

Use this procedure to back up and save the configuration changes defining the users for MDC.

1. Type **LD 43**
2. Type **.edd**

4.8.14 Useful Commands

4.8.14.1 Who

Used to display userid used to log in:

1. Type **who**

Example:

```
>who
```

```
PORT ID OVERLAY NAME    SPRT MONITOR
TTY 05   0  SANDRA
```

4.8.14.2 Exit from Overlay or Command

Used to escape overlay with four asterisks:

1. Type ********

4.8.14.3 Display Information on Error Code

Used to display information on an error code:

1. Type **err <error code>**

Example:

```
>err SCH0099
```

```
>
```

```
SCH0099
```

This message appears when invalid input is detected by the machine.

The actual output may vary, according to the input received.

Refer to the following examples for possible output.

Severity: Info

4.9 CS 1000 WLAN Phone Configuration

The WLAN phone configuration on the CS 1000 is used as the asset information provisioned on the MDC Management Station. The asset information on MDC must match exactly what is provisioned on the CS 1000. This is facilitated by being able to load information for the asset from the CS 1000 when adding new assets at the MDC Administration GUI.

MDC supports the use of Multiple Call Ringing (MCR) or Single Call Ringing (SCR) however all phone, users and roles (if used) must be the same call type.

- The use of Multiple Call Ringing (MCR) can be advantageous over Single Call Ringing (SCR). When multiple phones are assigned with the same phone number (for example, a desk phone and a mobile handset), MCR will permit the other phones to ring when a new call is received even when one of the phone is busy with an earlier call. In this instance, MCR must be enabled on the user's phones AND the MDC handsets. Note: MCR is incompatible with certain call features such as call waiting.

The following is recommended for WLAN phone configuration:

- All WLAN phones should have default DNs.
- All WLAN mobile phones must have the same call type configured, either all MCR or all SCR.
 - All employees and roles must have the same call type feature configured as well.
- Permit multiple-loop dial number on CS 1000. This will enable the CS 1000 to allow for the same phone number to be used across different loops.
- Use CLID for all users and phones. It is helpful to enable the CNDA (Calling Name Display Access) feature if permitted. This might mean changing CNDD (Calling Name Display Denied) temporarily to testing MDC functionality.
- Default names on the WLAN phones are not needed. Existing names assigned to WLAN phones as CPND will be overwritten when the phones are checked out to users.
 - If default names are used, the following substrings cannot be part of the name:
 - SCH<one of more digits> e.g. SCH8
 - NPR705
 - OVL429
- If the optional role feature will be used on MDC with both personal phone number and role phone number assignment to the WLAN phone, ensure that all WLAN phones have two lines provisioned i.e. key 0 and key 1. The configuration of the second line must conform to all requirements identified earlier.
 - In situations where only some MDC Stations will be provisioned with checkout of both role and personal phone numbers, for easier deployment it is recommended that all WLAN phones have two lines provisioned unless the dual line WLAN phones can be easily distinguished.

- Any feature which requires a user specific number to be dialed should not be configured on the WLAN handsets used in the MDC solution. For example, the Dialed Intercom Group (DIG) feature should not be used on the WLAN handsets.
- Test all WLAN phones once they have been provisioned to ensure that they are operational. It is recommended to use the WLAN handset to make a phone call, and to receive a call by ringing the WLAN handset.
- Each WLAN phone must physically have a unique barcode label attached to the back of the handset or inside the battery compartment if using a protective silicon cover (e.g. zCover) on the WLAN handset. See NN49010-501 Nortel Healthcare Solutions MDC Deployment Guide for information on label generation.

The configuration for an existing WLAN phone on the CS 1000 which will be using MDC should be reviewed to ensure that it is compatible with MDC.

The mapping of certain phone types within the CS 1000 may be different. For example, the 6140/6120 phone type is shown as 2210.

Remember to do a backup after entering all configuration changes.

