

Nortel Contact Recording

Planning, Installation and Administration Guide

Product release 6.5

Standard 01.15

October 2009



Nortel Contact Recording

Planning, Installation and Administration Guide

Publication number:	NN44480-300
Product release:	6.5
Document release:	Standard 01.15
Date:	October 2009

Copyright © 2008-2009 Nortel Networks. All Rights Reserved.

All materials provided herein are the exclusive property of Nortel Networks and its licensors. Only expressly authorized individuals under obligations of confidentiality are permitted to review materials in this document. By reviewing these materials, you agree to not disclose these materials to any third party unless expressly authorized, and to protect the materials as confidential and trade secret information. Any unauthorized review, retransmission, dissemination or other use of these materials is strictly prohibited. If you are not authorized to review these materials, please return these materials (and any copies) from where they were obtained. All materials found herein are provided "AS IS" and without warranty of any kind. Information is subject to change without notice.

Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

Any other use of the data and the transmission process is a violation of the user license unless specifically authorized in writing by Nortel Networks prior to such use. Violations of the license by alternative usage of any portion of this process or the related hardware constitutes grounds for an immediate termination of the license and Nortel Networks reserves the right to seek all allowable remedies for such breach.

Nortel, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

Contents

1	New in this Release	9
2	Getting Started	11
	Overview	12
	Definitions	13
	What's New	14
	Who should read this guide	15
	Additional Resources	16
	How to get help	17
3	System Overview	19
	Introduction	20
	Recording Options	21
	Server components	29
	Optional Server Applications	30
	End-User tools	33
	Component Co-residency	35
	Limitations of this release	36
4	Planning and Prerequisites	38
	Introduction	39
	Recording Requirements	40
	Storage Requirements	44
	Server Platform	47
	Network Issues	49
	Nortel Contact Center prerequisites	50
	Topologies	52
	Integrating with other systems	58
	Remote Support Strategy	60
5	Installation	62
	Overview	63
	Preparing your call center for Contact Recording	64
	Platform Installation	66
	Order in which to Install Applications	69
	Installing the Nortel Contact Recording Master	70
	Installing a Nortel Contact Recording Standby Server	71
	Installing Nortel Contact Recording Slaves	72
	Installing Nortel TDM Contact Recorders	73
	Installing Nortel Quality Monitoring	75
	Installing Viewer	76
	Installing Archive Manager	79
	Installing Nortel Contact Recording Desktop (CRD)	80
	Upgrading	86

6	Configuration	88
	Overview	89
	Accessing the System	90
	Licensing	92
	Security	93
	General Setup	95
	System Monitoring	101
	Operations	103
	Search and Replay	110
	Backup/Restore	115
7	Operations, Administration & Maintenance	122
	Introduction	123
	Status Monitoring	124
	Alarms	129
	Audit Trail	130
	Local Archive	131
	Preventative Maintenance	133
	Best Practice: Restarting Servers	136
8	Advanced Configuration	138
	Properties File	139
	Contact Recording Desktop (CRD)	145
	User Defined Fields	154
	Customizing Search and Replay	155
	Installing a Signed SSL Certificate	159
	Installing Unlimited Strength Encryption	162
A	Technical Reference	164
	IP Recorder Interfaces	165
B	Troubleshooting	168
	Hints and Tips	169
	Interpreting Log Files and Alarms (CS1000 systems)	171
	Specific Problems	176
C	Alarms	182
	Alarms	183
	Alarms Table	184
D	Recorder Control Protocol	200
	Introduction	201
	Java API Toolkit	202
	TCP/IP Protocol Overview	203
	TCP/IP Message Sequences	206

E Auto-dialer Integrations (only available with 6.5.1 update) 212

Introduction	213
Configuration	215
Avaya PCS/PDS Dialer	223

Glossary 226

Chapter 1

New in this Release

Features

CRQM Release 6.5.1 provides the following new or enhanced features:

- Support for Nortel CS2x00 and DMS switches

Other Changes

Revision History

October 2009	Standard 1.15 This document is up-issued to reflect changes made in the section System Monitoring.
September 2009	Standard 1.14 This document us up-issued to reflect changes made in the section Planning and Prerequisites.
August 2009	Standard 1.13 This document is up-issued to reflect updates included in version 6.5.1 of CRQM.
July 2009	Standard 1.12 This document is up-issued to reflect changes made in Advanced Configuration. See Chapter 8, “Advanced Configuration,” for more information.
June 2009	Standard 1.11 This document is up-issued to include enhancements to the instructions for performing a Postgres database backup. See Chapter 6, “Configuration,” for more information.
May 2009	Standard 1.10 This document is up-issued to include updates for Communication Server 2x00 (CS2x00) and Digital Multiplex Switch (DMS) systems.

May 2009	Standard 1.09 This document is up-issued to add section ‘Windows Authentication’ to the Chapter ‘Configuration’
April 2009	Standard 1.08 This document is up-issued to update the information about changing system settings in the section “ <i>Properties File</i> ”.
April 2009	Standard 1.07 This document is up-issued to update the information about Current Java TimeZone(TZ) in the section “ <i>Platform Installation</i> ”.
March 2009	Standard 1.06 This document is up-issued to update the technical content in the section “ <i>Restoring data to a new PostgreSQL database</i> ”.
January 2009	Standard 01.05 This document is up-issued to update the technical content in the section “ <i>Nortel Contact Recording Master Co-resident with TDM Recorder</i> ”
August 2008	Standard 01.04 Updated page 39 to reflect that using a call recording card for bulk recording is not recommended.
April 2008	Standard 01.03

Chapter 2

Getting Started

In this chapter

Overview	12
Definitions	13
What's New	14
Who should read this guide	15
Additional Resources	16
How to get help	17

Overview

This document is the main reference source for the Nortel Contact Recording System. It explains the capabilities of the system and how to plan, design, install, configure and maintain the system. Appendices provide:

- a technical reference
- trouble-shooting tips
- a reference guide to alarms raised when things go wrong
- the recorder control protocol

Definitions

Throughout this guide, the term CS 2x00/DMS switch applies to the following switch types:

- Digital Multiplex Switch (DMS)
- Communication Server 2000
- Communication Server 2100

Note: The Meridian SL-100 is not supported.

What's New

In 6.01

Release 6.01 provides the following new or enhanced features:

- Simplified and improved fault tolerant configurations
- Nortel Contact Recording Desktop application - allows users to control recording from their PC
- Post-call tagging - allows users and applications to amend call details after the call has completed.
- Call Recording Card can be used alongside other recording methods
- MARP/MADN supported on TDM sets

In 6.5

Release 6.5 provides the following new or enhanced features:

- Support for the latest version of Quality Monitoring and the new Enterprise Reporting
- A centralized licensing model on the Nortel Contact Recorder for the secondary TDM Contact Recorders. This licensing simplification capability reduces time for installation and configuration of the Nortel Contact Recording and Quality Monitoring system along with discontinuing the breakout of IP versus digital licensing – there is no longer any distinction.

In 6.5.1

Release 6.5.1 provides the following new or enhanced features:

- Support for Nortel CS2x00 and DMS switches
- Recordings can be controlled from IP phones
- Agent log ins can be determined at startup without the agent having to log off and on again
- More than two DN keys can be recorded per phone Support for S.E.R. Davox and Avaya auto-dialers (optional license required for the latter two)

ATTENTION

Release 6.5 is intended to support both CS1000 and CS2x00/DMS systems. However, the initial Release has only been tested and certified on CS2x00/DMS systems.

Who should read this guide

This guide is intended to be used by:

- Pre-sales Systems Engineers developing system topologies and designs
- Professional Services staff installing and deploying systems
- Systems Administrators
- Support personnel

The reader is expected to be familiar with:

- System administration of Microsoft Windows servers
- TCP/IP Networking and Voice over IP (VoIP)
- Nortel Contact Center systems operation and administration tasks

Additional Resources

If your recording system includes any of the optional components you will also need to refer to the manuals for these components. These include:

Nortel Quality Monitoring User Import Guide
Nortel Quality Monitoring Forms and Evaluations Guide
Nortel Quality Monitoring Migration Tool Guide
Nortel Quality Monitoring Server Infrastructure Guide
Nortel Quality Monitoring Configuration Guide
Nortel Quality Monitoring Installation Guide
Nortel Enterprise Reporting Custom Reports Integration Guide
Nortel Enterprise Reporting Data Dictionary
Nortel Enterprise Reporting Quality Monitoring Meta-Model Guide
Nortel Enterprise Reporting Report Description Guide
Nortel Cognos 1.1.4 Installation Guide.
Nortel TDM Recorder Installation Guide
Nortel TDM Recorder System Administration Guide
Nortel TDM Recorder System Infrastructure Guide
Nortel Viewer Installation and Administration Guide
Nortel Viewer User Guide
Nortel Viewer Quick Reference Guide
Nortel Archive Manager Installation and Administration Guide

End users of the Nortel Contact Recording System should refer to:

Nortel Contact Recording Search and Replay User Guide

You may also wish to refer to the following Nortel publications:

Nortel Contact Center - Manager Meridian Link Services Interface Specification
Nortel Contact Center - Manager Symposium Event Interface Guide
Nortel CS1000-CS2000 VoIP Solution and Configuration Guide
Nortel Network Interface Specification NIS Q218-1 SCAI (Switch-Computer Application Interface)
Nortel Linkplexer Installation and Configuration Guide
Nortel IP Phones Description, Installation, and Operation
Nortel Call Recording Card Planning, Installation and Administration Guide

How to get help

This section explains how to get help for Nortel products and services.

Finding the latest updates on the Nortel Web site

The content of this documentation was current at the time the product was released. To check for the latest updates to the Nortel Contact Recording and Quality Monitoring documentation, go to <http://www.nortel.com/documentation> and navigate to the Contact Recording suite.

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is the Nortel Support Web site:

<http://www.nortel.com/support>

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software and related tools
- download technical documents, release notes, and product bulletins
- sign up for automatic notification of new software and documentation
- search the Support Web site and Nortel Knowledge Base for answers to technical issues
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the Web site below to obtain the phone number for your region:

<http://www.nortel.com/callus>

Getting help from a specialist by using an Express Routing Code

You can use an Express Routing Code (ERC) to more quickly route your call to the appropriate support specialist. To locate the ERC for your product or service, go to:

<http://www.nortel.com/erc>

Getting help through a Nortel distributor or reseller

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

Chapter 3

System Overview

In this chapter

Introduction	20
Recording Options	21
Server components	29
Optional Server Applications	30
End-User tools	33
Component Co-residency	35
Limitations of this release	36

Introduction

This chapter describes the major components of the Nortel Contact Recording system. It describes the Nortel Contact Recorder (which is a mandatory component) and the optional components.

The Nortel Contact Recording system is a comprehensive recording suite designed to provide Nortel customers with world-class call recording, storage and retrieval for the two major categories of recording applications:

- Bulk Recording—recording (typically) all calls from specific Directory Numbers (DNs) or Position IDs and retaining these for a specified period of time to meet a regulatory or business risk management requirement or to provide evidence in case of future disputes or complaints. This is restricted to voice recording only.
- Quality Monitoring—sampling and assessing a small proportion of calls, and using the results to assess performance, coach staff and identify process improvements. This can include both voice recording and screen content recording.

Recording Options

The Nortel Contact Recording system provides more than one way to capture voice recordings. You should choose the most appropriate capture technology depending on your recording requirements and switch configuration. The following sections describe the recording options and indicate when they should be chosen.

Duplicate Media Streaming over IP

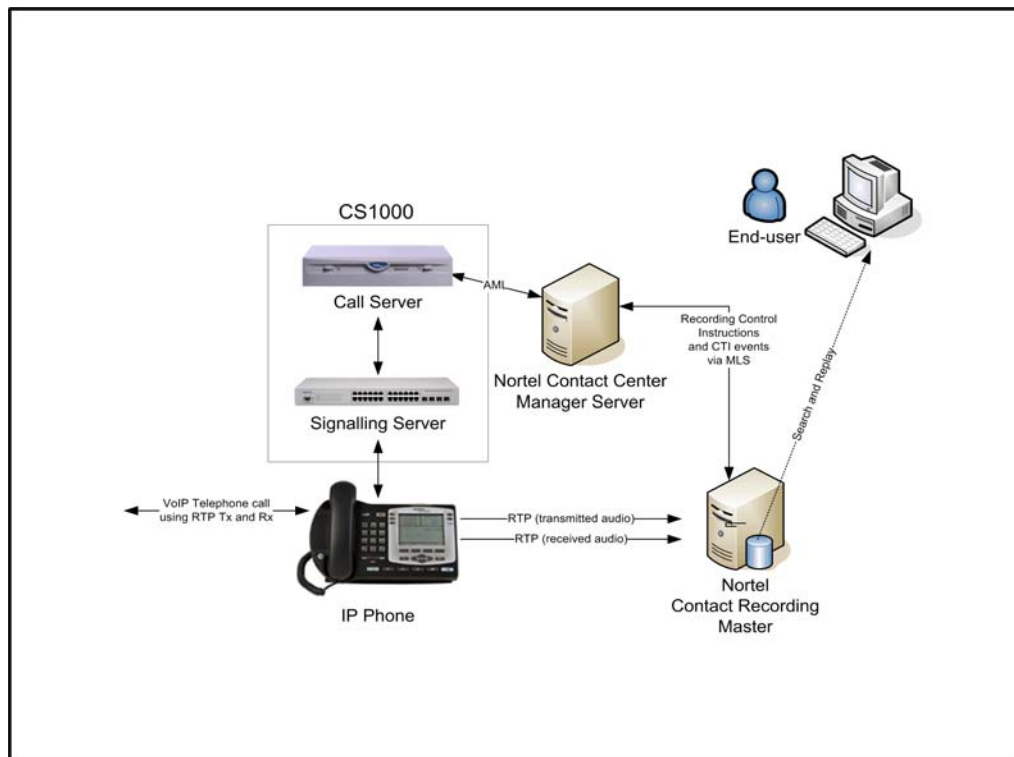
This mechanism overcomes the difficulties inherent in passive-tap IP approaches and allows greater flexibility in the location of recorders as well as increased capacity and reliability of recorders. It requires only a standard 100Mbps full-duplex Ethernet card in the recorder. It can be used on any type of switched Ethernet system, as it does not require port mirroring.

This is the preferred method of recording and should be used where possible as it provides the simplest, most flexible and usually the most cost effective approach to recording. In this approach, the recorder instructs the telephone system to stream a duplicate copy of the audio directly to it over IP.

CS 1000 Systems

Here, the audio is streamed by the IP phone itself; this approach is only available for systems using Phase II (or later) IP phones. The recorder sends instructions via a Meridian Link Services (MLS) interface as shown in the illustration that follows.

Duplicate Media Streaming in CS 1000

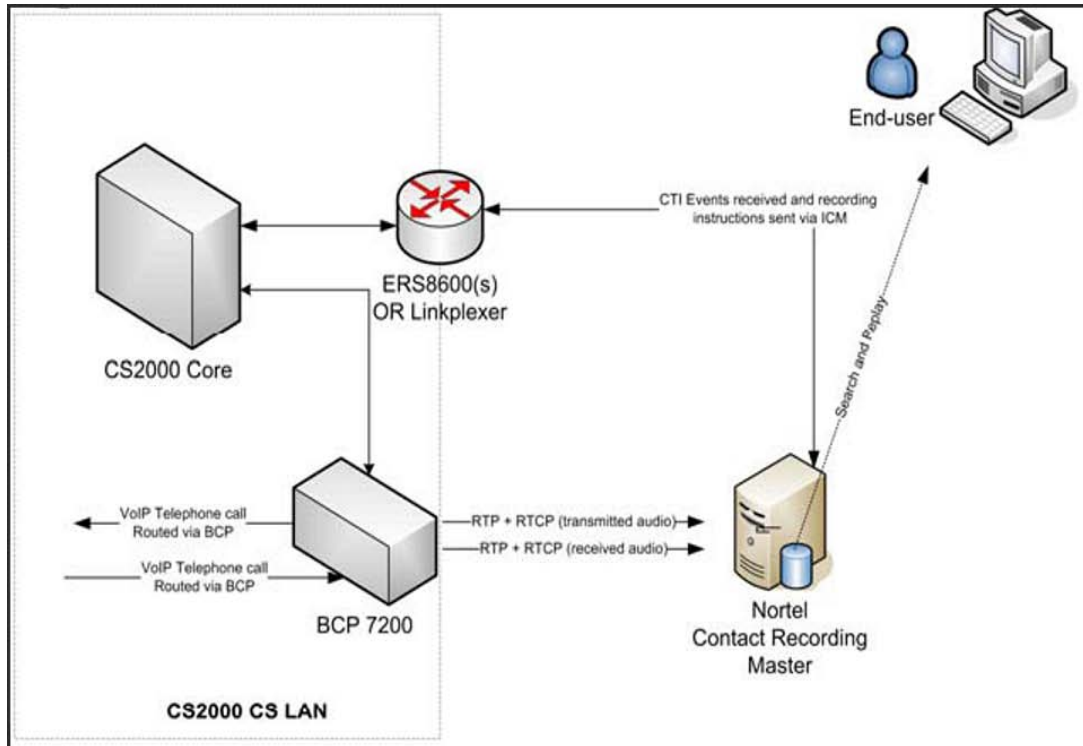


CS 2000 Systems

CS2x00 switches

In systems that use Border Control Point (BCP) 7200s, these devices can replicate the IP streams going to and from a particular phone - regardless of the type of telephone in use. The recorder sends instructions via an Intelligent Call Management (ICM) interface as shown below.

Duplicate Media Streaming in CS2x00



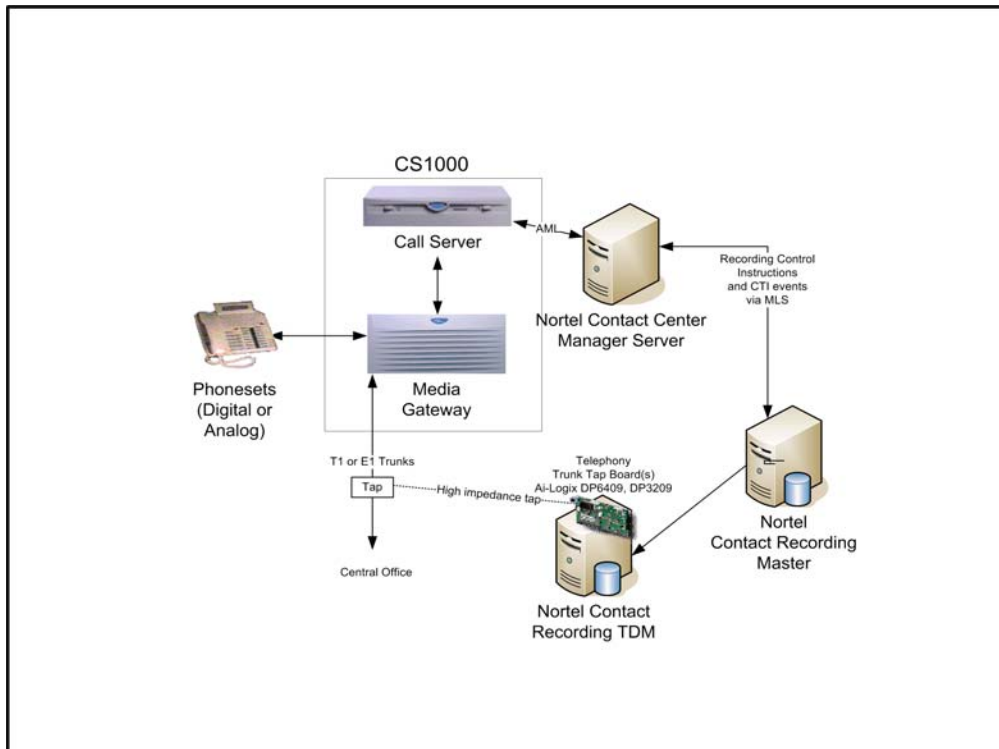
Trunk-side tap

Where the bulk of telephone sets are not IP, or the number of trunks carrying recordable calls is limited, tapping into the trunks may be appropriate. Using E1 or T1 passive tap cards, Nortel TDM Contact Recorders can record any of the time slots as required. One or more TDM recorders are controlled by the Master recorder as shown in the following figures.