Location tracking is an optional feature of MDC. If location tracking is being used for WLAN phones, the following is required:

- A site survey must be done for 802.11 A/B/G for location tracking. RFid tags use 802.11 B/G whereas the phones use 802.11 A.
- There must be sufficient licenses on Ekahau Position Engines to track the location-enabled WLAN phones. See the Nortel Healthcare Solution Asset Tracking Management Documentation Suite or EPE Product documentation for more information.
- Each WLAN phone which will be location tracked must be physically configured on the handset to enable location tracking by configuring the following:
 - RTLS Enable
 - Transmit interval should be set to 1 minute.
 - Enter the IP address of the EPE as location service.
 - Set ELP (Ekahau Location Port) to default 8552.

The important information for provisioning the WLAN phones for MDC is:

- Terminal number (TN)
- Directory number (DN)
- Phone type or terminal type
- Optional (for location tracking only): IP address of EPE
- Optional (for location tracking only): ELP

4.9.1 Enable MCR/SCR on Mobile phones

To enable MCR/SCR for an IP phone, define key 0 as MCR/SCR when the phone is created for the first time.

Note: MCR is shown but SCR can be used.

Example:

```
>Ld 11
New
.....
>Key 0 mcr xxxx (xxxx) the phone number
.....
```

4.9.2 Permit Multiple Loop Dial Number

Enable multiple loop dial number, which permits the CS 1000 to allow for the same phone number to be used across different loops.

Example:

```
>ld 17
CHG
PARM
.....
MLDN YES (enter yes to MLDN enable multiple loop DN on the system)
.....
```

4.9.3 Enable Location tracking

Hold the orange button down to turn off the phone.

To enter the administrative mode on the phone, hold the green button while you turn the phone on by pressing the orange button.

A prompt for the Administrative password will appear. Enter the password; the default is 123456. The password can be changed.

Under Phone Config > Location Service set the following:

- RTLS Enable
- Transmit interval as 1 minute
- Location Service: enter the IP address of the EPE
- ELP Port: default is 8552



5 Communication Server 2100 Configuration for MDC

This section provides an overview of the required Communication Server (CS) 2100 configuration steps that precede integration with the rest of the MDC Solution and a list of the required information. The MDC Solution integrates with CS 2100 Release CICM 10.1 MR2 load, which is compatible with SE10, SE11, and SE13.

WARNING: It is strongly recommended that the CS 2100 configuration steps should only be performed by a qualified CS 2100 Administrator who has detailed knowledge and understanding of the CS 2100 system.

If needed, the CS 2100 Product documentation should be used as reference for the detailed steps for the procedures. Remember to use the documentation specific to the release of CS 2100 being used.

The following manuals are useful. Use the appropriate version based on the CS 2100 release being used:

- CVM11 Engineering Rules - Carrier Voice over IP CS-LAN SEB-08-00-001
- Nortel ATM/IP Solution-level Administration and Security NN10402-600
- Nortel Communication Server 2100 Service Order Reference, Commercial Systems NN42100-103
- Nortel OSSGate User Guide - NE10004-512
- Nortel ATM/IP Solution-level Administration and Security - NN10402-600
- Nortel CICM Fundamentals - NN10044-111
- Nortel CICM Configuration - NN10240-511
- Nortel CICM IP Phones fundamentals - NN10300-135
- Nortel WLAN Handset Fundamentals NN43001-505
- Nortel WLAN IP Telephony Installation and Commissioning NN43001-504
- Nortel WLAN Handset 6120 and WLAN Handset 6140 User Guide NN43150-100
- Nortel WLAN Handset 2210 User Guide NN10300-077
- Nortel WLAN Handset 2211 User Guide NN10300-078
- Nortel WLAN Handset 2212 User Guide NN10300-071

5.1 Roadmap Overview of CS 2100 Configuration for MDC

It is intended that these preparatory steps for CS 2100 can be performed in advance of the deployment of the MDC Solution. The CS 2100 configuration for MDC Solution consists of the following sequence of steps:

1. Verify you have the information needed prior to starting to configure the CS 2100 for the MDC Solution. The required information is listed in Section 5.2 *Required Information for CS 2100 Configuration for MDC*.
2. Execute basic CS 2100 configuration to enable the MDC application to communicate with the CS 2100. These details are summarized in Section 5.1.1 *Summary of CS 2100 Configuration for MDC Server*.
3. Create new employee configuration on the CS 2100 or verify existing employee configuration to ensure these are compatible with the MDC Solution. The employee configuration will be used as the basis for users on the MDC Solution. The details are summarized in Section 5.1.2 *Summary of CS 2100 Configuration for MDC Users*.
4. Create new WLAN handset configuration on the CS 2100 or verify existing WLAN handset configuration to ensure these are compatible with the MDC Solution. The WLAN handset configuration will be used as

the basis for phone asset on the MDC Solution. The details are summarized in Section 5.1.3 *Summary of CS 2100 Configuration for MDC Phone/Assets*.

5. If the optional role feature is licensed on MDC, create new role configuration on the CS 2100 or verify existing role configuration to ensure these are compatible with the MDC Solution. The role configuration will be used as the basis for roles on the MDC Solution. The configuration of roles is similar to the configuration of employees except roles are associated with functions (such as Doctor on call) rather than people. For further guidelines on configuring roles, refer to Section 5.1.2 *Summary of CS 2100 Configuration for MDC Users*.

If multiple people may be assigned the same role (even for a short duration), it is strongly recommended that the line mode be MCA for all the roles and users on the call server.

6. Backup the CS 2100 configuration to preserve any configuration changes made for the MDC Solution.

WARNING: In addition, it is recommended to coordinate the following CS 2100 activities to avoid impacting MDC operations:

- It is recommended to avoid scheduling CS 2100 maintenance activities during shift changes or periods of high MDC Station usage (i.e. checkout or returns). Any CS 2100 activities which prevent the ability to make CS 2100 line provisioning changes or stops journaling (such as reload restarts or upgrades) will adversely affect MDC checkout or returns.

5.1.1 Summary of CS 2100 Configuration for MDC Server

This section 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

Verify you have the information needed prior to starting to configure the CS 2100 for the MDC Solution. The required information is listed in Section 5.2 Required Information for CS 2100 Configuration for MDC.

1. It is recommended the document SEB-08-00-001 Engineering Rules - Carrier Voice over IP CS-LAN be followed when connecting the MDC to CS 2100. In particular, to secure communications over OSSGATE, it is recommended the MDC should have secure access to the OAMP VLAN of CS-LAN.
2. Using procedure in NN10402-600 Nortel ATM/IP Solution-level Administration and Security document, login into SESM Server and create SESM userid for MDC to access OSSGATE with a primary group of **succssn** and secondary user group authorization of **Insprov**
3. Perform a backup.
4. Validate the basic network connectivity and communication between CS 2100 and MDC Server if the operating system has been installed on MDC Server.
 - From a terminal window on the MDC Server, ping the IP address of Packet Telephony Manager (PTM).
 - If the ping is successful, you have established network connectivity. Attempt to log into the OSSGate on Packet Telephony Manager (PTM) server using the command: **telnet <IP address of PTM> <OSSGATE port number on SESM>**
 - When prompted, enter the SESM userid and password created for MDC
 - Type **servord** to enter Service Order (SERVORD) level.

- If you get a prompt **>** you have successfully established communications between CS 2100 and MDC.
- To exit PTM, type **<ctrl> B**. At the **?** prompt, enter **logout**.
- To exit telnet connection, type **<ctrl> B**. At the **?** prompt, enter **clearcon**.

5.1.2 Summary of CS 2100 Configuration for MDC Users

Create new employee configuration on the CS 2100 or verify existing employee configuration to ensure these are compatible with the MDC Solution. The employee LEN (terminal number) and directory number configured on the CS 2100 are used as the user information provisioned on the MDC Administration GUI. The user information on MDC must match exactly what is provisioned on the CS 2100.

Note: This section describes the creation of MDC users on the CS 2100. These requirements also apply to creating roles on the call server if the optional roles feature will be used in the MDC.

Verify you have the information needed prior to starting to configure the CS 2100 for the MDC Solution. The required information is listed in Section 5.2 Required Information for CS 2100 Configuration for MDC.