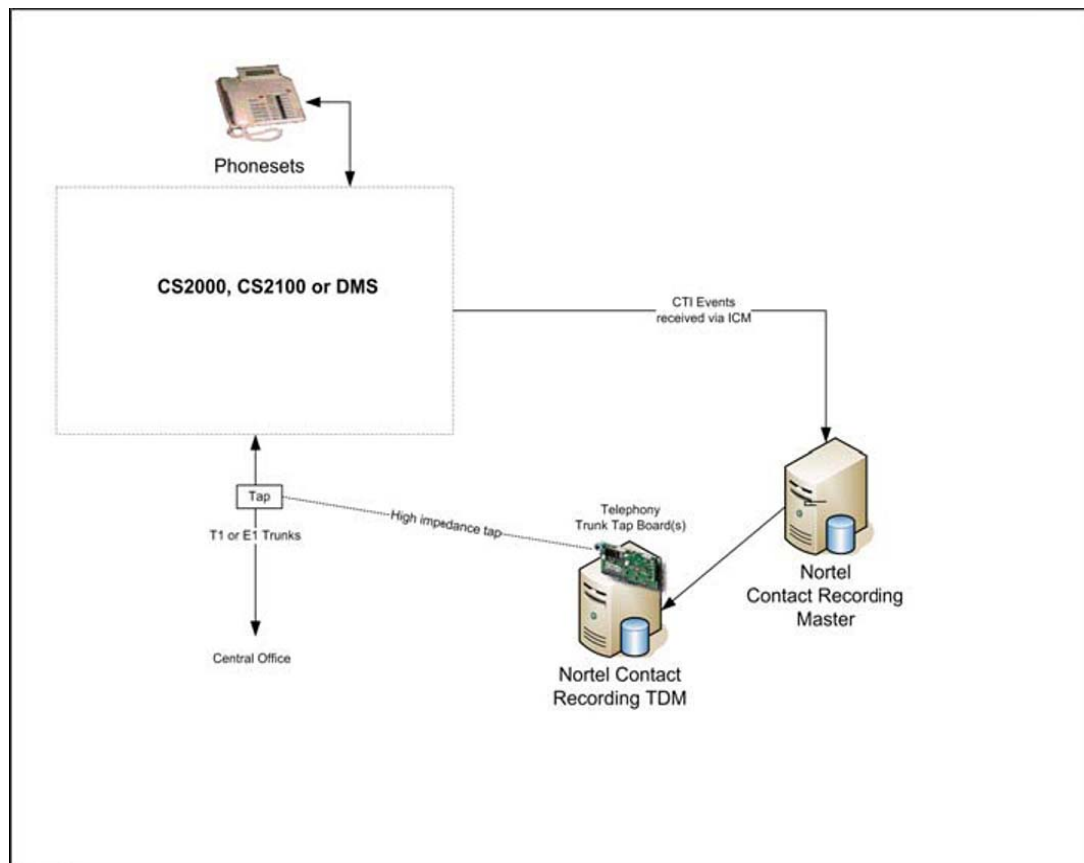
Note: Internal calls cannot be recorded using this approach.

Note: In Trunk-side tap recording a Nortel Contact Center Manager Server is required.

Trunk-side Recording on CS 1000



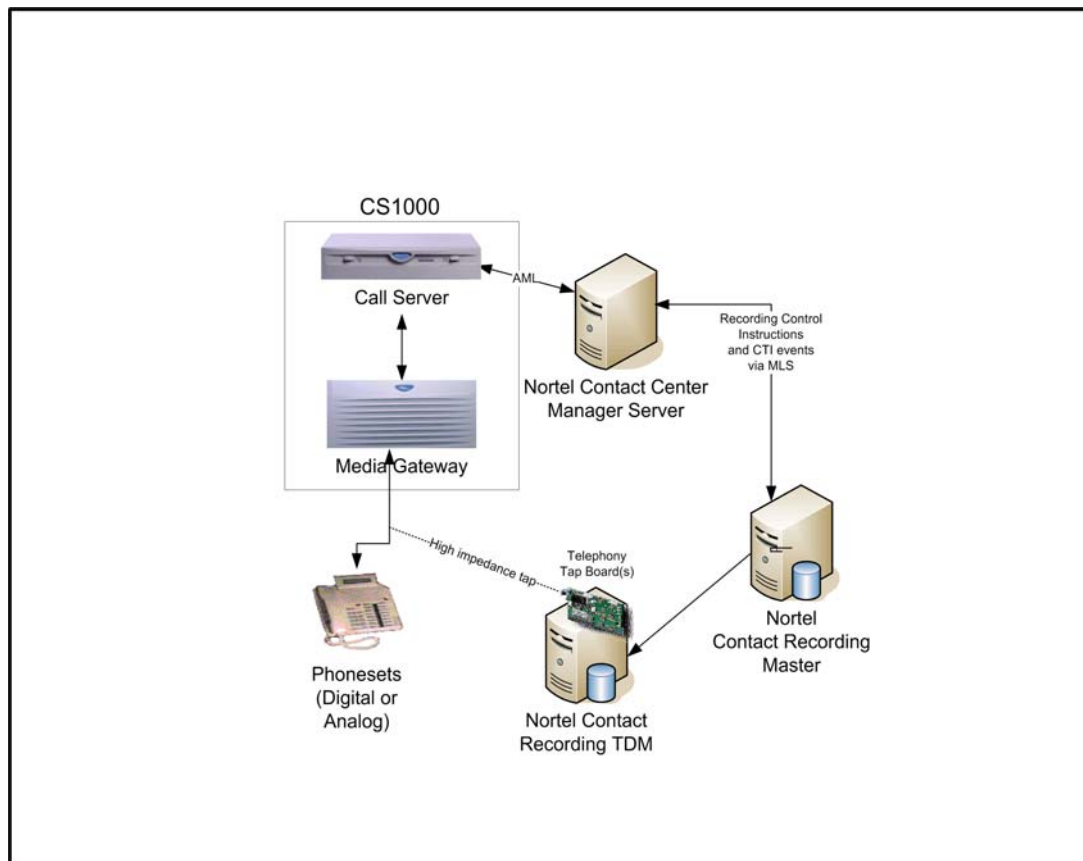
Trunk-side recording on CS2x00 and DMS switches

**TDM Station-Side Tap**

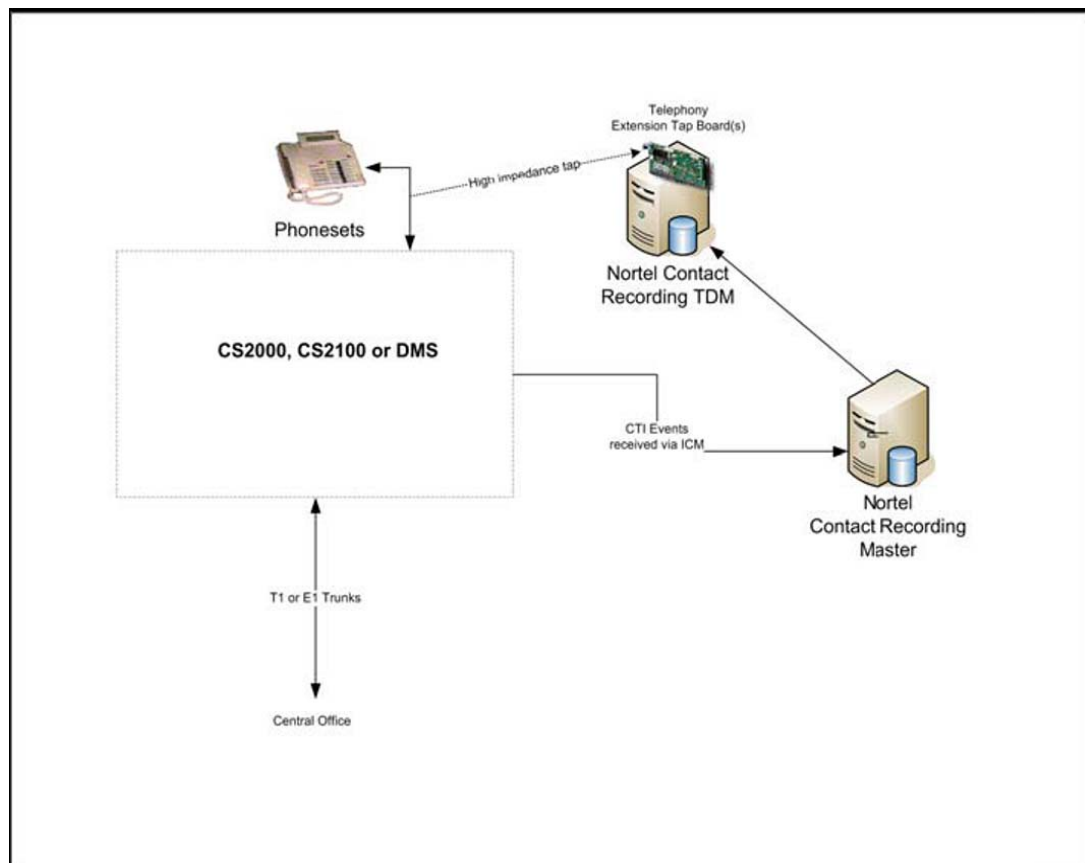
Where the telephone sets are digital and you only need to record a limited number of telephones, tapping into the extensions may be appropriate. Using digital extension tap cards allows a Nortel TDM Contact Recorder to access the audio passing to or from the tapped telephones. The following figures show this topology.

Note: In Digital Extension Tap recording a Nortel Contact Center Manager Server is not required, but is often used.

Digital Extension Recording on CS 1000

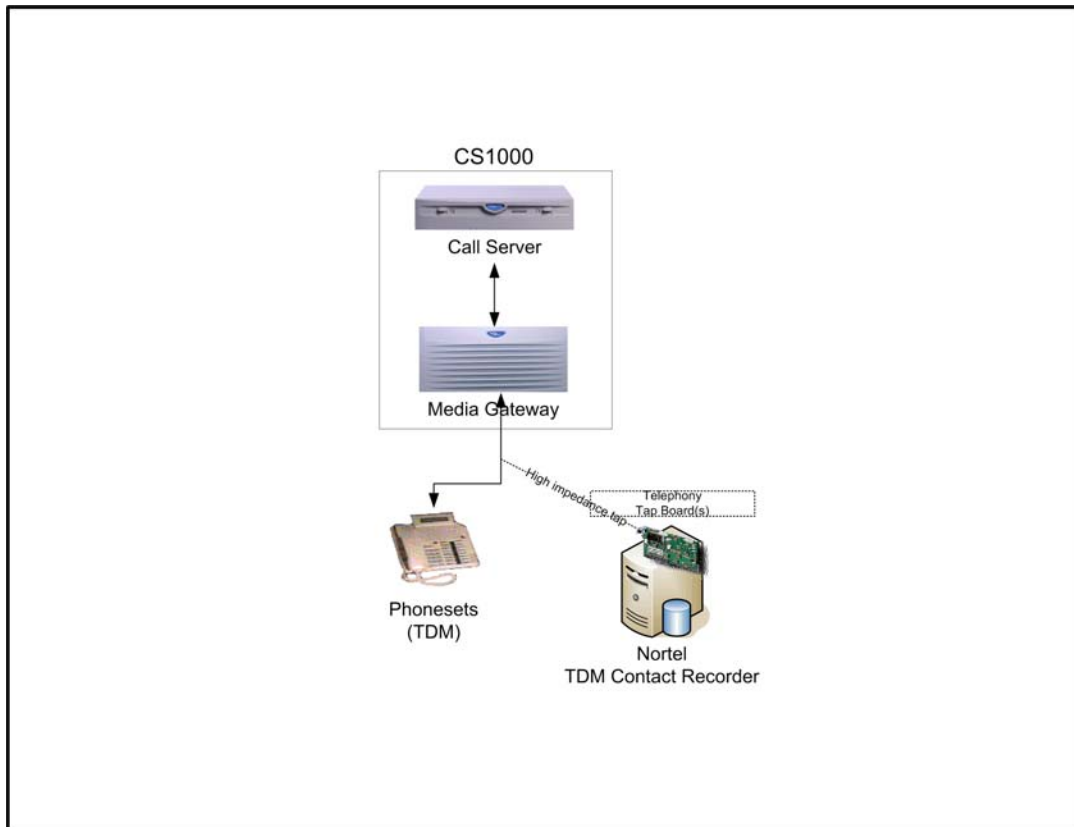


Digital Extension Recording on CS2x00 and DMS switches



As with trunk-side recording, the TDM recorder is usually controlled by the master recorder, which connects to the appropriate CTI feed (MLS for CS 1000 and ICM for the CS2x00 and DMS). However, this mode of recording can also be deployed in a standalone fashion. The following figure shows this mode of operation in a CS 1000 environment. In this mode of

operation a Nortel Contact Center Manager Server is not required. Where it is provided, full tagging is provided in the call recording details. If there is none, a limited amount of tagging is derived from the D-channel of the phoneset signalling path. (Tagging is never derived from the T1 D-channel.)



Call Recording Card

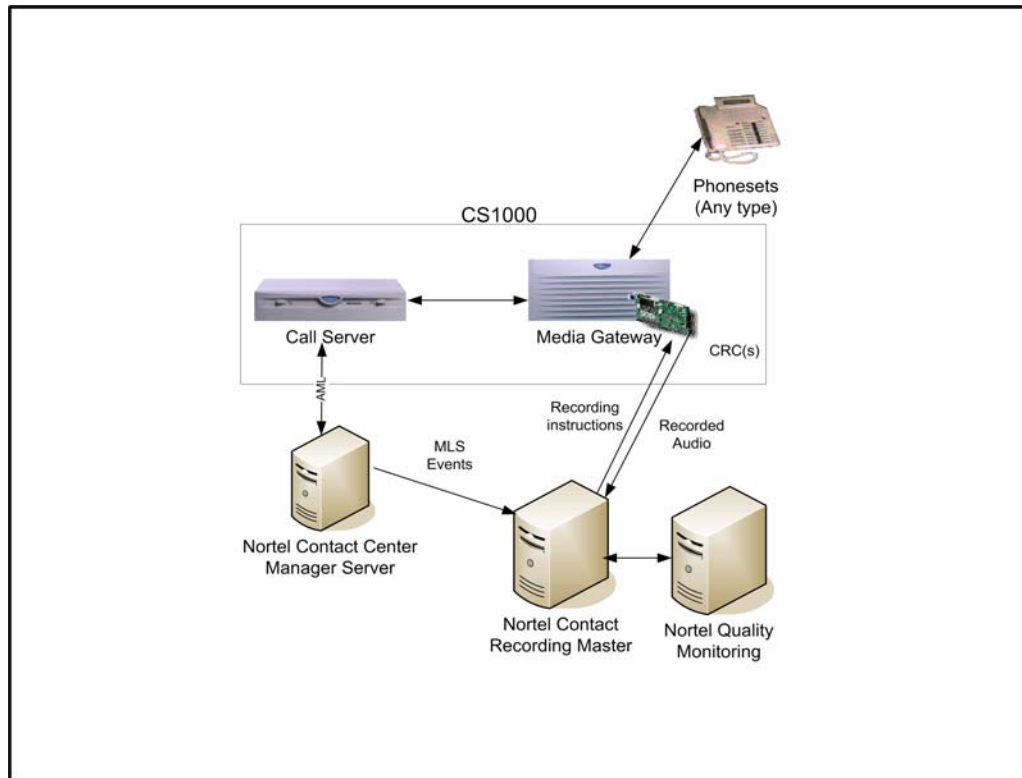


CAUTION:

Nortel switches support many different types of extension. Check the TDM Recorder manuals to confirm precise models supported.

Note: This recording method is only available on CS1000 not CS2x00 or DMS switches.

Where a relatively small number of concurrent recordings will be made across a large number of extensions and/or trunks, it can be appropriate to tap into the audio within the switch using a Nortel Call Recording Card. Each card can record up to 16 simultaneous calls but can only record call center positions. The card sends a voice recording to the recorder's disk over an IP connection. Up to 120 channels (on 8 cards) can be supported on a single recorder – subject to constraints within the switch. The figure below shows this approach.



For more information on the Call Recording Card, refer to the *Nortel Call Recording Card Planning, Installation, and Administration Guide*.

Server components

Every Nortel Contact Recording system must contain one server configured as a Nortel Contact Recording Master. This master server can make bulk recordings itself, using the Duplicate Media Streaming recording option.

You can extend the scope of the system by adding additional optional server applications in order to:

- perform quality monitoring and screen recording
- record different types of phonesets
- provide centralized shared search and replay
- provide centralized archive facilities

These optional server applications normally require their own physical server, but may sometimes be installed together on the same server. See [“Component Co-residency” on page 35](#) for details. All of the applications in the suite require Windows servers.

Note: This Guide is the detailed reference for the Nortel Contact Recorder only. This component can record voice sent to it using Duplicate Media Streaming. It can also act as the Master – controlling other recorders that provide additional capacity or supporting alternate recording approaches.

Each of the other components has a corresponding guide as detailed in [“Additional Resources” on page 16](#). Refer to the specific guide for more detail on a particular component.

Nortel Contact Recording Master

In most small to medium-sized (up to a few hundred channels) Bulk Recording systems, one of these applications provides the entire recording and replay system (as shown in [“Duplicate Media Streaming over IP” on page 21](#)).

In larger systems (where a single physical server is not powerful enough), you should install multiple instances of this application on different physical servers, each providing a subset of the system’s overall functionality. The Nortel Contact Recorder can:

- connect to the Nortel telephony system via MLS or ICM (as appropriate) and control all voice recordings (only one instance, the “Master,” can do this at any one time)
- record and store telephone calls using Duplicate Media Streaming over IP
- archive the recordings it makes to a local DVD+RW drive
- provide basic search and replay services to users connecting via their browser
- provide voice recording services to the Nortel Quality Monitoring application
- control other IP recorders, TDM recorders or Nortel Call Recording Cards.
- control other Nortel Contact Recorders – known as Slaves
- be controlled by another Nortel Contact Recorder – i.e. act as a Slave
- act as a warm Standby to a Nortel Contact Recording Master

Optional Server Applications

Nortel Quality Monitoring Application

This application provides the features needed to automate your agent quality assessment process, including:

- Design of evaluation forms
- Various call selection methods
- Screen content recording and storage
- Performance recording and reporting

From Version 6.5 onwards you must install the Nortel Quality Monitoring software on a separate physical server.

See the Nortel Quality Monitoring guides listed in [“Additional Resources” on page 16](#) and [“Quality Monitoring” on page 108](#) for how to integrate it into the overall system.

Nortel Contact Recorder TDM (Time Division Multiplexed)

This application provides Bulk Recording capabilities for customers whose telephony systems do not support the preferred Duplicate Media Streaming recording mechanism. This recording application supports a range of special circuit boards (available from Nortel) that allow it to record TDM calls by tapping across trunks or phonesets (non-IP). The recorder scales from 8 to 360 channels in a single server, depending on hardware constraints.

In most cases, the TDM recorder(s) will be under the control of a Nortel Contact Recording Master, as shown in [“Trunk-side Recording on CS 1000” on page 23](#) and [“Trunk-side recording on CS2x00 and DMS switches” on page 24](#).

However, where no MLS link is available, a standalone TDM recorder can perform extension-side recording as shown at the end of [“Trunk-side recording on CS2x00 and DMS switches” on page 24](#).