Only the minimal configuration is discussed. The CS 2100 administrator can configure additional features beyond what is described. Refer to CS 2100 documentation if further details are required on the procedures.

There are two deployments for users:

- Dual Line Equipment Number (also referred to as Dual Terminal Number (TN))
- Shared Line Equipment Number (also referred to as Shared Terminal Number (TN))

The important information to provision the employee is:

- Line Equipment Number (LEN) (which is refer to as Terminal number on MDC)
- Key number (especially relevant for user in a shared LEN deployment)
- Directory number (DN)
- Phone type or terminal type
- Name of employee

MDC supports the use of Multiple Call Arrangement (MCA) or Single Call Arrangement (SCA) however all users and roles (if used) must be the same call type.

- Note: the use of Multiple Call Arrangement (MCA) can be advantageous over Single Call Arrangement (SCA). When multiple phones are assigned with the same phone number (for example, a desk phone and a mobile handset), MCA will permit the other phones to ring when a new call is received even when one of the phone is busy with an earlier call. Note: MCA is incompatible with certain call features such as call waiting.
- If roles are used with MDC, this is another situation where multiple phones can be assigned the same phone number. This can occur when 2 or more users to select the same role. MCA should be used if multiple people will have the same role (even when the overlapping time period is short) so when one phone is in use the other phones will still ring.

Use the following checklist which highlights the key CS 2100 provisioning compatibilities for MDC users:

- All users of MDC must have the same multiple-appearance call type configured, either all MCA or all SCA.
 - The multiple-call appearance call type chosen for users must also apply to roles, if the optional role feature is used.
- With dual TN, the MDC users must be assigned as the primary member of Multiple Appearance Directory Number (MADN) on their main phone. With shared TN, the MDC users should be assigned as the primary MADN member on the shared terminal (i.e. shared LEN).
 - Note: On the CS 2100, the maximum number of members of a MADN group (i.e. DN) is 32. Since 1 member is permanently assigned, usually to a shared TN, this leaves 31 members available for assignment to the mobile phones. Therefore, a maximum of 31 mobile phones can be simultaneously checked-out with the same role DN. This maximum is fixed and cannot be modified through provisioning
- With Shared TN: to enable Call Forwarding (CFW) for users, the CFW feature must be assigned to the shared TN
 - As the same CFW is used by all DN on a shared TN, this should be provisioned to voice mail.
 - You may consider using Remote Call Forwarding (RCF) for user DNs which are not checked-out. This was to allow calls to those DNs to forward to voice mail even when there is no physical phone associated with them. The alternative is to assign these DNs to the various keys of an unused terminal which would have the Call Forward Don't Answer (CFDA) feature assigned to forward calls to the individual user's voice mail box
- For all users it is recommended to assign their names to their DN
- Most of user features do not get transferred to the WLAN handsets with checkout.
 - Only DN gets assigned to the mobile, so only certain DN features get assigned automatically (CFW and name display)
- The configuration for any existing users of CS 2100 who will be using MDC should be reviewed to ensure that it is compatible with MDC.

Remember to do a backup after entering all configuration changes.

Tip: Retain the user information provisioned on CS 2100 for provisioning users on MDC Administration GUI. There is no automatic loading information for the user from the CS 2100 when provisioning users at the MDC Administration GUI. Refer to Section 3.3.1.3 *Preparing for Bulk Loading Users and Phones into MDC* if bulk loading will be used.

Note: For CS 2100 call servers, when provisioning users on the MDC it is necessary to specify DN with the full 10 digit DN, even if extension dialing is supported.

5.1.3 Summary of CS 2100 Configuration for MDC Phone/Assets

Create new WLAN handset configuration on the CS 2100 or verify existing WLAN handset configuration to ensure these are compatible with the MDC Solution. The WLAN phone configuration on the CS 2100 is used as the asset phone information provisioned on the MDC Administration GUI. The asset information on MDC must match exactly what is provisioned on the CS 2100.

Verify you have the information needed prior to starting to configure the CS 1000 for the MDC Solution. The required information is listed in Section 5.2 Required Information for CS 2100 Configuration for MDC.



Use the following checklist which highlights the key CS 2100 provisioning compatibilities for MDC WLAN phones:

- If the optional role feature will be used on MDC, ensure that all WLAN phones have two lines provisioned i.e. key 1 and key 2. The configuration of the second line must conform to all requirements identified.
 - In situations where only some MDC Stations will be provisioned with checkout of both role and personal phone numbers, for easier deployment it is recommended that all WLAN phones have two lines provisioned unless the dual line WLAN phones can be easily distinguished.
- All WLAN phones should have default DNs.
 - The WLAN handsets must only have a default DN assigned to key 1. Key 2 must be left unassigned even when roles are supported
 - These default DNs must be unique in the system and cannot be used with any other existing LEN on the CS 2100 i.e. WLAN phones default DN must be a single DN, cannot be part of MADN
- Key assignment must match what has been provisioned for key 1 and key 2 (if used) on the CICM;
 - It is recommended to create a CICM profile for the handset to define key 1 and key 2 (if required) as DN keys
 - The CICM handset profile must permit autologin.
 - It recommended to provision the WLAN phones using their DN as username and the same password for all handsets
- Any features assigned to the WLAN phones used in the MDC solution should not be user specific (such as group intercom or speed call containing personal numbers)
- Test all WLAN phones once they have been provisioned to ensure that they are operational. It is recommended to use the WLAN handset to make a phone call, and to receive a call by ringing the WLAN handset.
- Each WLAN phone must physically have a unique barcode label attached to the back of the handset or inside the battery compartment if using a protective silicon cover (e.g. zCover) on the WLAN handset. See NN49010-501 Nortel Healthcare Solutions MDC Deployment Guide for information on label generation.
- The configuration for an existing WLAN phone on the CS 2100 which will be using MDC should be reviewed to ensure that it is compatible with MDC.
- After configuring the WLAN phones on the CS 2100 call server, test each phone to ensure they are working and physically configure each individual phone for use with MDC:
 - Power on handset and login to verify WLAN handset is working.
 - Enable the autologin feature on the handset (Note that the ability to configure autologin on the handset must be enabled through the CICM profile).
 - Configure the extension (Ext.) display to the default DN for the handset (this is not automatic as on CS 1000)
 - Enable location tracking if this optional MDC feature will be used.
- After the phone has been verified to be operational, assign RSUS option (Requested SUSpension) for the phone's default DN.
 - For CS 2100 call server, WLAN phone must not be operational unless checked out. The option to Disable Return Phones must also be selected when configuring the CS 2100 call server on the MDC Administration GUI.

Remember to do a backup after entering all configuration changes.

Tip: Retain the WLAN phone information provisioned on CS 2100 for provisioning phone (assets) on MDC Administration GUI. There is no automatic loading information for the WLAN phone from the CS 2100 when provisioning phones at the MDC Administration GUI. Refer to Section 3.3.1.3 *Preparing for Bulk Loading Users and Phones into MDC* if bulk loading will be used.

Note: For CS 2100 call servers, when provisioning phone/asset on the MDC it is necessary to specify DN with the full 10 digit DN, even if extension dialing is supported.

Location tracking is an optional feature of MDC. If location tracking is being used for WLAN phones, the following is required:

- A site survey must be done for 802.11 A/B/G for location tracking. RFid tags use 802.11 B/G whereas the phones use 802.11 A.
- There must be sufficient licenses on Ekahau Position Engines to track the location-enabled WLAN phones. See the Nortel Healthcare Solution Asset Tracking Management Documentation Suite or EPE Product documentation for more information.
- Each WLAN phone which will be location tracked must be physically configured on the handset to enable location tracking by configuring the following:
 - RTLS Enable
 - Transmit interval should be set to 1 minute.
 - Enter the IP address of the EPE as location service.
 - Set ELP (Ekahau Location Port) to default 8552.