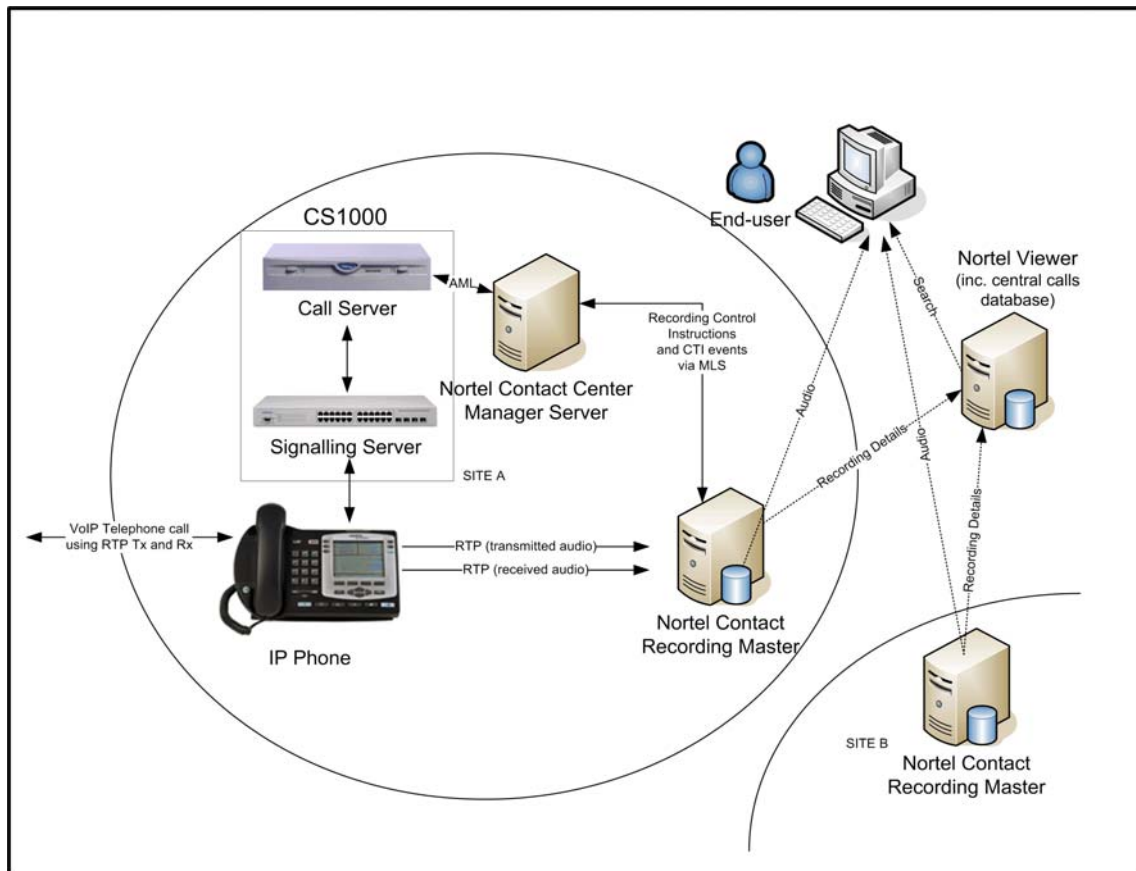
See the TDM guides listed in [“Additional Resources” on page 16](#) for full details of this component and [“Installing Nortel TDM Contact Recorders” on page 73](#) for how to integrate these recorders into the overall system. Note that this recorder does not include an integral search and replay application. You must use the Viewer application with Nortel Contact Recording TDM.

Nortel Viewer

Although the Nortel Contact Recording Master application includes search and replay facilities within it, these are limited to searching for calls made by that recorder. If you have more than one recorder, you will probably want to be able to search for and replay a recording, regardless of which server recorded the call.

Nortel Viewer is required for Nortel TDM.

In this case, you may install Nortel Viewer on an additional server and configure each of your recorders to copy the details of its recordings to the database on this server. The database holds detailed information on all recordings including where the audio content is stored (for example, either on individual recorders or archived offline). The following figure shows a typical CS 1000-based system, using Nortel Viewer to provide access to recordings from two independent recorders.

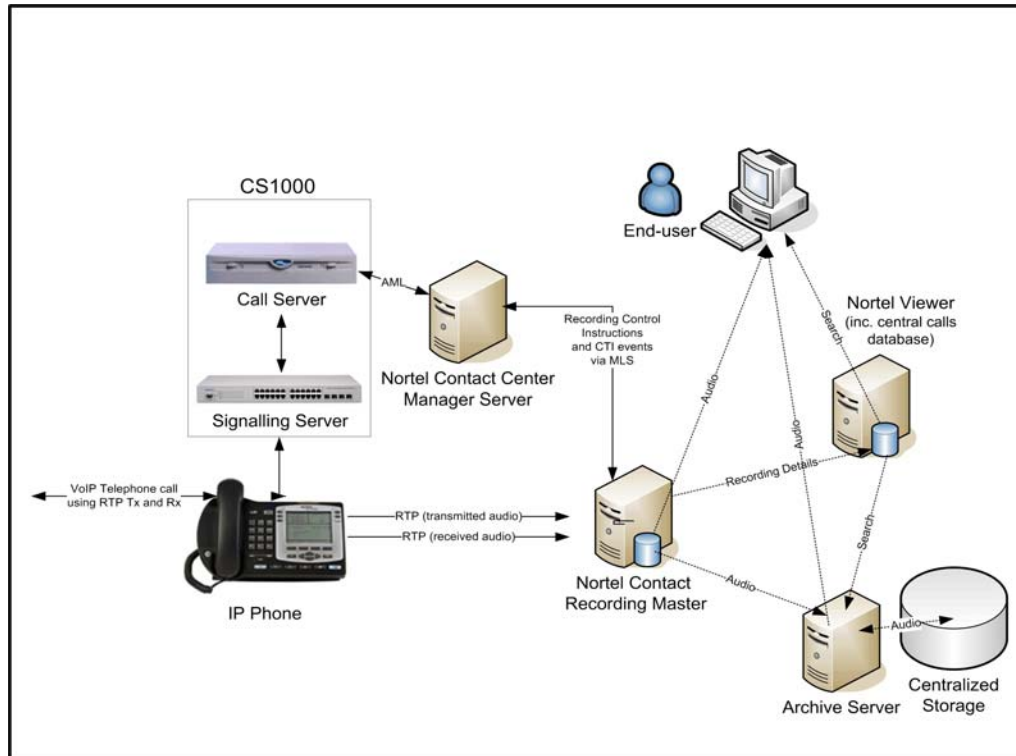


You can install Viewer on the same server as a TDM recorder as long as your total channel count does not exceed 360 and you do not intend to keep more than 10 million recordings in the database.

See *Nortel Viewer Installation Guide* for full details of this component and [“Installing Viewer” on page 76](#) for how to integrate this application into the overall system.

Archive

The Nortel Contact Recording Master can archive the recordings that it makes itself via a single, locally connected DVD+RW drive. If you need more sophisticated archival – from multiple recorders to a common destination, such as a Network Attached Storage (NAS) device or of selected recordings only, you can deploy the Archive Manager application on a separate server as shown below.



See *Nortel Archive Manager Installation and Administration Guide* for full details of this component and [“Installing Archive Manager” on page 79](#) for how to integrate this application into the overall system. Note that you must first deploy Viewer in order to use Archive.

External Interfaces

In addition to the data provided by the MLS link, you may wish to control and/or tag your recordings with details from other CTI feeds or application interfaces. These may include third party systems and/or your own in-house applications. Appendix D, “Recorder Control Protocol,” provides more details.

End-User tools

To access the recordings held in the system, users have a variety of options.

Bulk Search and Replay

Users search for and replay bulk recordings using a browser-based application. They can search for calls based on a range of criteria, including:

- date/time range
- parties on the call
- call duration

The application provides a standard set of search parameters and result columns which users can customize to suit their own requirements.

There are two search and replay applications:

- one integral to the Nortel Contact Recording Master application (see *Nortel Contact Recording Search and Replay User Guide*).
- one used in larger systems and described in [“Nortel Viewer” on page 30](#) (also see *Nortel Viewer Installation Guide*).

Quality Monitoring

Supervisors and quality assessors use a web application to evaluate recordings – using both voice and screen content where available. They can assess and review calls with their staff as well as analyze and report on the results of assessments.

Audio is replayed via the desktop PC’s sound card.

Live monitoring of audio and screen content is only supported when recording is performed using a Nortel Call Recording Card. In this configuration, audio is forwarded via the user’s telephone set.

Nortel Quality Monitoring Search and Replay User Guide provides full details of the Nortel Quality Monitoring application.

Contact Recording Desktop (CRD)

This is a very simple desktop application that lets users control recording of a DN or Position ID line that they are using alongside the PC on which they are running this application. The application typically shows as an icon in the tool tray. Users can then use the right-click menu or the restore the main window to:

- Start or stop recording
- Request that a recording is deleted or retained
- Tag a recording with additional details

Note: Users with IP phones can perform the first two tasks directly from keys on their phone if the 6.5.1 service update is installed.

[“Contact Recording Desktop \(CRD\)” on page 145](#) describes how to configure and use this application.

Administration Tools

As the suite is designed specifically for Nortel systems, much of the complexity associated with generic recording systems has been removed resulting in a system that is easy to configure and maintain. The recorders are administered via a web interface. The detailed use of this interface is the subject of later sections in this guide.

Component Co-residency

A single server IP recorder of up to 180 channels (codec dependant) will support the co-existence of the following application and components:

- Nortel Contact Recording Master
- IP Recorder
- Postgres Database
- Viewer X Search and Replay application
- Custom adapter (Unify component) – if applicable

See [“Recording Capacity” on page 47](#) for more details about the codec dependencies.

A single server TDM Recorder of up to 360 channels will support the coexistence of the following applications and components:

- Nortel Contact Recording Master (without IP Recorder)
- TDM Recorder
- Database
- Viewer
- Custom adapter (Unify component) – if applicable

These components can reside on their own server platforms if the size of the solution dictates such a configuration or if circumstances make a different configuration desirable. For example, you might have an SQL server farm or enterprise instance where you want to locate the database component. For additional information about supported component deployments, see [“Topologies” on page 52](#).

Limitations of this release

This section notes known limitations of this release.

International Support

Nortel Contact Recording is provided in English only.

CS 1000 Systems

Beep tone

Beep tone is only supported in Duplicate Media Streaming recording modes. It is not supported in any of the TDM recording modes.

Number of Recordable Line-Keys per TN

Recording is triggered by events received over the MLS interface. (This requires that the DN appearances to be recorded can be monitored via MLS and hence must have their AST flag set). There is a limitation of two such flags per TN. This means that the system can record a maximum of two line appearances on each TN. For more information on AST flags, see *Contact Center, Communication Server 1000/Meridian 1 and Voice Processing Guide*. (However, where a DN appears on multiple keys on a TN, setting the AST flag on any of these allows calls to be recorded regardless of which key is used.)

ATTENTION: If you have the 6.5.1 service update installed the limitation of two flags per TN no longer applies. In 6.5.1 you can record multiple line appearances on each TN.

MARP/MADN

Multiple Appearance DNs (“MARP” and “MADN”) can only be recorded when in Bulk Recording mode in a knowledge worker environment. These are not supported by the Quality Monitoring application, or the Nortel Contact Center environment.

Recording of calls made from one instance of a number to another line key on the same number are NOT supported. The CSTA computer telephony model which underpins the call state tracking cannot handle the same address being involved in two separate connections on the same call.

CS2x00 and DMS Switches

Beep-tone

This is not currently supported.

MARP/MADN

Recording of calls made from one instance of a number to another line key on the same number are NOT supported. The CSTA computer telephony model which underpins the call state tracking cannot handle the same address being involved in two separate connections on the same call.

Chapter 4

Planning and Prerequisites

In this chapter

Introduction	39
Recording Requirements	40
Storage Requirements	44
Server Platform	47
Network Issues	49
Nortel Contact Center prerequisites	50
Topologies	52
Integrating with other systems	58

Introduction

There is no one “right” order in which to plan a system. A number of the requirements and prerequisites are inter-dependent and it may be necessary to iterate through this section several times, refining your plans each time. This section will guide you through:

- identifying what is to be recorded, the options for doing so and the relevant license requirements for the preferred option
- determining the storage needed to hold your recordings
- sizing the servers needed for each application
- quantifying the network bandwidth needed

You can then determine an appropriate system topology.

Recording Requirements

This manual only considers audio recording load. For information on recording screen content, please refer to the Nortel Quality Monitoring documentation.

What is to be recorded?

The first task in designing any recording system is to define what is to be recorded. This is often driven by the reason for wanting the recordings.

If you need to record all of the calls taken by specific Directory Numbers (DNs), then you require Bulk Recording.

If, however, the end goal is to assess the quality of your interactions with customers, then see the Nortel Quality Monitoring guides listed in [“Additional Resources” on page 16](#) to determine how you will use the Quality Monitoring system to control recording. From this you will be able to determine the number of concurrent audio recording “channels” required to support the Nortel Quality Monitoring application.

How can it be recorded?

Audio can be recorded in a variety of ways according to the technology you have deployed and the topology of your network. Several modes of recording are supported: Duplicate Media Streaming over IP, passive tap traditional and conferencing methods.

It is possible to mix these approaches within a single system to give the optimal recording solution for a wide range of topologies and technology mixes. See [“Recording Options” on page 21](#) for an overview of these different recording methods.

Note: The preferred recording method for all types of recording is Duplicate Media Streaming but alternate approaches are supported. These options are described below in descending order of preference.

Duplicate Media Streaming

This approach requires no additional hardware in the recorder and provides the most effective means of recording.

You can use this option for Bulk Recording or Quality Monitoring if both of these requirements are met:

- your Nortel system meets the prerequisite requirements for Duplicate Media Streaming as shown in [“Nortel Contact Center prerequisites” on page 50](#).
- the required bandwidth is available between the Nortel Contact Recorder(s) and the media duplication points. These are the IP phonesets in the case of CS1000 and the BCP 7200s in the case of CS2x00.
- The recorder can be used with either G.711 (A- or μ -law), or compressed G.729A data streams - the latter with or without Voice Activity Detection (VAD).

The G.729A streams use much less bandwidth to the recorder – and also allow the recorder to support more channels because it does not have to compress the audio before storing it. However, the phone system will always stream packets to the recorder in the same format that it is using on the telephone call being recorded. You therefore may wish to consider changing the audio codec used in order to reduce traffic to the recorder – even though there is no need to reduce traffic over the route of the call itself.

Bandwidth from CS 1000 IP Phone

Note that a phoneset using bandwidth of X kbps to make a phone call will require an additional 2X kbps (twice X) for the streams being copied to the recorder. This results in a new total bandwidth of 3X kbps (three times the bandwidth of the unrecorded call) from the phone being recorded.

The recorder can have multiple NIC cards. This allows the recording traffic to be segmented from the CLAN.

Bandwidth from CS2x00 Nortel BCPs

Each call recorded in this way requires twice as much bandwidth between the BCP and recorder as is used between the BCP7200 and the phone being recorded.

Call Recording Card

Up to 8 Call Recording Cards may be installed in a CS 1000 switch – subject to card-slot availability and other limitations as described in *Nortel Call Recording Card Planning, Installation and Administration Guide*. This option has a limited capacity and uses up card-slots within the Meridian chassis. Each card is capable of recording 16 calls concurrently – regardless of the type of phoneset being used. It can only record call center positions, not ordinary DNs. It should therefore be considered where Quality Monitoring of non-IP agent phonesets is required. It is also required for live monitoring.

Call Recording Cards stream audio to the Nortel Contact Recording Master using the FTP protocol.

You can use this option for recording if all five of these requirements are met:

- the CS 1000 can accommodate the required number of cards,
- the required bandwidth is available between the CS 1000 and the recorder,
- not more than 120 recording channels are required,
- the CS 1000 has sufficient conference capability,
- you only need to record call center agent positions.

Note: Each channel on the Call Recording Card requires 3 conference ports on the CS 1000. Smaller CS 1000s have a limit of 96 conference ports and can therefore support a maximum of two cards.

Note: If a supervisor is already observing an agent when the recorder attempts to do so via the Call Recording Card, the quality recording will fail and no audio will be stored. Screen capture will continue.

“Traditional” or Passive Tap TDM Recording

If you require Bulk recording of non-IP phonesets, or are using a purely TDM switch, calls can be recorded using third party telephony cards housed in a PC chassis and physically wired across either the phonesets or the incoming T1 or E1 trunks.

This approach is rarely suitable for Quality Monitoring unless 100% bulk recording is also required. The need to dedicate a recording channel, to wire the recorder to each phoneset or trunk and provide bandwidth between recorder and Quality Monitoring application normally makes it an expensive option in comparison to Nortel Call Recording Cards.

See *Nortel TDM Recorder System Infrastructure Guide* for more details of this recording method.

Note: Trunk-side recording is not well suited to Quality Monitoring applications. Internal calls cannot be recorded and this makes it difficult to assess agent quality.

How will we record it?

Having determined the options open to you for recording the required calls, you must determine which method, or combination of methods to use. Wherever possible, you should attempt to use Duplicate Media Streaming. The tables below show the preferred recording methods, and the network load and requirements for each of the recording methods.

Reason for recording	Duplicate Media Streaming	Call Recording Card	Passive Tap TDM
Bulk Recording	Preferred	Not recommended	Only where necessary
Quality Monitoring	Preferred	Good	Only where necessary

Network Requirements	Duplicate Media Streaming	Call Recording Card	Passive Tap TDM
IP Network Bandwidth per Bulk Recording channel	Equivalent of additional 2 x VoIP voice calls per recording channel between phoneset (CS 1000) or BCP (CS2000) and recorder.	Approx. 100kbps between the card and the Nortel Contact Recording Master.	0

Network Requirements	Duplicate Media Streaming	Call Recording Card	Passive Tap TDM
Network Bandwidth per Quality Monitoring channel	As above	Approx 100kbps between the card and the Nortel Contact Recording Master.	G.711 tap ~150kbps G.729 tap ~20kbps Between TDM recorder and Nortel Contact Recording Master.
Quality of Service (QoS) required for above bandwidth	Same QoS as voice calls	Data QoS. Uses FTP over TCP hence retries on dropped packet.	Data QoS normally acceptable.

Taking the above factors and the potential location(s) of your recorders into consideration, you must determine how many channels of each type of recording you wish to deploy and on which site.

Licenses Required

Having identified your recording channel requirements, calculate your license requirements as follows:

1. One Bulk Recording channel license per concurrent recording that can be made.
2. One Quality Monitoring license per agent phoneset that you wish to record for quality monitoring purposes.

Storage Requirements

Having determined the type, size and location of your recording capacity, you must now determine how much storage is required within the system. Storage requirements of many terabytes are not uncommon.

Storage is required for:

- the operating system and applications installed on each server
- the audio content of recordings
- the database holding the searchable details of these recordings

In each case you should consider requirements locally at each recorder and centrally.

To do this, you will need to know:

- how many recordings will be made on the recording channels already identified (typically expressed in channel hours per day). In other words, how many hours of audio you expect to record on each recorder every day.
- how long you wish to retain recordings (typically expressed in days).
- the average duration of a call (typically expressed in seconds).

Storage at Each Recorder

In addition to the operating system, installed software and its configuration data, each recorder stores:

- details of the recordings it has made in a local database
- the Bulk Recordings it has made as files on its hard disk

In all cases, the system automatically notes the location of the recordings so that when a user wishes to replay a call that is no longer in local online (disk) storage, the application prompts them to insert the appropriate removable media (if any).

Each recorder type differs slightly in how it manages this storage and how much storage is used per call. The Nortel Contact Recorder stores recordings as follows:

Duplicate Media Streaming Bulk Recording

Bulk recordings are stored in G.726 compressed form at 16kbps (if received as G.711) or as a pair of G.729 files (totaling 16kbps) if received as such from the telephony system. This allows for high volumes of recordings to be stored on the available disk space.