The important information for provisioning the WLAN phones for MDC is:

- LEN (used as Terminal number (TN))
- Directory number (DN)
- Phone type or terminal type
- Optional (for location tracking only): IP address of EPE
- Optional (for location tracking only): ELP

5.2 Required Information for CS 2100 Configuration for MDC

The following information is needed prior to starting to configure the CS 2100 for the MDC Solution:

Table 33: Required Information for CS2100 Configuration for MDC

	Required Information for CS2100 Configuration for MDC	
1	SESM Server IP Address	This is the same as PTM IP Address

2	user name and password to login to SESM Server	
3	Root password for SESM Server	
4	SESM account for MDC: <ul style="list-style-type: none"> • Userid • Password 	
5	OSSGATE port number on SESM	The port number is provisionable on the SESM
6	IP address for MDC Server	
7	Non-root username and password for MDC Server (due to OS security hardening, root account cannot be used to log into MDC Server)	
8	Root password for MDC Server	
9	Multiple Call Arrangement (MCA) or Single Call Arrangement (SCA)	This call type must be the same for all users and roles used with MDC.
10	These values are the same of all users, phones and roles with MDC: <ul style="list-style-type: none"> • Customer Group for phones and users • Customer Subgroup • Network Class of Service • Local Access and Transport Area (LATA) 	
11	To provision each user for dual TN (Terminal Number) deployment: <ul style="list-style-type: none"> • LEN (used as Terminal number (TN)) • Directory number (DN) • Phone type or terminal type • Name of employee (first & last) 	See table below to capture dual TN user information

12	<p>To provision users for shared TN (Terminal Number) deployment:</p> <ul style="list-style-type: none"> • Shared LEN (used as Terminal number (TN)) • Phone type or terminal type <p>To provision each users in this shared TN (Terminal Number) deployment:</p> <ul style="list-style-type: none"> • Key number • Directory number (DN) • Name of employee (first & last) 	See table below to capture shared TN user information
13	CICM Profile for handset	<p>Profile should define Key 1 and optionally Key 2. Key 2 is only required if the optional MDC role feature will be used in the mode where both the user's personal phone number and the role phone number will be assigned to the handset during checkout</p> <p>The CICM handset profile must permit autologin.</p>
14	Distinct user names for each WLAN handset	This is the parameter entered under the USERID option when the phone is provisioned. The USERID is typically part or all of the default DN. This username is needed to log the phone in.
15	Common password to be used on all WLAN handsets user names.	This parameter is entered when the phone is provisioned. This information is needed to log the phone in.
16	<p>To provision each mobile WLAN phones for MDC:</p> <ul style="list-style-type: none"> • LEN (used as Terminal number (TN)) • Directory number (DN) – key 1 	See table below to capture phone information.
17	<p>[Optional] To enable location tracking on the WLAN phone (only if the phone will be location tracked):</p> <ul style="list-style-type: none"> • IP address of EPE (Ekahau Positioning Engine) • ELP (Ekahau Location Port) number 	This information is only needed if optional MDC location tracking feature will be used.
18	<p>[Optional] To provision each role for dual TN (Terminal Number) deployment:</p> <ul style="list-style-type: none"> • LEN (used as Terminal number (TN)) • Directory number (DN) • Phone type or terminal type • Display Name of role 	<p>Only required if the optional MDC role feature will be used.</p> <p>See table below to capture dual TN role information</p>

19	<p>[Optional] To provision roles for shared TN (Terminal Number) deployment:</p> <ul style="list-style-type: none"> • Shared LEN (used as Terminal number (TN)) • Phone type or terminal type <p>To provision each role in this shared TN (Terminal Number) deployment:</p> <ul style="list-style-type: none"> • Key number • Directory number (DN) • Display name of role 	<p>Only required if the optional MDC role feature will be used.</p> <p>See table below to capture shared TN role information</p>
----	---	--

Table 34: Required CS 2100 Information for Dual TN User Information

Line Equipment Number (LEN)	Directory number (DN)	Phone type or terminal type	Name of employee (first & last)

Table 35: Required CS 2100 Information for Shared TN user information

Shared Line Equipment Number (LEN)	Phone type or terminal type	Key number	Directory number (DN)	Name of employee (first & last)