Nortel strongly recommends RAID arrays or fault tolerant Storage Attached Network (SAN) devices for online storage of recordings on the recorder platform.

The recorder automatically manages the available recording storage space. This is used as a circular buffer providing instant access to the most recent recordings and deleting the oldest, as space is required for new recordings.

Rather than storing bulk recordings on RAID arrays in each recorder, many customers prefer to use Storage Attached Networks. These must be connected directly to recorders.

Hierarchical File Storage (HFS) Systems and Network Attached Storage (NAS), however, can only be supported via the separate Archive application.

The table below summarizes the requirements for Bulk Recording using Duplicate Media Streaming to a Nortel Contact Recorder.

	Details of Recordings	Content of Recordings
Stored	In local database	Stored as WAV files on local disk in a hierarchical folder structure
Purged	Nightly, after user defined period (default 60 months)	100 at a time as disk space is needed for new recordings
Volume	Approximately 2KB x recordings/day x days retained.	Approximately 7.2MB per channel hour of audio (G.726 mono or 2 x G.729 files) 7.2MB x channel hrs/day x days retained
Location	D:	F:
File System	NTFS	NTFS
Type	RAID 5 recommended. Local hard drive or SAN, not NAS.	RAID 5 recommended. Local hard drive or SAN, not NAS.

Quality Monitoring

When used to provide audio recording services for the Nortel Quality Monitoring application, the Nortel Contact Recording Master only uses a small amount of local storage for voice recordings (less than 1GB). As each Quality Monitoring recording is completed, the recorder transfers it to the Quality Monitoring application's storage area.

As the volume of recordings made by a selective, quality monitoring application is normally much less than that of a bulk recording system and is comparable to the screen recording volumes, audio is normally stored in G.711 64kbps PCM format (approximately 27MB per channel hour).

This application also has to store:

- screen content recordings
- the agent configuration and evaluation data

See the Nortel Quality Monitoring documentation for the storage requirements for the Quality Monitoring application.

Central Database Storage

You must deploy Nortel Viewer for search and replay if any of the following apply:

- you have more than one recorder (of any type) and wish to search and replay from any recorder through a single query.
- you anticipate more than five concurrent users of the integral search and replay application on a Nortel Contact Recording Master.
- you are using any Nortel Contact Recording TDM servers.

If you deploy Nortel Viewer, you will need to size the storage it requires in accordance with *Nortel Viewer Installation Guide* to hold the call details from all the recorders that are contributing to it.

Archive Call Storage

Where you wish to retain calls for longer than it takes to fill the hard disk storage on a recorder, two options are available:

- connect a DVD+RW drive to the recorder. All recordings made on the recorder will automatically be archived to the removable media. This requires only 1GB of buffer space on the recorder. It is suitable for systems recording less than 4GB per day.
- add Nortel Archive Manager to the system. This application supports selective archival of recordings to multiple destinations. See *Nortel Archive Manager Installation and Administration Guide* for guidance on sizing of the storage for such systems.

Backup Storage

See [“Backup/Restore” on page 115](#) for a discussion of Backup and Restore options. You should determine whether additional storage space is required in your corporate backup system to accommodate the new recording system.

Server Platform

Having decided the total recording capacity at each of your locations, you must translate this into one or more server platforms capable of handling the load identified.

Dedicated server(s) must be provided with no other applications running on them.

Disk Partitioning and RAID

You should partition the disks of all servers so that the operating system and recordings storage are both separated and secure. See [“Disk Storage” on page 66](#) for more details. The C drive should be RAID 1 and other drives should be RAID 5.

Recording Capacity

The table below shows the server types that are used as benchmarks when assessing the Nortel Contact Recording server’s performance. The actual performance depends on the type of recording and codecs in use.

Server Type	Minimum specification
A	2.8GHz Xeon (hyper-threading) processor 500MHz front side bus 512K of L2 cache 1GB RAM Hard disk at least 7200rpm. RAID strongly recommended. Dual 100Mbps full duplex Ethernet NIC ports DVD+RW Drive required for local archiving.
B	As A but dual processor

Bulk Recording

The following table shows the maximum bulk recording channels supported on a single recorder of type A or B, for each of the supported codecs and for the most common Real Time Protocol (RTP) packet intervals.

Using	Interval	Type A	Type B
G.711	30ms	85	145
	20ms	75	125
G.729A	30ms	165	250
	20ms	125	180

Quality Recording

The following table shows the maximum quality recording channels supported on a single recorder of type A or B.

Using	Interval	Type A	Type B
G.711	30ms	100	120
	20ms	75	120
G.729A	30ms	32	60
	20ms	30	60
Call Recording Card	N/A	120	120

Network Issues

In planning the network that will support your Nortel Contact Recording system, you must consider:

- the additional load imposed on the network
- the IP ports used – so that firewalls can be configured appropriately
- Network Address Translation (NAT) issues

Load

You must design your network topology to accommodate the additional traffic created by the recording system. See the table in [“How will we record it?” on page 42](#) for details of the bandwidth required by each type of recording channel.

TCP/UDP Ports Used

The components of the system use a number of IP ports to communicate:

- between each other
- to the Nortel CTI Server (Contact Center Manager Server in CS 1000 systems and the ICM connection point in CS2x00 and DMS systems)
- to the Duplicate Media Streaming devices (phoneset in CS 1000 and BCPs in CS2x00 systems)

[“IP Recorder Interfaces” on page 165](#) provides a diagram and table listing all of the interfaces to and from the Nortel Contact Recording software. Your network and firewalls must be configured to permit traffic to pass over these links.

Network Address Translation

The IP address of a Nortel Contact Recorder is sent to the Nortel telephony system as part of the Duplicate Media Streaming command. It is therefore essential that when the IP phoneset or BCP transmits to this address, the packets are routed correctly to the recorder. The recorder must therefore be visible to the IP phones or BCPs on the IP address that it uses itself.

Nortel Contact Center prerequisites

CS 1000 Systems

To use the Nortel Contact Recording system you will need:

- CS 1000 Release 4.5 or higher
- adequate AST ISMs provisioned to ensure that all phonesets you wish to record can be “mapped”.
- The latest patches for CS 1000, available via ESPL under Multimedia PEP Tools (www.nortel.com/espl)

Note: Even if you are recording trunk-side with TDM recorders, the system still monitors the phonesets you wish to record (not the trunks). You therefore require as many AST ISMs as you have phonesets to be recorded.

Note: The only exception is when you have no Contact Center Manager Server and are using extension side tap.

To use Duplicate Media Streaming you will also require:

- SCCS 5.0 or CCMS 6.0 or higher
- Nortel IP Client Phase 2 sets loaded with firmware that supports Duplicate Media Streaming.

Finally, review the table below to make sure that parameters are set correctly.

Setting	Description	Value
ISAP	Integrated Services Digital Network/Application Protocol (ACD messages sent across the ISDN/AP link).	Default=NO. Set to YES only for Meridian Mail applications. Hence for AML/ELAN messages it should remain NO.
SECU	Security for Meridian Link applications.	When set to NO, the host computer must specify both the TN and DN of the associate set in connect, answer and release messages. For AML/ELAN messaging this should be set to YES.
IAPG	Meridian Link Unsolicited Status Message (USM) group. IAPG assigns AST DNs to a status message group defined in LD 15. These groups determine which status messages are sent for an AST set.	The default Group 0 sends no messages, while Group 1 sends all messages. For AML/ELAN messaging it is better to set it to 1.
ICRA	IP Call recording allowed.	Set to YES.

CS2x00 and DMS Systems

NOTE FOR NORTEL - PLEASE CHECK AND CORRECT AS REQUIRED.

CTI Connection via ICM or Linkplexer 6.0

If the phones to be recorded are already controlled and/or monitored by an external application such as an IVR, Symposium or Genesys then a Linkplexer (6.0) must be inserted so that both the existing application(s) and the recorder can monitor the same DNs and Position IDs via the underlying ICM feed.

Similarly, if you wish to provide Master and Standby Nortel Contact Recorders for fault tolerance, you will also require a Linkplexer.

Otherwise, if the phones are not under external ACD control, and you do not require a standby recorder, the Master recorder can connect directly to ICM. In this case, you will need to create a linkset for the recorder to use. In all other cases, you must configure the Linkplexer to accept connections from the Master and, if you have one, Standby recorder.

Version Compatibility

When using a Linkplexer (see above) you must confirm that all existing applications can connect using the same SCAI Version that the recorder requires, because a Linkplexer can only support applications that all use the same SCAI Version.

For Extension-side TDM recording you require:

- SCAI Version 17 or higher (tested on SN9 and higher)

For Trunk-side TDM recording you require:

- SCAI Version 19 or higher (available on SN9 and higher) - Feature A00012526

For IP recording you require:

- SCAI Version 20 or higher (available on SN10 and higher) - Feature A00013915.
- BCP 7200 Version

Topologies

This document has so far discussed functionality in terms of “applications” without being specific as to the physical location of these. As the individual components of the recording system interconnect using IP-based mechanisms, you may distribute the components across your Enterprise’s network in a wide range of topologies.

In small systems, a single server can perform recording, storage and retrieval but in larger systems, you can separate these tasks onto different servers in a variety of ways as discussed below. A number of the basic topologies have already been shown in the diagrams of [“Recording Options” on page 21](#). The following paragraphs define the rules under which each of these basic topologies can be used and introduce the more advanced topologies required for larger and more fault tolerant systems.

Bulk Recording System

At its simplest level, a Nortel Contact Recording System consists of a single Windows server running the Nortel Contact Recording software and configured as a Master. This application provides:

- system administration functions via a browser
- voice recording using Duplicate Media Streaming from IP Phonesets (CS 1000) or BCPs (CS2x00)
- integration via Meridian Link Services (MLS) on CS 1000 systems OR Intelligent Call Management (ICM) on CS2x00 systems for real-time control and tagging of recordings
- integral search and replay capabilities.

See the diagrams [“Duplicate Media Streaming over IP” on page 21](#) for this basic Bulk Recording Topology

For most small to medium sized bulk recording requirements, this single server is all that is required.

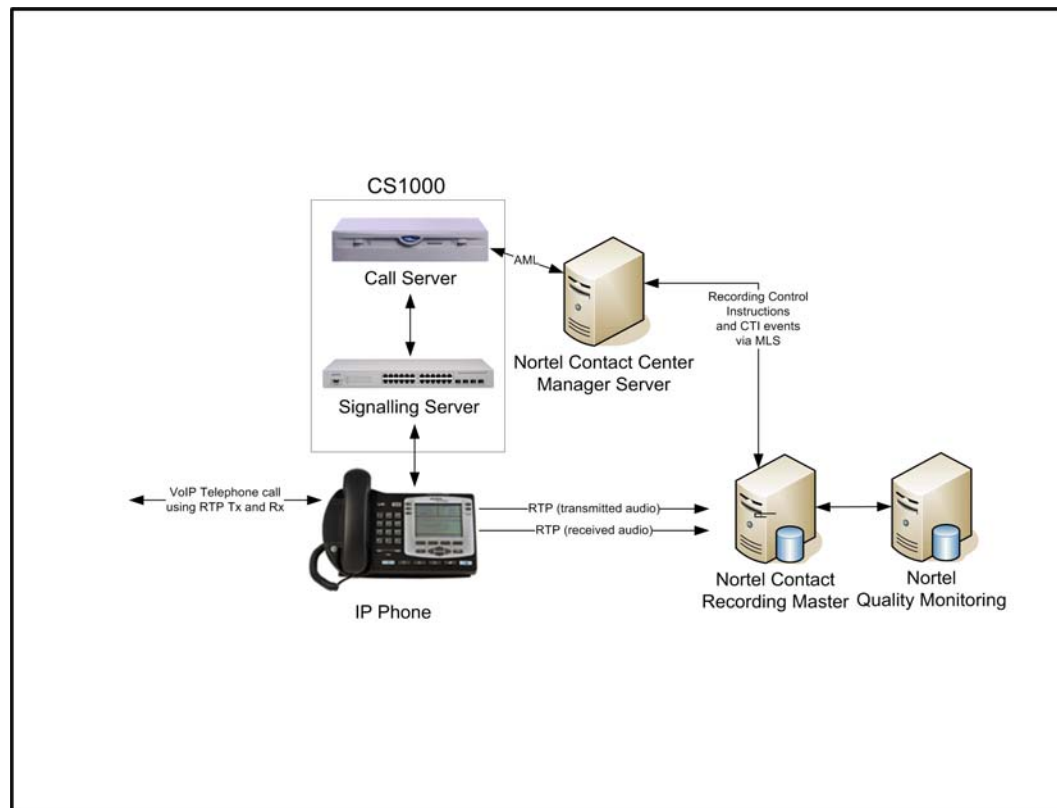
Quality Monitoring System

When Nortel Contact Recording is used for Quality Monitoring, an additional server is required to run the Nortel Quality Monitoring software application.

While the underlying Nortel Contact Recording Master provides the voice recording capabilities of the overall system, this optional application adds:

- evaluation form design
- various call selection methods
- screen content recording and storage
- agent performance recording and reporting

The Nortel Contact Recorder continues to provide the voice recording in this case – but passes the completed recording files over to the Quality Monitoring server's file-share at the end of each recording.

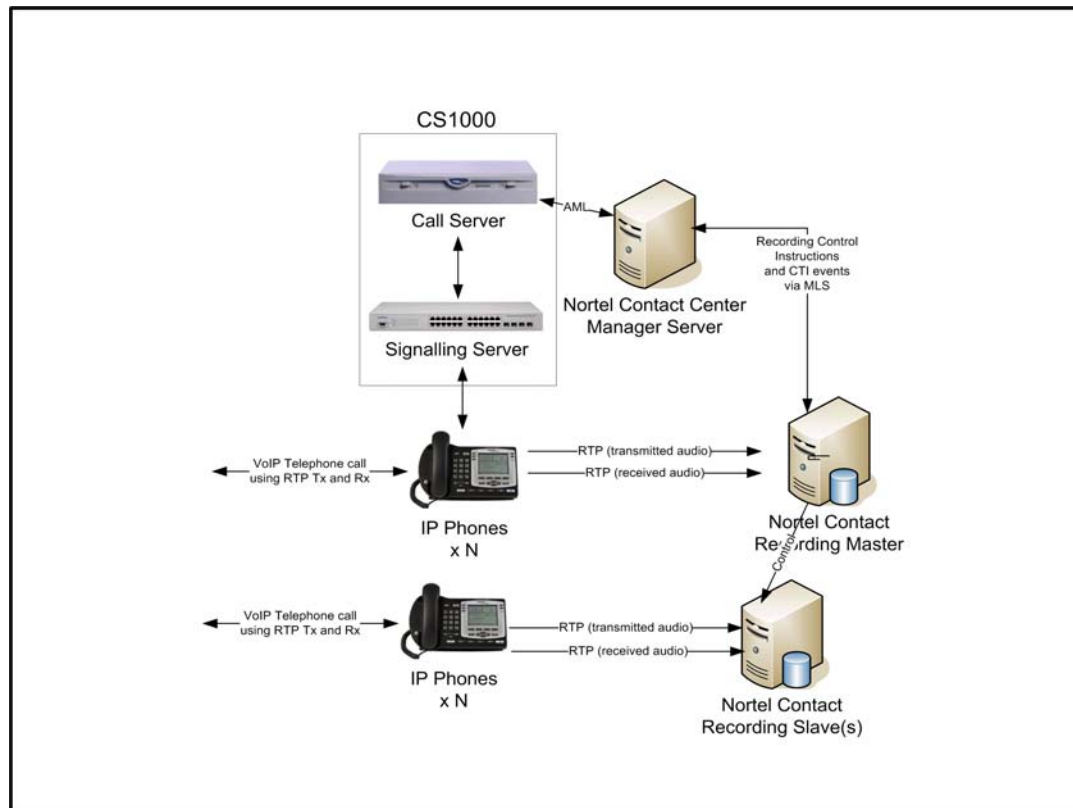


Large Bulk Recording Systems

Master/Slave Recorders

Where your recording load exceeds the capacity of a single server, or where a distributed topology is more appropriate, you can split the control of recording from the actual recording of the audio stream.

In such cases, the “Master” recorder is connected to the appropriate CTI feed and is aware of the recording rules – and of the type and locations of the other, “Slave” recorders as shown below.



The Master recorder communicates with each Slave via a TCP/IP link. It instructs the slaves to tag the required data/voice streams with the details it learns from the CTI link. The slaves can be additional Nortel Contact Recorders for Duplicate Media Streaming capacity or can be Nortel Contact Recording TDM servers for traditional recording. The Master may also perform some Duplicate Media Stream recording itself if required.

Recorder Type and Location

You may distribute these recorders across your network. They can be of different types as required by your equipment profile and network topology.

For example, if you wish to record calls on an overseas site to which you have limited bandwidth, you can opt for:

- IP Streaming Recording on the remote site and overnight archival to central site
- trunk-side recording across all sites

Each option has pros and cons according to your corporate strategy and existing infrastructure.

High Availability Systems

Because the recording system is based on industry standard PC hardware, you can spend as much or as little as you like on fault tolerant hardware to increase the reliability of each server. Nortel recommends that you use RAID disk arrays, redundant power supplies and fans as a matter of course.

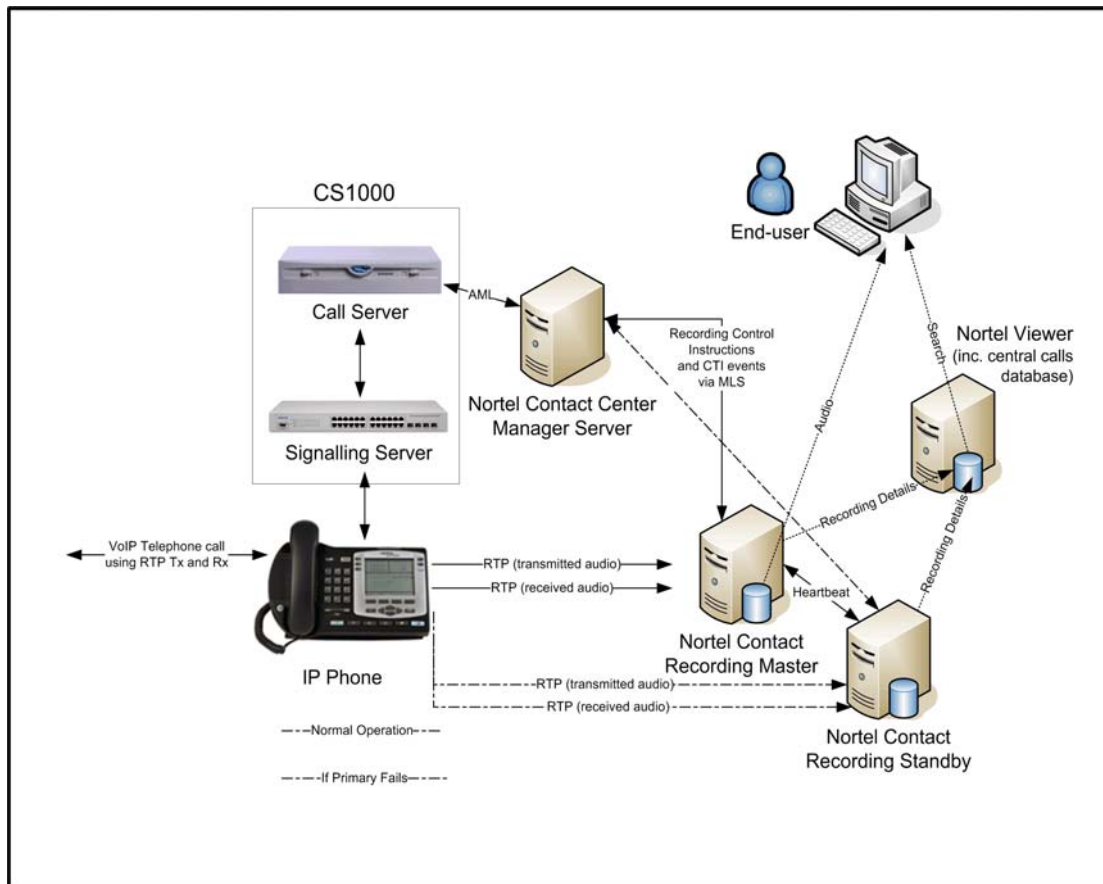
With the basic topologies described so far, the system handles the most common failure scenarios as follows:

- for an MLS failure the system connects with a backup link (if configured).
- If two IP addresses are configured in a single ICM Link Set, both will be used if available. Should one fail, the recorder will continue to use the remaining one.
- the system automatically repairs failure of any internal connections. The system attempts to recover after 2 seconds, then 4, 8, 16 and 32 seconds later before settling at attempts being made once a minute.
- if a slave recorder fails, the master recorder will attempt to reassign its recordings to ports on other recorders in the same “pool”.

However, should you wish to invest in a very high availability system, several options, described in the following sections are supported.

Master/Standby Recorders

You can install and configure a Standby recorder to “shadow” the recording Master. The standby copies configuration details automatically from the primary via a fault-tolerant TCP/IP connection between the two. Over these same links, the two recorders exchange “heartbeats” every second. The standby will take over should the heartbeat fail or should the Master request that it do so. This latter case will occur, for example, due to the Master’s disk filling or connection to the CTI link failing completely. The figure below shows a typical CS 1000 configuration.



Note: It is normal to provide Nortel Viewer so that all recordings, whether made by Master or Standby, are visible in the central database to end users. Otherwise, users would have to know which recorder was active at a given time and search against its database to be sure of finding a recording.

Note: The standby recorder only provides cover for bulk recording; it does not take over quality monitoring if the master fails.

In larger systems, where a Master recorder controls one or more “Slave” recorders, the use of a Standby recorder ensures that the Master does not become a single point of failure for the whole system. In this case, each of the slaves permanently connects to both Master and Standby. This allows the Standby to take over rapidly should the Master fail.

Fault Tolerant Pools

When using Duplicate Media Streaming, recordings can be directed toward any available recorder. Therefore a “pool” of recorders can be equipped with one more recorder than is needed for the projected loading. In this configuration, if one Slave fails, the Master recorder will reassign the telephone calls being recorded by the failed unit across the remaining slaves. The Master and standby recorders can also be in a “pool”. This means that should one of them fail, only half of the recordings are affected and are transferred to the remaining server. This gives less disruption and faster recovery.

Centralized Applications

In any system with more than one recorder, you may wish to deploy central search and replay (Nortel Viewer) and/or Nortel Archive Manager applications. In this case, each of the recorders:

- provides details of its recordings to the central database
- responds to requests from the central applications for replay of recordings that it is holding.

See *Nortel Viewer Installation* and *Nortel Archive Manager Installation and Administration Guides* for sizing and planning of these servers. Note that the recording system is designed to continue recording regardless of the state of these central servers. This means that the availability of the central applications cannot affect the reliability of the recorders themselves.

Integrating with other systems

The Nortel Contact Recording system supports integration with a wide variety of other applications including other CTI feeds, third party and customers' own applications. There are three options, depending on the complexity of the integration required.

Standardized Dialer Integrations (only available with 6.5.1 update)

An automated or predictive dialer is often used with Nortel switches. These typically require an agent to connect to a specific port on the switch for the duration of their shift. The basic recording system will see this shift as a single, long call and will not be aware of the individual customer calls that are handled by the agent. The Nortel Contact Recorder includes support for a number of commonly encountered dialers. When configured to suit your dialer and data structures, these split and tag the recordings so that each customer call is stored as an individual recording and can be found by searching for one or more data fields provided by the dialer.

See [Auto-dialer Integrations \(only available with 6.5.1 update\)](#) on page 212 for details of the current integrations and how to configure these. Note that these integrations may be charged for and licensed separately from the core recorder capacity. At present, support for the Nortel/SER dialer is included in the basic license but other dialers require an additional license.

Supplementary Tagging of Bulk Recordings

It is a common requirement to “tag” recordings with additional details, such as customer account numbers, trouble-ticket numbers etc. This information is often held in a third party or custom application and is known while the call is in progress or shortly afterwards.

The recorder implements a TCP/IP socket based interface. Applications can:

- receive events as recordings start and end
- send “tag” information to the recorder to be associated with the recording, alongside the basic call details.

Users can then search for recordings based on this enhanced set of call details.

This interface is very simple as the recorder makes contact with the application at an IP address specified in the recorder's administration pages. The recorder advises the application as recordings start and stop on each DN/Position ID. Each start message contains a unique reference (or “INUM”) to that recording. If the application wants to tag a call, it sends a “TAG” command specifying the INUM and DN/Position ID plus the data formatted as XML.

This interface is included within the core Nortel Contact Recording software and you may use it immediately. A typical tagging project requires the purchase of two to three person-days of services to learn how to interface to and control the recorder.

See Appendix D, “Recorder Control Protocol,” for details of the protocol used, associated Java APIs and example applications that are available.

Explicit External Control of Bulk Recording

In normal operation, the recorder is given some basic DN/Position ID/Agent ID rules, that it uses to determine which calls are to be recorded. However, you can build more sophisticated recording systems in which the decision to record is made by an existing call routing/handling application. By including control of recording as an integral part of call flow, such applications can, for example,

- automatically stop recording a call during security questions and resume once the customer has been validated
- automatically start recording as the agent accesses the “customer complaint” form
- add additional tagging as the agent traverses a series of menus

Applications can control recording using the same interface as described under [“Supplementary Tagging of Bulk Recordings” on page 58](#). By using the additional commands “START”, “STOP” and “BREAK”, they can override the rules applied by the administration interface.

This interface is included within the core Nortel Contact Recording software and you may use it immediately. A typical external control project requires the purchase of five person-days of services to learn how to interface to and control the recorder.

See Appendix D, “Recorder Control Protocol,” for details of the protocol used and associated Java APIs and example applications that are available.

Remote Support Strategy

Remote Support

You must arrange for remote support to allow Nortel engineers to assist with any problems that might arise.

Remote access strategies and related security policies can vary depending on the customer, therefore from Nortel's perspective it is not possible to define a single mandatory remote support configuration but instead a range of preferred remote support options that can be deployed. This applies to both the access mechanism (e.g. Contivity, VPN, Modem) or the actual remote support application (e.g. pcAnywhere). The preferred access mechanism is Contivity.

The host-only version of pcAnywhere is shipped as part of the Contact Center portfolio and is also supported on the Contact Recording and Quality Monitoring Servers.

Microsoft Remote Desktop is an alternative that is also fully supported on Contact Recording and Quality Monitoring Servers (this is usually deployed in conjunction with VPN access).

VNC is a freely available alternative to pcAnywhere.

If an alternative remote support architecture is put in place, then this needs to be mutually agreed between all parties who will need to use the remote support solution (e.g. customer, channel, Nortel support, other parties as appropriate).

As part of the site installation, an explicit check should be performed that confirms remote support is available and operational for all servers that require it.

Remote support over VPN

If you require remote technical support, your distributor or Nortel technical support staff must be able to connect remotely to your server. Virtual Private Network (VPN) is more secure than direct connected modems. While many VPN technologies and configurations are available, for remote support of Enterprise voice equipment, Nortel supports a standard with a technology based on the VPN Router 1100 (as a minimum) in a particular host-to-gateway configuration.

When you set up your VPN for remote support, follow these guidelines:

- Create a dedicated subnet for Nortel voice application servers (for example, the Nortel Server Subnet), and treat this subnet as mission-critical.
- Install, at a minimum, VPN Router 1100 (or later) version 4.8 (or later) with the modem option. Configure the modem as a user-tunnel to listen on the PSTN.
- Connect the VPN Router to the Nortel Server Subnet.
- Configure the VPN Router, as well as any network routers and firewalls, to give inbound remote support users unrestricted access to the Nortel application servers.
- Optionally, restrict remote support users' access to other subnets in your LAN/WAN. As usual, ensure that the Nortel application servers have unrestricted access to the enterprise LAN/WAN.

- Activate Split Tunneling on the VPN Router. Concerns over access into the corporate network may be alleviated by restricting access (through the VPN Router and firewalls) of remote support staff from other subnets upon logon.

Remote support over a direct-connect modem

If VPN is not available, it is still possible to provide remote support over a direct-connect modem. To facilitate remote support through a direct-connect modem the following is required:

- A modem connected to each Server
- Remote Access Services (RAS) configured on each server
- Remote Access software (e.g. pcAnywhere)

Chapter 5

Installation

In this chapter

Overview	63
Preparing your call center for Contact Recording	64
Platform Installation	66
Order in which to Install Applications	69
Installing the Nortel Contact Recording Master	70
Installing Nortel Contact Recording Slaves	72
Installing a Nortel Contact Recording Standby Server	71
Installing Nortel TDM Contact Recorders	73
Installing Nortel Quality Monitoring	75
Installing Viewer	76
Installing Archive Manager	79
Upgrading	86

Overview

Installation of a complete recording system requires:

- configuration of your Nortel telephony system, including installation of any Nortel Call Recording Cards needed
- application of all required patches to the Nortel switch and Nortel CCMS
- hardware installation of telephony cards in any recorders performing circuit-switched (non-IP) recording
- software installation on each server (see [“Order in which to Install Applications” on page 69](#))

Preparing your call center for Contact Recording

Before installing any Nortel Contact Recording components, you must ensure that your Nortel Call Center is correctly configured and, where necessary, upgraded to support the recording system. You should ensure that your call server has the latest SU and PEPs. Up-to-date information is available at www.nortel.com/espl.

Complete Prerequisites

Refer to the appropriate Nortel documentation to apply any prerequisite upgrades and/or additional licenses as detailed in “[Nortel Contact Center prerequisites](#)” on page 50.

CS 1000 Systems

Install Nortel Call Recording Cards

If you wish to use one or more Call Recording Cards to perform Quality Monitoring, you should install and configure these cards in accordance with *Nortel Call Recording Card Planning, Installation and Administration Guide*.

Determine Meridian Link Services (MLS) Connection Details

You will need the following details in order to configure the Nortel Contact Recording Master:

- the IP address of the Nortel Contact Center Manager Server
- the IP address of any fallback Nortel Contact Center Manager Server to be used in the event of failure of the default server
- your Meridian1 Customer Number (if using a multi-tenanted system)
- your Meridian1 Machine Name (if using a multi-tenanted system)

Test Phonesets

You should provide three phonesets close to the Master recorder – in the same or a neighboring rack. You can then use these to place test calls while working on the recorder.

Configure these phonesets with all of the features in use on the phonesets that you intend to record.

CS2x00 and DMS Systems

NOTE FOR NORTEL - PLEASE CHECK AND CORRECT AS REQUIRED.

ICM or LinkPlexer Configuration

If you are connecting the Master recorder directly to ICM, you must configure a Link Set for it to use. Ideally, in this case, configure two links on IP addresses that will take separate routes between the switch and the recorder. You must not use SS7 Datafill (to avoid issues with Network Node ID setting).

If using Linkplexer 6.0, the recorder will be sharing the linkset that all applications connected to the Linkplexer use. It will therefore have the same connection parameters as the other applications.

You require the following information regarding the appropriate linkset:

- IP addresses of the ICM or Linkplexer connection points
- The Network NodeID of the switch to which you need to connect
- The Service ID that is configured for this linkset
- The Service Version in use (this should be at least 19 for trunk-side TDM Recording and 20 for IP recording)
- The Business Group ID of the phones to be recorded
- The Application IDs of all other applications that are already connected - so that you can assign the recorder(s) IDs that are not already in use.
- The switch password assigned to the linkset
- The name of the linkset

CTI Configuration

The recorder must be able to observe CTI events on each Position ID and IDN that it is expected to record. It does this by issuing a "DN_ASSOCIATE" message to the switch. Therefore

- the position IDs to be observed must belong to the same Business Group ID as the recorder is configured with.
- each IDN or DN to be recorded must be configured with the Extended Call Management (ECM) option on.

Test Phonesets

You should provide three phonesets close to the Master recorder – in the same or a neighboring rack. You can then use these to place test calls while working on the recorder.

Configure these phonesets with all of the features in use on the phonesets that you intend to record.

Platform Installation

Before installing the Nortel Contact Recording (Master, Slave or Standby) software on the designated server(s), you must prepare each server as described below.

Note: For the other server components (including TDM recorders) refer to the relevant installation manual.

Operating System

Ensure that the operating system installed is:

- Windows 2003 Server, Release 2, Service Pack 2

Disk Storage

Prepare your disk storage – configuring RAID arrays and partitions as required for the application(s) you intend to install on that server.

For the Nortel Contact Recording application, prepare three partitions, shown below as C:, D: and F:. (The E: partition needs no preparation.)

- C: will hold the operating system and other tools/applications – this need only be a few GB. 10 or 20GB is recommended
- D: will hold the Nortel Contact Recording application. This will include the local call details database and should be sized at 10GB + 2GB per million recordings that you want to keep accessible in the local database.
- E: CD/DVD
- F: will hold the actual voice recordings. See [“Storage Requirements” on page 44](#) for sizing guidance.

If you intend to use a DVD+RW drive for archiving calls directly from the Nortel Contact Recorder, you must install and test your DVD+RW drive by writing a test file to the disk before attempting to use it with the recording system.

Soundcards

Nortel requires that you install a soundcard with a set of speakers or headphones in each recorder server. Please note that:

- many rack-mountable servers do not include a soundcard as standard. You will have to add one. The simplest and safest way of doing so in many cases is to install a USB soundcard.
- a number of soundcards (especially the more sophisticated ones) are not compatible with Windows 2003. Check compatibility before ordering your soundcard.

Time Synchronization

You must synchronize all servers to the same source as your telephony switch. This will minimize any time differences if you need to compare events on the telephone system with timestamps of recordings or entries in log files.

Java TimeZone (TZ) Update

All installations should include the loading of the TZ Updater patch for Java due to the government changing the date of the daylight savings time. Without this patch, java will change with the date in the code which does not match the changed date. This patch is located at http://java.sun.com/javase/tzupdater_README.html. For this patch to be successful, one must first ensure Windows hotfix KB955839 has been installed. This patch can also be found on the Windows Update Web site at <http://support.microsoft.com/kb/955839/en-us>. If this patch is not loaded the Contact Recording may lose timing with the CCMS and will report timing of the calls one hour off from actual time.

Network Connectivity

Disable Media Sensing

ATTENTION

Windows contains a “Media Sensing” feature which can cause problems for recorders. Should all NIC cards in a server lose connectivity at the same time, this feature can lead to the recorder looping with 100% CPU usage. You must disable this feature by following the instructions in <http://support.microsoft.com/kb/239924/en-us>

Domain Name Server (DNS) Entries

Ensure that the IP node names of all servers that make up the recording system are stored in the appropriate Domain Name Servers. Subsequent configuration can then be done by using the host name rather than having to use numeric addresses.

Network Routes

You should ensure that valid IP paths exist between each of the servers and from servers to those devices that use Duplicate Media Streaming. These devices are the phonesets in CS 1000 systems and the BCPs in CS2x00 environments. See “TCP/UDP Ports Used” on page 49 for details of ports used.

Fault Tolerant Paths between Master and Standby Recorders

If you are deploying Master/Standby pairs of Nortel Contact Recording Servers it is imperative that you provide two totally independent network paths between the primary and its standby. Failure to do so will leave the system vulnerable to failure should a common component in the network paths between the two fail. In such a case, both recorders will attempt to take control of all recording, with unpredictable results.

To ensure this,

- 1 Assign IP addresses in one sub-net (call it A) for the first NIC from the Master and the first on the Standby.
- 2 Assign IP addresses in a different sub-net (call it B) to the second NICs on the Master and Standby
- 3 Connect the NICs in sub-net A to one Ethernet switch and those in sub-net B to a different switch. (If you do not have two Ethernet switches you can use a cross-over cable directly between the two NIC cards)
- 4 Log on to the Standby recorder and ping both IP addresses of the Master.
- 5 Remove the NIC cable from the first NIC (sub-net A) on the Standby server. Confirm that you can only ping the Master on its sub-net B address. Replace the cable.
- 6 Remove the NIC cable from the second NIC (sub-net B) on the Standby server. Confirm that you can only ping the Master on its sub-net A address. Replace the cable.
- 7 Log on to the Master recorder and ping both IP addresses of the Standby.
- 8 Remove the NIC cable from the first NIC (sub-net A) on the Master server. Confirm that you can only ping the Standby on its sub-net B address. Replace the cable.
- 9 Remove the NIC cable from the second NIC card (sub-net B) on the Master server. Confirm that you can only ping the Standby on its sub-net A address. Replace the cable.

If any of the above tests fail, adjust your network routing and/or firewall settings until you can be sure that there are two independent paths between Master and Standby and that these are being used rather than just being theoretically available.

Fault Tolerant ICM Path (CS2x00 only)

If you are not using a Linkplexer you can create an ICM Linkset with two IP addresses. The recorder can then connect to both and tolerate network failure of either path. For this to have real benefits, you must ensure that completely separate network paths are used. This typically means providing an additional NIC in the recorder and configuring your IP sub-nets to force connectivity via different NICs. Use the same approach as described above for Master/Standby paths to ensure that the routing is correct.

Order in which to Install Applications

In many cases, the recording system will consist solely of a single Nortel Contact Recording Master server. However, in topologies that are more complex it is important that you install the basic recording infrastructure first and then layer the other applications on top. To do this, install server components in the order shown below:

- 1 Install the Nortel Contact Recording Master unless installing a TDM slave on the same machine, see [“Nortel Contact Recording Master Co-resident with TDM Recorder” on page 74](#). This master server connects to your Nortel telephony system's CTI connection (MLS) and, under normal circumstances, controls all recording. Enter your master license key into this server. Follow the procedures in [“Platform Installation” on page 66](#) and [“Installing the Nortel Contact Recording Master” on page 70](#).
- 2 Install the Nortel Contact Recording Standby if required as described in [“Platform Installation” on page 66](#) and [“Installing a Nortel Contact Recording Standby Server” on page 71](#).
- 3 Install any Nortel Contact Recording Slaves required as described in [“Platform Installation” on page 66](#) and [“Installing Nortel Contact Recording Slaves” on page 72](#).
- 4 Install any slave Nortel Contact Recording TDM servers in accordance with *Nortel TDM Recorder Installation Guide* and then configure them as outlined in [“Installing Nortel TDM Contact Recorders” on page 73](#).
- 5 Install Nortel Contact Viewer (if required) as described in [“Installing Viewer” on page 76](#). This guides you through the options you should select as you work through *Nortel Viewer Installation Guide*.
- 6 Install Nortel Quality Monitoring (if required) in accordance with *Nortel Quality Monitoring Installation Guide* and configure the Nortel Contact Recorder to support it as described in [“Installing Nortel Quality Monitoring” on page 75](#).
- 7 Install Nortel Archive Manager (if required) in accordance with *Nortel Archive Manager Installation and Administration Guide* and configure it to support the recorders as described in [“Installing Archive Manager” on page 79](#).

Installing the Nortel Contact Recording Master

The Nortel Contact Recording Master is the application that will connect to your Nortel Contact Center Manager Server (via the MLS link) and control all recording. It will typically also be performing at least some, if not all, of your Duplicate Media Stream recording.