Table 36: Required CS 2100 Information for WLAN Handset

Line Equipment Number (LEN)	Directory number (DN) – key 1

Table 37: Required CS 2100 Information for Dual TN Role Information [Optional]

Line Equipment	Directory number (DN)	Phone type or terminal type	Name of role
----------------	-----------------------	-----------------------------	--------------

Number (LEN)			

Table 38: Required Information for Shared TN Role information [Optional]

Shared Line Equipment Number (LEN)	Phone type or terminal type	Key number	Directory number (DN)	Name of role



6 References

1. Nortel Healthcare Solutions MDC Documentation Roadmap NN49010-100
2. Nortel Healthcare Solutions MDC Administration Guide NN49010-600
3. Nortel Healthcare Solutions MDC Application Troubleshooting Guide NN49010-700
4. Nortel Healthcare Solutions MDC Deployment Guide NN49010-501
5. Nortel Healthcare Solution Asset Tracking Management Documentation Suite
6. Nortel Communication Server 1000 System Management Reference NN43001-600 Standard Release 5.5
7. Nortel Communication Server 1000 Software Input Output Reference – Administration NN43001-611
8. Nortel Communication Server 1000 Element Manager System Reference – Administration NN43001-632
9. Nortel Communication Server 1000 Network Routing Service Installation and Commissioning NN43001-564
10. Nortel Communication Server 1000 IP Phones Description, Installation and Operations
11. Nortel WLAN Handset Fundamentals NN43001-505
12. Nortel IP Line Fundamentals NN43100-500
13. Nortel WLAN IP Telephony Installation and Commissioning NN43001-504
14. Nortel WLAN Handset 6120 and WLAN Handset 6140 User Guide NN43150-100
15. Nortel WLAN Handset 2210 User Guide NN10300-077
16. Nortel WLAN Handset 2211 User Guide NN10300-078
17. Nortel WLAN Handset 2212 User Guide NN10300-071
18. MK1200 MicroKiosk for CE.NET 4.2, Product Reference Guide, 72E-87924-02 Revision A, *January 2008*
19. KRS User Guide for MDC is available from KRS. Within KRS, select **Product Control > Documentation, Forms & USER GUIDES**.
20. CVM11 Engineering Rules - Carrier Voice over IP CS-LAN SEB-08-00-001
21. Nortel ATM/IP Solution-level Administration and Security NN10402-600
22. Nortel Communication Server 2100 Service Order Reference, Commercial Systems NN42100-103
23. Nortel OSSGate User Guide - NE10004-512
24. Nortel ATM/IP Solution-level Administration and Security - NN10402-600
25. Nortel CICM Fundamentals - NN10044-111
26. Nortel CICM Configuration - NN10240-511
27. Nortel CICM IP Phones fundamentals - NN10300-135



7 Acronyms and Definitions

ATM	Asset Tracking Management
CEM	CS 1000 Element Manager
CFW	Call Forwarding
CICM	Centrex IP Client Manager
CLI	Command Line Interface
CS 1000	Communication Server 1000
CS 2100	Communication Server 2100
DN	Directory Number
DSC	Distant Steering Code
ELP	Ekahau Location Port
EPE	Ekahau Positioning Engine
GUI	Graphical User Interface
IP	Internet Protocol
KRS	Keycode Retrieval System
LATA	Local Access and Transport Area
LEN	Line Equipment Number
MADN	Multiple Appearance Directory Number
MCA	Multiple Call Arrangement
MCR	Multiple Call Arrangement with Ringing
MDC	Mobile Device Checkout
MDN	Multiple Appearance Directory Number
NRS	Network Routing Service
OSSGate	Operations Support System Gate
PTM	Packet Telephony Manager
PTY	Pseudo Terminal



RDM	Remote Device Manager
RSUS	Requested SUSpension
RTLS	Real Time Location System
SCA	Single Call Arrangement
SCR	Single Call Arrangement with Ringing
SERVORD	Service Order System
SESM	Succession Element Sub-element Manager
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
TN	Terminal Number
WLAN	Wireless Local Area Network



8 Appendices

End of Document