To install the Nortel Contact Recording Master on a Windows server:

- 1 Log on to the server using an Administrator's account
- 2 Insert the Nortel Contact Recording DVD. This contains the Nortel Contact Recording and Viewer installation kits.
- 3 The installation menu should start automatically. If it does not, navigate to the CD and double-click setup.exe found in the \NCR folder.
- 4 Follow the instructions on the screen to set the path where you want to install the application. Note that this also determines the location of the call detail database. This must be installed on the D partition which must have adequate space for your call details as described in ["Disk Storage" on page 66](#).

Note: The installation process creates a local user account. This account does not have administrator privileges. By default, the account name is "postgres" and the installer chooses the password for you. You may change this password later but if you do, you should make a careful note of these details, and then configure the PostgreSQL Database service with the new password to allow it to run under this account.

- 5 If you require any of the advanced or non-standard features that are controlled by entries in the properties file, set them now. See ["Properties File" on page 139](#) for details.
- 6 Complete the system Configuration for a Master recorder server as described in Chapter 6, "Configuration" – selecting licensing option (1) in ["Licensing" on page 92](#) and setting the recorder number to 1 (unless you have multiple independent Nortel Contact Recording systems within your enterprise. In this case, set the recorder number to a unique value, higher than any previously installed recorder.)

Installing a Nortel Contact Recording Standby Server

Install a Standby server in the same way as the Master recorder (see [“Installing the Nortel Contact Recording Master” on page 70](#) – steps 1-7). When configuring a Standby server use the Standby option listed in the second bullet in [“Licensing” on page 92](#).

If the Standby is to copy the configuration of the Master recorder (the default) then you need to configure very few other details. Work through Chapter 6, “Configuration” configuring just those fields with “Edit” links next to them.

However, if you wish to configure the Standby manually so that it does not act in the same way as the Master recorder:

- 1 Add the following line to the properties file (See [“Properties File” on page 139](#) for detailed instructions)

standby.localconfig=true
- 2 Restart the Nortel Contact Recording service
- 3 Configure all settings as you would on a Master recorder.

Installing Nortel Contact Recording Slaves

Slave Duplicate Media Streaming recorders are installed in the same way as the Master recorder (see [“Installing the Nortel Contact Recording Master” on page 70](#) – steps 1-7). When configuring a Slave server use option (3) in [“Licensing” on page 92](#).

The Slave’s Administration interface only shows the settings that are relevant to a slave recorder. Work through Chapter 6, “Configuration” configuring just those fields with “Edit” links next to them.

Note: A Nortel Contact Recording TDM server acting as slave to the Master recorder is still a TDM recorder and must be installed in accordance with [“Installing Nortel TDM Contact Recorders” on page 73](#) rather than this Section.

Installing Nortel TDM Contact Recorders

Read this section first and then install the hardware and software on each TDM Contact Recorder in accordance with *Nortel TDM Recorder Installation Guide*.

You can use TDM Contact Recorders in three ways:

- as slave to a Master Nortel Contact Recorder
- as a slave, but co-resident with the Master Nortel Contact Recorder
- standalone with no CTI connection

You configure the TDM recorder differently in these three modes.

Configuring a TDM Slave to a Nortel Contact Recording Master

Do not configure the recording channel names on the TDM recorder itself. Instead, enter the details of the TDM recorder on the General Setup > TDM Tap Points page of the Master recorder's administration application. You will need to have the information of how the physical cross-connects have been made between the recorder's high-impedance tap ports and the phoneset and/or trunk cabling.

Note: The license key encryption used by the TDM recorder is stronger than normally supported by the Master. You must install a java patch on the Master first, as described in [“Installing Unlimited Strength Encryption” on page 162](#). (You should also install the same java patch on any Standby recorder.)

For each TDM recorder:

- 1 Edit the list of Slave TDM Recorder(s) shown at the top of the page. Set the IP address of each TDM recorder and assign it a Serial Number. Make sure you give each TDM recorder within your enterprise a unique serial number. Serial Numbers must be 6 digits long, beginning with 6. As the Master and Standby recorders are 890001 and 890002 you should start numbering TDM recorders at 600003.
- 2 Fill in the table indicating which physical port on the recorder has been cabled to which phoneset or trunk/loop. Follow the detailed instructions in [“TDM Tap Points” on page 98](#).
- 3 Check that the link to the recorder shows on the Recorder Status > Summary page and is UP. If it does not connect within 1 minute, check the Alarms page and correct any problems shown there.
- 4 Click "Apply Changes & Restart if necessary". This applies the appropriate channel licenses to the TDM recorders. If you have changed the number of channels on a TDM recorder, it will restart after this. This will interrupt any recordings already in progress so should be done out of hours.

Clicking this button will always send the current license details to all configured TDM recorders. Each responds indicating whether or not it requires a restart and only those that do will be restarted.

Nortel Contact Recording Master Co-resident with TDM Recorder

TDM recording systems of up to 360 channels can be configured with the Nortel Contact Recording Master on the same server as the TDM recording software. In this case, you must install the Nortel Contact Recording Master first, then Viewer and finally TDM (if required on the same server).

Note: The latest Nortel Contact Recording Coresident Patches should be installed prior to the Viewer or TDM applications.

When installing the TDM recorder you **MUST** change the port number from the default 8080 value to avoid a clash with the Nortel Contacting Recording Master. Use 8888 instead. You will then access the TDM recorder via this port and the Nortel Contact Recording Master on port 8080.

You must also specify this new port number when you enter the TDM recorder as a capture platform in the Viewer database, and when you configure the address of the TDM slave in the Nortel Contact Recording Master.

In the cs.properties file for Contact Recorder, you must add dms.maxchannels=1 for Contact Recording Master Co-resident with TDM Recorder. Please refer to [Properties File](#) on page 139 to make this change.

Configuring Standalone TDM Recorders

Because there is no Nortel Contact Recording Master in this case, you must configure the recording channel names on the TDM recorder itself.

Installing Nortel Quality Monitoring

Install and configure this application as described in *Nortel Quality Monitoring Installation Guide*.

Then, on the Nortel Contact Recording Master, complete the settings on the Operations › Quality Monitoring page as described in [“Quality Monitoring” on page 108](#).

Look on the Recorder Status › Summary page on the Master to confirm that the link between the Master and the Quality Monitoring application is UP. If it does not connect within 1 minute, check the Alarms page and correct any problems shown there.

Installing Viewer

The installation and configuration process for this server component is quite complex and has many options. The instructions below describe a basic installation approach that is appropriate for most installations. They complement the *Nortel Viewer Installation Guide* as they highlight easily overlooked items. You should print out the guide for ease of reference as you work through the installation.

Prerequisites

Before starting to install Viewer, double-check that:

- you have installed the Windows components IIS and Message Queuing services.
- Active Directory Integration is not selected.
- you are not trying to access the server using Internet Explorer 5.0 or earlier. You must use 5.5 or higher.
- you have installed the appropriate version of SQL Server - including any service packs and hotfixes specified in the Viewer manual.

Follow the *Nortel Viewer Installation Guide* meticulously. It is critical that you set up mixed mode security and note the System Administrator (sa) password. Consider using “sa” as the password temporarily and changing it once the system is fully configured. This helps support personnel access the system to address any initial setup problems you may have.

- check that all the servers in the recording system exist in DNS correctly so that you can ping each by name rather than just numerical address. You are less likely to make errors entering names than numbers. Check that you can ping the Viewer server by name from the recorders and vice versa.

Installing Viewer

You must install the application while logged in as an administrator.

Note: Ensure that you install the Core components first.

When asked for a username and password for the Viewer account, consider leaving it at the default username and setting the password temporarily to “N0rt3l” and changing it once the system is fully configured. This helps support personnel access the system to address any initial setup problems you may have.

Configuring Viewer

Follow Configuring the System in the *Nortel Viewer Installation Guide*, noting the corresponding points below as you go. These will provide a basic working setup that you can then return to as you become familiar with the application.

- 1 Using the console created above, add the local Administrator user to all four roles.
- 2 Shutdown and restart the Application Portal.

- 3 Open a browser on the server or any other networked computer and access <http://servername/witness>. If asked, log in as Administrator.
Note: If you see errors, try adding the server to your list of Trusted Sites – it is trying to download an ActiveX control to you.
Tip: You do not need to add locations at this stage.
Attention: You must use the server's hostname rather than dotted IP address (nor the name localhost) when accessing the URL and when entering the domain name as part of the username if you are prompted for username and password.
- 4 Click on the Admin tab and then add a system – with the following settings:
 - a. System Name = your server name
 - b. System Type = Contact Platform Database
 - c. Server Name = your server name
 - d. DatabaseName = EWareCalls (Case sensitive)
 - e. Location = Default Location
- 5 For each TDM recorder in your system, add a Capture Platform as described in *Nortel TDM Recorder Installation Guide*.
- 6 For each Duplicate Media Streaming Nortel Contact Recording Master, Standby and Slave, add a Capture Platform with the following settings:
 - a. Name = the Nortel Contact Recording Server's name
 - b. Capture Platform Type = Other Recorder
 - c. Machine Name=your Nortel Contact Recording server name
 - d. Location=Default Location
 - e. Contact Platform Database = the one you added in step 3 above
 - f. Serial Number = 89xxxx – (where the last four digits are the recorder number you assigned it when entering the license.)
 - g. Port=8080
 - h. URL Path=replay (not adapter/replay or retriever/replay)
- 7 Follow the section “Generating a Template”. Make sure you log in using the account and password you set in [“Installing Viewer” on page 76](#). Add the View, nortelcallsview, giving it the name NortelView (no space between), Screen Name Nortel View.
- 8 Log back in as Administrator.
- 9 Create a Basic Query. Bring up the browser on <http://servername/witness> again and this time select the Viewer tab and click on the New icon at the top left to start the Nortel Query Wizard.
 - a. Step 1/8. Select the query Nortel View that you created in step 6. Click Next.
 - b. Step 2/8. Skip this step. Click Next.
 - c. Step 3/8. Select the following fields:
StartedAt
Duration
FirstParty

OtherParty

Agent

Service

CallID

Click the box at the top right to select all fields for the details tab.

Click Next.

- d. Step 4/8. Select the order you wish the fields to be displayed. Click Next.
- e. Step 5/8. Choose StartedAt, sort descending as the default sort order. Click Next.
- f. Step 6/8. Leave the languages as the default. Click Next.
- g. Step 7/8. Set the name to Basic Query and leave the remaining fields blank. Click Next.
- h. Step 8/8. Pick an icon and set 100 maximum results. Click Finish.
- i. "Release" the Query by selecting the bent black arrow icon at top left.
- j. Use the Administration tab to make this query accessible to users.

Configuring Nortel Contact Recorder

For each Nortel Contact Recording Master, Standby and Slave, you will need to do the following to configure and test the connection.

Do not do this until you have proved that each recorder is recording calls successfully and that these are playable from the recorder's integral search and replay page.

- 1 Set the Viewer server's address in the recorder's General Setup > Recorder page.
- 2 Restart the Nortel Contact Recording service.
- 3 Check that the Link to Viewer is showing on the Recorder Status > Summary page and is UP.
- 4 If not, check the Alarms page and correct any problems showing there.
- 5 Make a new test recording.
- 6 Access Viewer using a browser and search for the new recording.
- 7 Play the recording.

Installing Archive Manager

Do not attempt to install or configure Archive Manager until you have proved that Viewer is working with all recorders.

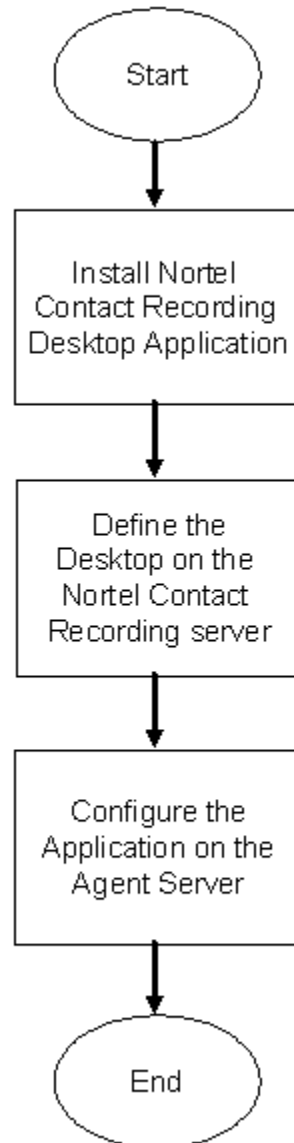
Follow the installation instructions in *Nortel Archive Manager Installation and Administration Guide*.

Because Archive Manager relies on Viewer, there is no additional configuration necessary on the recorder itself.

Installing Nortel Contact Recording Desktop (CRD)

Follow the instructions in this section to install and configure the Contact Recording Desktop on each PC that requires it. See the “Contact Recording Desktop (CRD)” section under “Advanced Configuration” for full details of functionality and configuration options.

Install Nortel Contact Recording Desktop Tasks



Install the Nortel Contact Recording Desktop application



- 1 Access the CD from the Client workstation
- 2 Open the Nortel Contact Recording Desktop Installation Folder.
- 3 Double click setup.exe.
- 4 Click OK.
- 5 Click the computer icon in the upper left corner of the screen.
- 6 Ensure that Contact Recording Desktop is selected in the Program Group field.
- 7 Click Continue. The installation will begin.
- 8 When the installation is complete, a dialog box states Contact Recording Desktop Setup was completed successfully.
- 9 Click OK.

Define the desktop on the Nortel Contact Recording server

Example Desktop showing all possible controls

- 1 Navigate to the Nortel Contact Recording server and login with a user account that has local admin privileges.
- 2 Open the dcs.xml file. The default location is
D:\ProgramFiles\Nortel\ContactRecording\properties\desktop.
- 3 In the <pcs> section, add the computer name and the DN of the phone you wish to control. Use the following format, substituting the client machine name for Computer1 and the DN for DN1. When you have completed entering client machine names and DNs, enter </pcs> as the last line entry in your list.


```
<pc name="Computer1" extension="DN1" />
<pc name="Computer2" extension="DN2" />
</pcs>
```

Repeat for each agent.

For example:

Using computer names xyzcoagttl and xyzcoagt2, and DNs 1000 and 1001 respectively, you would enter:

```
<pc name="xyzcoagt1" extension="1000" />
<pc name="xyzcoagt2" extension="1001" />
</pcs>
```

- 4 In the <udfs> section, you will define the user-definable fields. The fields are displayed on the Nortel Contact Recording Desktop GUI on the agent's PC. The format is:

```
<udf name="field header1" label="text field" type="text"> <mask>#</mask>
```

Replace "field header1" with a field name of your choice.

Repeat for each field.

Ensure you have </udfs>> at the end of your field list on the following line.

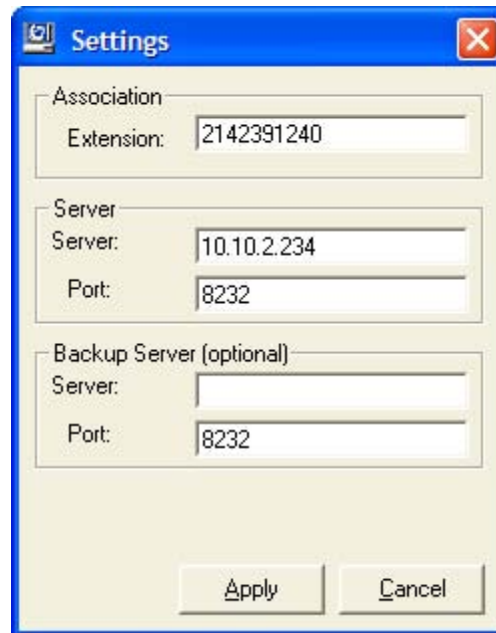
Example:

```
<udfs>
<udf name="spare1" label="First Field" type="fixed">
<entry>Fixed Text Entry</entry>
</udf>
<udf name="spare2" label="Second Field" type="text">
<mask>##/##/####</mask>
<mask>[abcd]</mask>
<mask>[!xyz]</mask>
<mask>##/##/####</mask>
</udf>
```

- 5 In the buttons section, define which buttons on the Nortel Contact Recording Desktop GUI that you would like the agent to control. There are five options: start, stop, update, delete, and retain. You control the agent's access to these by editing the mode="disabled" to mode="enabled" for the buttons you would like them to control.
- 6 Save your changes to the dcs.xml file.
The changes to the dcs.xml file take effect when you stop and then start the Nortel Contact Recording service.
- 7 Login to the Nortel Contact Recording software.
- 8 Access the Bulk Recording tab via the Operations tab.
- 9 Click on the Edit field next to the DN/PosID you have just configured.
- 10 You can choose to apply global settings to all of your agents or you can specify the parameters for each DN/PosID to give individual agents their own unique access to the level of control they have over the GUI.
 - For individual settings use the options listed under the advanced tab of each DN/PosID.
After you complete the settings for an agent, click Save to close the window.
Repeat for each agent that you want to assign individual settings.
 - For global settings, edit the fields in the Bulk Recording tab choose each of the parameters by clicking on Edit and selecting Yes or No.

Note: Settings made in the advanced tab of each DN/PosID override settings made globally.

Configure the Nortel Contact Recording Desktop application on the agent's machine

The image shows a Windows-style dialog box titled "Settings". It has a blue title bar with a minimize button, a maximize button, and a close button (red X). The dialog box is divided into three sections. The first section is labeled "Association" and contains a single text field labeled "Extension:" with the value "2142391240". The second section is labeled "Server" and contains two text fields: "Server:" with the value "10.10.2.234" and "Port:" with the value "8232". The third section is labeled "Backup Server (optional)" and contains two text fields: "Server:" which is empty and "Port:" with the value "8232". At the bottom of the dialog box are two buttons: "Apply" and "Cancel".

You will complete this procedure to configure the Nortel Contact Recording Desktop application for the agent to login to the application from their own desktop. You perform this procedure at the agent's PC.

- 1 At the Agent machine, right-click on the system tray icon and select Configure.
- 2 Enter DN number and the IP address of the Nortel Contact Recording server in the server field.
- 3 The port number is preset at 8232. Nortel recommends you use the default.
- 4 In the Backup server section, enter the IP address of the standby Nortel Contact Recording server, if any.
- 5 Click Apply.
- 6 You will be prompted to enter a username and password. Leave the default username. The password is admin, all lowercase.
- 7 After successfully saving the parameters, the login page is displayed. Click Logon.
- 8 The status displayed in the tool tip of the system tray icon will be Line Idle. Double click on the system tray icon.
- 9 The Nortel Contact Recording Desktop application will display. You can view the user-defined fields and buttons that you specified in dcs.xml file.

Configuring Record on Demand and/or SAVE keys on IP Phones (only available with 6.5.1 update)

Customers running CCSM release 7.0 and CS1L release 6.0 or higher can give users with IP phones control over recording and deletion/retention of recordings.

To use these features:

- 1** Apply the necessary CCMS licenses.
- 2** Add ROD and/or SAVE buttons to the appropriate IP phones
- 3** As you work through the following sections of this document, ensure that you set the appropriate options on [“Start recording automatically at start of call” on page 105](#).
- 4** If using a SAVE key, you must indicate that this is present on the appropriate DN/Position Ids.

Upgrading

The upgrade process is straightforward but must be performed exactly as per these instructions. Failure to do so can result in loss of data.

External Control

While the interface to external controllers should be backwards compatible with existing integrations, it is impossible to test all possible modes of working. Ideally, test the existing control scripts against a lab system running the new version. If this is not possible, consider setting up a Master/Standby pair to provide a rapid rollback in the event of problems.

Multiple IP Recorder Systems

The interaction between IP recorders changed between 6.0 and 6.01. When upgrading across this boundary, you must apply the upgrade to all Nortel Contact Recording Master, Slave and Standby recorders but this can be done in stages for large systems.

- 1 Upgrade the Nortel Contact Recording Master. If you have a Standby server, turn it off for the moment as it will not interact correctly with the new Master. If you experience problems with the Master, turn the Master off and turn the Standby on. This provides you with a rapid rollback path.
- 2 When you are confident that the Nortel Contact Recording Master is performing satisfactorily, upgrade the Nortel Contact Recording Standby and bring it back online.
- 3 Upgrade the Nortel Contact Recording Slave recorders.

When upgrading from 6.01 to 6.5, on the other hand, recorders may be upgraded one at a time if desired.

Other Nortel Components

You should upgrade Viewer and Archive Manager BEFORE upgrading your Nortel Contact Recorders.

If you have TDM recorders, you should upgrade these AFTER upgrading the Nortel Contact Recording Master (and Standby if present) that control them.



If using Nortel Quality Monitoring on systems with Slave IP recorders, you must upgrade all recorders to at least 6.01 at once - or do not use the quality monitoring application until all recorders have been upgraded

Upgrading a Nortel Contact Recording IP Recorder

- 1 Log on as an administrator
- 2 Stop the services Nortel Contact Recording and PostgreSQL Database (in that order).
- 3 **IMPORTANT:** To retain your previous configuration data, copy the \properties\.. folder to a safe location e.g. D:\upgradedata\.

- 4 Install this version of Nortel Contact Recording as described in [“Installing the Nortel Contact Recording Master” on page 70](#).
- 5 Confirm that you would like to Upgrade.
- 6 Enter the password of the postgres user (by default this will be NCR_nqm60).
- 7 Enter the name of a folder where the installer can make a backup of the database. The installer will check that you have chosen a drive with enough disk space.
- 8 If you wish to restore your previous configuration data,
 - a. Stop the Nortel Contact Recording service and the PostgreSQL Database service (in that order).
 - b. If upgrading FROM 6.0

Copy the \Nortel Contact Recording\properties folder contents over the newly installed \properties\ (Do not delete the newly installed folder for 6.5 recorder as this contains new files that you will need for the Contact Recording Desktop application).

Copy the \Nortel Contact Recording\postgresql\data folder, allowing it to overwrite any files of the same name.

Copy the Calls folder (Note this is if you plan to have the same serial number for your 6.5 recorder.)

If upgrading FROM 6.01 or higher

Copy the \Nortel Contact Recording\properties folder saved in Step 3 back to \properties, allowing it to overwrite any files of the same name.

Copy the \Nortel Contact Recording\postgresql\data folder, allowing it to overwrite any files of the same name.

Copy the Calls folder (Note this is if you plan to have the same serial number for your 6.5 recorder.)

Note: If you are upgrading to 6.5 on a different server, then copy the folders mentioned from step 8 from the older version of the Nortel Contact Recording server to the same location on the new 6.5 Nortel Contact Recording server.
 - c. Restart the Nortel Contact Recording service on the recorder server.

Chapter 6

Configuration

In this chapter

Overview	89
Accessing the System	90
Licensing	92
Security	93
General Setup	95
System Monitoring	101
Operations	103
Search and Replay	110
Backup/Restore	115

Overview

You must now configure the recording suite to suit your requirements. This section guides you through the various tasks in a logical order. You should follow its steps immediately after installation of the Nortel Contact Recording application.

Accessing the System

Before you can configure the system, you must first:

- Access the administration web-interface via its URL
- Log in

URL

To access the web interface with which you administer the Nortel Contact Recording system:

- 1 Open Internet Explorer and navigate to `http://servername:8080` – replacing `servername` with the name of the server you wish to administer.

Result: you see a login page asking you to enter a username and password.

- 2 Enter a username of your choice and leave the password field blank.
- 3 Click OK.

Note: The login page uses Java script. If you see the login page but nothing happens when you click OK, your Internet Explorer settings may be blocking this. See [“ActiveX Control Download” on page 111](#) for detailed instructions on this and other necessary settings.

Initial User Account

The application will accept any username during the first log on attempt after installation and will automatically create a local application account for you under that name and give it administrator rights.

As the password of this account has not yet been set, the web application immediately directs you to a page asking you to set the password for this account. In this instance, leave the Old Password field blank and enter a new password of your choice into the two other fields. Click OK.

ATTENTION

Make a note of this username and password otherwise you will not be able to access the web application in the future. Note that both username and password are case sensitive.

Windows Authentication

If you enter a simple username without a domain qualifier (for example, *admin* rather than *mydomain\admin*) then the account is administered by the recorder application. Administrators may reset this account's password, and the user may change their account password and log off from the application using the administration web pages.

If you specify a windows domain and username, the system will attempt to authenticate you by your normal Windows domain controller or WINS server(s). In this case, you will not see **Logoff** or **Change Password** links on the web pages presented by the recorder. This feature is also known as "Single Sign On" (SSO), as users only have to log onto their Windows workstation, but do not need to log on to the search and replay application separately. See [“Windows Domain Authentication” on page 91](#) for details of how to enable this feature.

Windows Domain Authentication

You can create local user accounts within the recorder application itself. However, it is more secure to use Windows domain accounts. You may wish to enable this feature, or even restrict access so that only windows domain accounts have access to the system.

To ENABLE Windows Domain Authentication:

- 1 Create a user account with the username in the format of ***domain\username***. For example, **CORP1\JSmith**.

Note: The username is case sensitive and must match exactly the case of the username stored in the domain controller.

- 2 Add properties to the properties file to define either your domain controller or WINS controller as follows:

sso.dc=IP address of domain controller

OR

sso.domain=domain name to use

sso.wins=IP address of WINS server to use

To ENFORCE Windows Domain Authentication only:

- 1 Enable Windows Domain Authentication as above.
- 2 Log in as an Administrator using a domain account.
- 3 On the **Security > Users** page, set **Allow local user accounts?** to **No**.

Note: If users are prompted for their domain passwords when they access the web interface, ensure that the recorder is either part of the intranet zone, or make it a trusted site and configure Internet Explorer to automatically log on to trusted sites.

Licensing

The first time you access the system, the web application will direct you to the license entry screen and you will not be able to access the rest of the application until you enter the information for the server to become a Master, Slave or Standby server as follows:

- Master: Enter a license key – which you can obtain from the Nortel Keycode Retrieval Website.
 - a. Access <http://www.nortel.com/>
 - b. Under **Support & Training** choose **On line self-service** then **Keycode Retrieval**.
 - c. In the popup window, leave **Step One** as **Global Login** and under **Step Two** choose **Meridian 1**.
 - d. Enter your Nortel username and password.
 - e. In the new window, enter the switch serial number in the **System Id/Product Id** box and click **Search**.
 - f. In the new window choose your product from the drop down list.
- Standby: Enter two IP addresses of the Master recorder, separating them with a semi-colon (one for each NIC).
- Slave: Enter the IP address of the Nortel Contact Recording Master. If you also have a Standby server, enter its address, separating the two with a semi-colon.

Recorder Number

You must enter the recorder number that this server is to take within your enterprise. Nortel recommends that you set the Master as number 1. If you have a Standby server, set it to number 2. This identifier must be unique within your enterprise as it identifies not only the recorder itself, but also all recordings that it makes and any DVD media it produces.

Reinstallation

Make a note of the license key and store it safely in case you need to reinstall the application on the same server – in which case you will be able to reuse the key. To reinstall on a different server, you will need a new key, because the MAC address, to which it is tied, will be different.

Once you have successfully entered a license key, or the recorder has contacted a Master recorder that has a valid license key, you will be able to access the other pages of the administration interface.

Security

Security of recordings is very important. Nortel Contact Recording supports the following security features for Bulk Recording:

- separate roles for administrators and replay users.
- locally administered account name and passwords.
- authentication via your Windows logon mechanisms.
- search and replay rights configurable for each user account.
- administration and search/replay access to bulk recording can be restricted to https only.
- an extensive audit trail holds details of all significant administration and end-user activity.

Note: If you have installed Nortel Viewer then you should only configure Administrator accounts on each Nortel Contact Recording server. Use Nortel Viewer to create and control end user replay rights. (Nortel Viewer provides a consolidated view of IP recordings and TDM recordings and must be used for Search and Replay if you have a mixed environment, or more than one recorder.)

Securing the System

The system automatically creates an initial administrator account as you log in for the first time. If you wish to create additional administrator accounts, you should do so now. Until you do so, the only means of accessing the system is with the initial account.

To create a new user account:

- 1 Click on System › Manage Users at the top of the Administration screen.
- 2 Click on Add User.
- 3 Enter the user's name (with domain name if using Windows domain accounts).
- 4 Check the "User is an administrator" box if you wish to grant this user administrator rights.

Note: The Comment field is for your own notes.

Tip: See ["Search and Replay Access Rights" on page 110](#) for an explanation of how to use the "Is allowed to replay calls owned by" field.

Windows Domain Accounts

If you enter a simple username without a domain qualifier (for example, "admin" rather than "mydomain\admin") then the account is administered by the Nortel Contact Recording server. Administrators may reset this account's password and the user may change their account password and log off from the application using the administration web pages.

However, if you specify a windows domain and username, the system will attempt to authenticate you via your normal Windows domain controller or WINS server(s). In this case, you will not see Logoff or Change Password links on the web pages presented by the Nortel Contact Recording server.

Use of SSL (optional)

You should consider whether you wish to enforce the use of Secure Sockets Layer (SSL). By default, users can access the recorder via http (on port 8080) or by encrypted https (on port 8443).

You can force users to use the secure https port, by including the following line in the properties file (see [“Properties File” on page 139](#) for details):

```
cs.forcesecure=true
```

When you do this, any user who attempts to access the recorder through the unsecured (http) route is automatically redirected to the secure (https) address.

The Nortel Contact Recording application is distributed with an SSL certificate that is valid for three years from the date it was issued. The certificate makes it possible to give users secure access to the server. When users access it through this secure https port, the traffic between their browser and the recorder is automatically encrypted.

However, Internet Explorer will warn your users that the name on the certificate does not match the name of the server using it. You can either advise your users that this is acceptable and should be ignored or, for greater security, you may acquire and install your own SSL certificate as explained in [“Installing a Signed SSL Certificate” on page 159](#).

General Setup

You can configure how the system makes recordings and how it interfaces with your Nortel Contact Center Manager Server. To do this, click on the General Setup tab at the top of the Administration page.

Recorder

Note: It is important that you review and change any of the settings that are not correctly defaulted.

Call storage path

You must specify the path into which the recorder will store its recordings. This should be the F drive.

Optional Local DVD+RW drive

Enter the Drive Letter of the DVD+RW drive (if fitted). Once you enter a letter, all subsequent recordings are queued for local archival to the DVD. If you intend to configure local archive, but have not yet installed the drive enter a dummy unused drive letter so that recordings are marked for archival. If you do not intend to use local archive leave this field blank.

Maximum recording segment duration (mins)

To optimize the playback experience, the recorder cuts long recordings into segments of the designated length. A typical value for call centers is 120 minutes. This is the default. However, if your switch regularly handles longer calls, you may increase this value.

Retain call details for (months)

At some point, the size of the call details database will become either unmanageable or will fill the available disk space. Specify, in months, how long the system should retain call detail records before they are purged from the system. This ensures that the database stabilizes at a finite size. Purging is carried out at 1:00 a.m. each night and does not affect recording or replay.

SNMP Read Community

See [“SNMP” on page 102](#) for notes on this setting.

IP Address to use on this server for Duplicate Media Streaming

When using duplicate media streaming you can specify which IP address (and therefore which NIC) on the server should receive the audio streams. If you leave this field blank, the recorder will default to the same NIC used to communicate with the CCMS server. To use a different NIC, specify its IP address here.

Viewer Database Server

Note: This setting is not required in a TDM-only environment.

If using Viewer for replay, set this field to the name of the EWare database server. Once you have administered this setting, the recorder queues call details to send to the database. However, it does not actually start sending them until you have subsequently stopped and restarted the Nortel Contact Recording service.

Note: If you intend to install a Viewer server and want all call details to be uploaded to it, enter a string in this field before you start recording. Do this even if the Viewer server is not yet ready. This way, all recordings' details will be queued ready for upload when the server is available. The recorder will raise an alarm daily until you install and correctly configure the Viewer server. Ignore this alarm.

Allow Full Database Vacuum on Startup if required

Once every 6 months, the recorder must perform essential database functions. It does this on startup, but only after warning you that this will happen. If you receive an alarm saying that this is required but cannot afford to have the recorder do this on its next restart, you can defer this activity by clearing this checkbox. After each restart, this checkbox is reset and you must clear it again if you want to defer the task further. You must allow the recorder to perform these tasks within one month of being alerted.

Contact Center Interface

Click this tab to configure the CTI link(s) that the recorder will use to obtain real-time information regarding active calls and to control Duplicate Media Streaming.

Nortel Switch Type

Select the CS 1000 switch. The default on installation is CS 1000 and if you change this setting you must restart the Nortel Contact Recording Service (or restart the server) before proceeding.

CS 1000 Systems

When used with a CS 1000 switch:

- Enter the IP address of the Nortel Contact Center Manager Server(s) that the recorder is to establish an MLS link to. There is no need to add a port number as MLS always uses a fixed port number. If you have a standby CCMS, add its address - separated from the first by a semi-colon. The recorder will attempt to connect to this server if it fails for a minute using the first address.
To find the correct IP address of the CCMS, login in to CCMA, choose Config and pick the CCMS server. You will find the IP address in Properties.
- If you share a multi-customer system, you must specify your Machine Name and Meridian 1 Customer Number. Otherwise, leave these fields at their default values (blank and 0 respectively).
- If your switch is an Option 11, you must indicate this here.

Check the status of the MLS link on the Recorder Status › Summary page and correct any problems shown on the Alarms page.

CS2x00 Systems

When used with a CS2x00 switch:

- Enter the IP address of the ICM or Linkplexer that the recorder is to establish a link to. There is no need to add a port number as these always use a fixed port number. If you are using ICM directly and have configured two links in the linkset, add the second address - separated from the first by a semi-colon. The recorder will then connect via both addresses
- Network Node ID - this specifies the switch with which the recorder will communicate. It is defined by the operating company. The Network Node ID used to identify the switch must be the NetNodeID datafilled in table SCAIGRP.
- Destination Point Code - If you are dual links you must enter the Destination Point Code (PTCODE from C7NETWRK table). This should take the form of three or four numbers depending on the country.
- Service ID - identifies the service profile that the operating company has defined for this connection
- ServiceVersion - specifies the SCAI signalling version in use. Use 19 or 20 for TDM recording. Use 20 for IP recording.
- Business Group ID - Identifies the customer to whom the computer application belongs. This is defined by the operating company and is associated with the linkset by means of table SCAIGRP.
- Application ID - Identifies the recorder application and must be different from the ID used by any other application connected to this switch.
- Password - Is used for security purposes and corresponds to a specific BusinessGroupID. The password used for logging in is defined for the customer group in table SCAIGRP
- Linkset Name - Specifies the TCP/IP linkset to be requested.

Check the status of the ICM/Linkplexer link(s) on the Recorder Status › Summary page and correct any problems shown on the Alarms page.

TDM Tap Points

If your system includes TDM recorders, you must configure the Master with their IP addresses and specify which devices are connected to the inputs of these recorders.

- 1** Open the TDM Tap Points page.
- 2** Click the "edit" button to enter the list of "Slave TDM recorder(s)".
- 3** In the form enter the host names (preferably not numeric addresses) of the Slave TDM recorders (separated by semicolons) that this master Recorder is to control. Assign each recorder a unique Serial Number. This must be six digits long and start with 6. As the Master and Standby recorders are 890001 and 890002, slave TDM recorders should start at 600003. Then Click the "enter" button.
- 4** Click the "Add Tap(s)" button to enter details of the phones and/or trunks to which the TDM recorders' ports are connected.

- 5 Enter the connections according to the table below:

Tip: For trunk-side tapping, refer to the *Nortel TDM Installation Guide* to ensure that you understand the relationship of the channels.

	Extension-side Taps	Trunk-side Taps
CS 1000	Enter the TNs of the phone sets connected to the TDM recorder.	First determine whether the trunk is a T1 or E1 and if T1, whether 23 or 24 channels of audio are present. (This information is also needed by the TDM recorder itself). Then determine the loop number for each trunk. These are determined from the switch using LD21 on the switch console and entering LTM (List Trunk Map). Once these have been found, set the type of trunk and enter the loop number for each trunk being tapped.
CS2x00	Enter the PositionIDs or DNs of the phones connected to the TDM recorder. To record calls taken on secondary DNs on a phone (whether IDNs on a position or additional lines on a standard phone) click "Add Tap(s)" again and add the additional DNs - resulting in additional lines in the table at the bottom of the page. Calls will only be recorded on DNs or Position IDs listed on this page. The recorder has no other means of knowing that the secondary DNs are actually configured on any particular phone set.	First determine whether the trunk is a T1 or E1 and if T1, whether 23 or 24 channels of audio are present. (This information is also needed by the TDM recorder itself). Then TODO.....

Tip: If extension side tapping, connect phone sets with consecutively numbered TNs on the CS 1000 (or Position IDs on the CS2x00) to consecutively numbered media channels so that you can enter ranges of phones rather than have to specify each one and its detail separately.

- 6 Enter an optional comment to describe the device or trunk being tapped.

- 7 Enter the Recorder host name (preferably not numeric address) of the TDM recorder that is tapping this device/trunk.
- 8 Enter the “starting media channel number” of the connected device. If extension side tapping, the “starting media channel number” is the “Channel ID” on the TDM recorder for this particular device, or the starting “Channel ID” for a group of consecutively numbered devices. If trunk-side tapping, the “starting media channel number” is the “Channel ID” on the TDM recorder for the first channel of the trunk being tapped.
- 9 Repeat steps 4 through 8 for each trunk and phone or group of consecutively numbered phones.
- 10 Click “Apply Changes & Restart if necessary”. This applies the appropriate channel licenses to the TDM recorders. If you have changed the number of channels on a TDM recorder, it will restart after this. This will interrupt any recordings already in progress so should be done out of hours.
- 11 If you have changed any existing mappings you must restart the Nortel Contact Recording Master to have these take effect.

Note: (For CS 1000 Systems) Even though you enter TNs in the TDM tap points page to tell Nortel Contact Recording which physical phones or loops are being tapped, you still enter DN's when specifying what to record. Nortel Contact Recording uses CTI information to determine which TN is involved when a recordable DN is active, and enables the relevant port on the TDM recorder. The DN's are administered in Operations > Bulk Recording as described in [“Bulk Recording” on page 103](#).

Trunk-Side Recording of Specific Trunks Only

You can suppress these alarms on a particular trunk by creating an appropriate entry in the properties file as shown below. See [“Properties File” on page 139](#).

CS 1000 Systems

```
loop.ignore.nn=true
```

where

- nn is the loop number to be ignored - from 1 to 255. Do not use leading zeroes.

CS2x00 Systems

```
carrier.ignore.ttt.nnn.ccc=true
```

where

- ttt indicates the PM type - and is one of "PVG", "GW", "DTC", "SPM" or "LTC"
- nnn is the PM number (0-1023)
- ccc is the carrier number (1-168)

System Monitoring

The status of your recording system is shown on several web pages beneath the Status link on the Administration interface. Here you can see:

- overall status summary for the server and its interfaces to other components
- loading levels – both current and peak
- which DNs and Position IDs are being monitored by CCMS
- individual recording channel detail

Alarms and events occurring within the system are stored in the database. You can view them via the Alarms link at the top of the Administration page. If this link is red, it indicates that there are one or more uncleared alarms. As you address the cause of an alarm, you should clear it by clicking the checkbox to the left of it and then clicking the Clear Selected Event(s) button.

You should configure email alerting and/or SNMP monitoring of the system as described below. The system will then be able to bring alarms to your attention promptly.

Email Notification

To have the recorder email alarms to you or your support staff, first create an email account that the recorder can use to send emails. Click the System > Email Server tabs at the top of the Administration page and enter the following details:

SMTP Mail “From” Address

Set the name from which alarm email messages should originate, for example, recorder1@alt.bigcorp.com.

SMTP Mail Server

Enter the name of the SMTP mail server on which you have established the email account that the recorder will use to send email messages. If you leave this blank, the system will not send email messages when alarms occur – and you can then leave the remaining settings on this page blank.

SMTP Username

Leave this blank if your SMTP server allows unauthenticated sending. If it requires authentication, set the username of the SMTP account here.

SMTP Password

Leave this blank if your SMTP server allows unauthenticated sending. If it requires authentication, set the password of the SMTP account here. The password is masked when entered in this field.

Send alarm/event emails to

Specify the email address(es) to which alarm and event messages should sent. Separate multiple addresses with a semi-colon (;). The email recipient can be a local system administrator, a manned help-desk and/or suppliers' support desks if you have a support agreement that includes

this facility. The system sends an email message each time an alarm occurs or is resolved. It also sends an email once per day as a “log files purged” message to let you know it is still operating. This email is sent overnight. You should investigate any failure to receive the daily “log files purged” message as it could indicate that the server has failed.

Note: The system will batch emails for up to 10 minutes to avoid flooding users’ inboxes. The default configuration is that all alarms and events are sent via E-mail. You can change this so that only alarms above a specified severity are sent by E-mail. Be aware that if you do so, you may be unaware of issues that are affecting your system. See “email.minialarmlevel” in [“Properties File” on page 139](#).

Confirm that you are receiving emails correctly after you make any changes to these settings.

SNMP

You can use an SNMP monitoring system such as HP OpenView to monitor Duplicate Media Streaming Nortel Contact Recorders. To do so, you must first set the name of the SNMP Read Community in the General Setup > Recorder page. The recorder will then respond to SNMPV1 Get messages.

For security reasons, Nortel Contact Recording servers:

- do not allow “well known” community names like “private” or “public”
- do not respond to SNMP Gets until a community name has been set
- do not use the usual port of 161, but instead use 4161.

Operations

Click the Operations tab to set up Bulk Recording and/or Quality Monitoring recording. (The tab will only appear if your license includes these modes.)

Bulk Recording

This tab is only visible if your license includes channels of Bulk Recording. At the top of the screen are a number of parameters that determine how Bulk Recording operates.

You configure this screen on the Master recorder, regardless of whether the calls are ultimately to be recorded on the Master recorder, a Slave or a TDM recorder.

The lower part of the screen lets you specify the Directory Numbers and/or Position IDs that are to be recorded. If you click the Advanced button when entering these addresses, you can override a number of the overall settings for specific address ranges. The settings are described in detail below.

Apply Beep Tone (only applies to Duplicate Media Stream recording on CS 1000 systems)

When recording calls using Duplicate Media Streaming, you can inject a warning or ‘beep’ tone onto the call to advise users that they are being recorded. This is a legal requirement in some countries and states.

Record Internal Calls

Use this setting to turn on or off the recording of internal calls. The default is ‘on’. This setting specifies the default behavior for Bulk Recording as a whole but you can override it for specific DNs or Position IDs (see [“Directory Numbers \(DNs\) and/or Position IDs to be recorded”](#) on page 106). (This parameter has no effect on trunk-side TDM recording.)

Filter calls by Agent ID

The MLS feed, which the recorder uses to track calls, provides information regarding specific DNs or Position IDs. It cannot directly advise activity by Agent ID. If you wish to record specific Agents regardless of where they sit (often referred to as “free seating”) then you must:

- 1 configure all of the Position IDs at which these agents may log in
- 2 configure this filter setting to select recordings by Agent ID.

With this setting you can choose to specify those Agent IDs that should be recorded or those that should not.

ATTENTION

In CC6 or earlier, a recorder can only determine the location of an agent when that agent logs in. There is therefore a risk that, if the recorder restarts, it will not be aware of the locations of all agents until they have logged off and on again. If it is critical that you record all calls made by certain Agents, you should configure this setting to NOT record all other agents. This way the recorder will record any Position ID for which it has not yet seen an agent login. You may therefore end up with a few more recordings than were strictly necessary but you will not have missed any calls.

This setting is the default for Bulk Recording as a whole but can be overridden for specific DNs or Position IDs (see [“Directory Numbers \(DNs\) and/or Position IDs to be recorded” on page 106](#)).

You can enter Agent IDs individually, in ranges or a combination of these. For example: 1000, 1010-1049, 2001, 2005, 2501-2599. When entering ranges in this setting, it does not matter if some of the numbers in the range are not in use in your Contact Center.

Note: the number of digits is important. For example, the range 100-999 is different from 0100-0999.

Warn when available channel license count falls BELOW

The recorder’s license key determines the maximum number of recording channels that can be active at once. You can specify the level at which a warning is generated to alert you should this limit be approached. This warning appears on the Alarms page and in alert emails— assuming you have configured the E-mail settings. A corresponding Information level message is generated when the available channel count rises above this level again.

If you know that your channel count cannot be exceeded (for example, you have 10 channel licenses and only 10 phonesets) then you can safely set this level to 0. As the available count will never go negative, this effectively turns the warning system off.

The default setting of 1 ensures that you are alerted should the recorder reach its maximum capacity.

URL(s) of external control port(s) to connect to

If an external application is being used to provide additional call tagging or recording control then enter the URL on which it is expecting the recorder to contact it. Specify a specific port number by adding a colon (‘:’) and the port number to the end of the IP address. To use multiple external controllers, enter the URL of each, separated by a semi-colon (‘;’). For every URL entered here, the Recorder Status > Summary page will show the status of the link and the Alarms page will show any problems with the link.

Start recording automatically at start of call

This is set to “Yes” by default. If you set it to “No” recordings will not start until a start command is received from an external controller such as the Contact Recording Desktop (CRD) application. Note that if using the CRD, you must also ensure the user’s CRD configuration file enables the appropriate command button.

Allow user to start/restart recording

This is set to “No” by default. Change it if you want to let users start recording or restart a stopped recording through the CRD running on their desktop. Note that if using the CRD, you must also ensure their CRD configuration file enables the appropriate command button.

Allow user to stop recording

This is set to “No” by default. Change it if you want to let users stop recording through the CRD running on their desktop. Note that if using the CRD, you must also ensure their CRD configuration file enables the appropriate command button.

Allow user to delete recording

This is set to “No” by default. Change it if you want to let users delete the current or previous recording through the CRD running on their desktop. Note that if using the CRD, you must also ensure their CRD configuration file enables the appropriate command button.

Note: This feature is only supported on Duplicate Media Stream recording - not via TDM or Nortel Call Recording Cards.

Retain ONLY those recordings requested by user

This is set to “No” by default. If you change this, all recordings will be deleted at the end of the call (or after a specified delay) except when the user has requested that it be retained through the CRD running on their desktop. Note that if using the CRD, you must also ensure their CRD configuration file enables the appropriate command button.

Note: This feature is only supported on Duplicate Media Stream recording - not via TDM or Nortel Call Recording Cards.

DNs and/or Position IDs configured

This setting is not directly editable. It shows the total number of DN’s and/or Position IDs that you have configured for bulk recording in the list at the foot of this page.

Note: (For CS 1000 Systems) Multiple appearance DN's (MARF/MADN) can result in more than one recording channel per DN. The maximum number of active channels can therefore exceed this number.

Directory Numbers (DNs) and/or Position IDs to be recorded

This table shows the addresses that you wish to record calls from. Each row in the table can show a single address or a contiguous range of addresses. The table below shows the types of address that you may enter here:

Address Type	Supported	Comment
Standard DN or IDN	Yes	Single occurrence on a single phoneset.
Position ID	Yes	Use in conjunction with Filter calls by Agent ID to record specific Agents.
Agent ID	No	See Position ID
MARF (CS 1000 only)	Yes	One line appears on the CTI monitor page per phoneset on which the DN appears. Only supported in knowledge worker environments, not on call center positions. Use the MARF/MADN Advanced settings checkbox to enable recording.
MADN	Yes	One line appears on the CTI Monitor page per phoneset because only one call can be connected at a time. In CS 1000 systems, this is only supported in knowledge worker environments, not on call center positions. Use the MARF/MADN Advanced settings check box to enable recording. On CS2x00 systems, if you attempt to record a DN that appears on multiple sets, it will be recorded on all sets.

Note: For CS 1000 systems the limit of two associated (AST) keys per phoneset applies so a maximum of two different addresses can be recorded on any given phoneset.

To start recording one or more addresses:

- 1 Click on Add DN or Position IDs.
- 2 Enter the address or range of addresses in the pop-up window that appears. You can, if you wish, enter a comment that will appear in the Detail column of the table.
Tip: If you do not want to save any changes, click on Close Window.
- 3 Click on Enter to start recording this range of addresses.
- 4 Click on Advanced to set a number of optional settings as follows:
 - a. Designated Recorder/Pool(s): By default the recording system will load balance recordings across all available recorders. In distributed systems, however, you may wish

to force certain addresses to be recorded on specific servers. If you enter a recorder number in this field, then the system will attempt to record the address(es) on that recorder if at all possible. If you have assigned recorders to named "pools" (see "recorder.pool" in ["Properties File" on page 139](#)) you can specify one of these pools. The Master will then choose the most lightly loaded of the available recorders in this pool. To specify alternate recorders or pools to be used in the event that the first is unavailable, add another identifier - separated from the first by a semi-colon. Master, Standby and Slave recorders can all be designated specifically (by their recorder number) or assigned to a named pool.

Caution: Once you have designated a recorder in this way, calls will NOT be recorded unless one of the recorders/pools you have listed is available.

- b. **Recording Owner:** By default, each recording is "owned" by the DN or position ID that the call was made from. If an agent is logged on at that position ID then calls are also given the agent's logon identifier as an additional owner. (Note that on CS2x00 you must set the "Appear(s) on Position ID(s) from" setting for IDNs. See below.) You can override this with an alphanumeric owner (for example, "sales"). This can make it easier to manage search and replay rights.
- c. **Record Internal Calls:** By default, the setting at the top of the Operations > Bulk Recording page applies but you can choose to override this here.
- d. **Filter Calls by Agent ID:** By default, the setting at the top of the Operations > Bulk Recording page applies but you can choose to override this here.
- e. **Block IP Recording:** By default, this checkbox is cleared and the Master recorder will attempt to use IP Duplicate Media Streaming or station-side TDM recording. Check this box to force the system to use a trunk-side TDM tap when recording this DN/Position ID.

Note: (For CS 1000 Systems) If the DN/Position ID is a Phase I IP phoneset (which cannot support Duplicate Media Streaming) you must check this setting.

- f. **Allow Multiple Appearances (CS 1000 systems only. Always on in CS2x00):** Check this box if the DN(s) appear on multiple line keys - either on the same or across several phonesets. The recording of such MARP and/or MADN DN is only supported in the CS 1000 knowledge-worker environments - not on call center positions.
- g. **Appear(s) on Position ID(s) from: (CS1000 systems only. Always on in CS2x00/DMS.)** This setting is for CS2x00/DMS systems only. If the DN range relates to one or more consecutive IDNs then you must specify which position IDs these occur on. This allows the recorder to tag calls made on these lines with the Agent ID of the agent logged on to the corresponding position.
- h. **Start recording automatically at start of call:** By default, the setting at the top of the Operations > Bulk Recording page applies but you can choose to override this here.
- i. **Allow user to start/restart recording:** By default, the setting at the top of the Operations > Bulk Recording page applies but you can choose to override this here.
- j. **Allow user to stop recording:** By default, the setting at the top of the Operations > Bulk Recording page applies but you can choose to override this here.
- k. **Allow user to delete recording:** By default, the setting at the top of the Operations > Bulk Recording page applies but you can choose to override this here.
- l. **Retain ONLY those recordings requested by user:** By default, the setting at the top of the Operations > Bulk Recording page applies but you can choose to override this here.

- m. Save/Delete Key Present (CS1000, CC V7 and later only). This instructs the recorder to send lamp updates to the SAVE key configured on these addresses. (Available in 6.5.1 service update only.)
- n. XML file to use for Contact Recording Desktop: By default all CRDs use the configuration file dcs.xml in the \properties\desktops folder. Enter the name of an alternate XML file in the same directory to have this DN or Position ID range use a different configuration.

To stop recording one or more address ranges, check the box in the Select column next to the range(s) and click on Delete Selected DN/Position ID(s).

Click on the arrows at the tops of the columns to sort the table by that column in the direction of the arrow.

If the table contains more than 50 address ranges, it displays as multiple pages. Click on the page number, Next, Previous links to display other ranges. You can also select the “Show All” button to see all ranges at once.

Quality Monitoring

This tab is only visible if your license includes Agent stations of Quality Monitoring.

Apply Beep Tone (Duplicate Media Streaming on CS 1000 Systems only)

Select whether or not to apply beep tone when recording for Quality Monitoring purposes. This setting only applies when Duplicate Media Streaming is used. If using Call Recording Cards, you must configure warning tone on the switch itself as described in *Nortel Call Recording Card Planning, Installation and Administration Guide*. When using Bulk Recording and Quality monitoring, you should set this parameter the same for both modes.

URL of Nortel Quality Monitoring application to connect to

Specify the IP node name of the Quality Monitoring server. The port number for the recording control and link between these applications will default to 1415. If you have installed Quality Monitoring on the same server as the recorder, you can simply specify 127.0.0.1 or localhost.

Username/Password for file-share on Quality server

Recordings made under the control of a Quality Monitoring application are only held temporarily in the recorder’s bulk recording call storage area and, after the call completes, are copied onto a location maintained by the Quality Monitoring application.

If you have configured Nortel Quality Monitoring to store recordings in a file-share, you must enter a username and password here so that the recorder can write recordings to and read recordings from the share. If, on the other hand, you have installed Nortel Quality Monitoring on the same server as the Nortel Contact Recording Master and have configured it to use a local path rather than a file-share, you can leave these fields blank.

Call Recording Cards (CS 1000 switches only)

Use this edit button to enter details of any Call Recording Cards. In the pop up enter the IP Address and corresponding security keycode of each card to be used.

Agent Stations Recorded and Remaining Capacity

These items show how many different phonesets you have recorded in the previous month using the Quality Monitoring application. This must remain within your licensed capacity or the recorder will cease to record on behalf of the Quality Monitoring application. At this point, an alarm is raised and no additional phonesets can be recorded.

ATTENTION

If you are using a Trunk-side TDM recording system for quality assessment, you should also consider setting the properties `siu.ignoreinternalcalls`, `siu.ignoreuntapped` and `loop.ignore` (CS 1000) or `carrier.ignore` (CS2x00/DMS) settings. See Advanced Configuration > Property File settings for details.

Search and Replay

Note: This section applies to IP recording systems only.

If you are deploying a centralized search and replay system using Viewer, you should see *Nortel Viewer Installation Guide* for instructions on how to customize, deploy and use the application. However, you should still prove that you can search for and replay calls directly from the recorder because:

- if you cannot, then Viewer will not be able to play calls either.
- in the event of server or network failure you may need to access recordings directly from the recorder.

The instructions below relate to the integral search and replay application that is part of the Nortel Contact Recorder. *Nortel Contact Recording Search and Replay User Guide* provides end user instructions on this application. As the system administrator, however, you may wish to:

- control which users can search and replay recordings
- ensure that the ActiveX control used can be downloaded to your clients' PCs
- modify default behavior via the properties file
- customize the search fields and/or display

The last of these is rarely required and is described with other advanced topics in [“Customizing Search and Replay” on page 155](#). The others are needed in most cases and are described below.

Search and Replay Access Rights

When a recording is made, the recorder assigns its “owner” as follows:

- If the Recording owner field is set on the Advanced settings for the DN or Position ID, the owner will be the number or name specified there.
- If an owner is not specified but the call was made by a logged in Agent, then the owner is that Agent's ID.
- If an owner is not specified and the call was not made by a logged on Agent, then the owner is the DN that made the recording.

Note: CS2000: Only calls taken on the positionID are owned by the logged on Agent. Those made on IDNs are "owned" by the IDN only.

You control which recordings your users can search for and replay by adding a user account for each person that needs to use the Replay page and specifying which range(s) of owner they are entitled to see.

To add a user account, follow the same procedure that you used in [“Securing the System” on page 93](#) but do not check the User is an Administrator box.

In order to search for and replay a call, the user's replay rights must include the owner of that call. Each user's rights are shown on the System › Manage Users page and are set when adding the user account. You can change these by clicking on the Edit link next to them.

The initial administrator's account is automatically given access rights to all number ranges up to 10 digits. As you add other users you must specify which ranges of owners each user is entitled to replay. The number of digits is significant. A user with replay rights over 0000-9999 can not replay calls made on and "owned by" DN 567 though they could play calls owned by DN 0567. In this example, you might grant the user replay rights over 0000-9999, 000-999.

Each user account is automatically entitled to replay any calls where the owner field is the same as their user name. This makes it easy to assign each DN to the person who uses it by setting their username on the Advanced tab of the Operations › Bulk Recording entry for that DN.

Typical examples of how to use replay rights are:

- A user allowed to play calls made on his own DN (1234) would be given replay rights 1234.
- An Agent who logs on as AgentID 0012 and is allowed to replay his own calls may be given replay rights 0012.
- A supervisor who logs on as AgentID 0050 and manages AgentIDs 0010-0019 and 0025-0028 may be given replay rights 0050,0010-0019,0025-0028.
- All recorded DNs used by the HR staff have their Recording Owner set to HR on the Advanced settings. The Human Resources Manager, who uses DN 5678 may be given replay rights HR, 5678.

ActiveX Control Download

The Replay page downloads two ActiveX controls, which it uses to decompress the audio for replay and export. If your default browser security settings prohibit the downloading of such controls, you need to provide a means of getting the ActiveX control to your users' desktops.

See ["Installing the ActiveX Controls Manually"](#) on page 112 for an alternate way to deploy the controls.

Internet Explorer (IE) determines rights by putting web servers into zones and then granting those zones specific rights.

To access and use the Replay page with its ActiveX control, the recorder must reside in a zone with the following rights:

- ActiveX controls and plug-ins
- Download signed ActiveX controls
- Run ActiveX controls and plug-ins
- Script ActiveX controls marked safe for scripting
- Scripting
- Active scripting

On Windows Vista you must also clear the "Enable Protected Mode" checkbox.

Your Intranet zone and/or the Trusted Site zone may already have these rights. If so, you need to verify that the Nortel Contact Recorder is in one of these zones. If the recorder is not in the local Intranet Zone or is not a Trusted Site, you can add it as follows:

- 1 In the Control Panel, open Internet Options.
- 2 Click the Security tab.
- 3 Click the Trusted Sites icon.
- 4 Click Sites.
- 5 Uncheck the 'Require server verification (https:) for all sites in this zone' box (unless you are forcing users to use https).
- 6 Enter the URL of the Nortel Contact Recorder server and click Add.

Note: Internet Explorer does not recognize that a certain Fully Qualified Domain Name (FQDN) and IP address are the same; you must add the URL to the list exactly as your end users are expected to type it in the address bar.

Before you advise end users of the URL of the recorder, you should make sure that your users can access the Replay page through your network and that the ActiveX controls download successfully. To test this:

- 1 Create a non-administrator account and assign it some replay rights.
- 2 From a typical client machine, enter the URL for the Nortel Contact Recording server in the form: `http://myservername:8080/` (replacing myservername with the recorder's IP address or hostname – assuming you have entered it in your DNS server). If using https, replace 8080 with 8443.
- 3 When prompted, enter the account's Username and a blank Password.
- 4 Set a new password as directed.
- 5 Confirm that the Replay page displays correctly and that the ActiveX control is downloaded.

Tip: You may wish to copy steps 2 to 4 above, fill in your URL and send them out as instructions to your end users.

Installing the ActiveX Controls Manually

The ActiveX controls needed for the Search and Replay application are typically downloaded and automatically installed the first time the application is accessed. In a closed environment where users may not be able to download and install programs on their computers, you need to manually set up the Active X controls.

To install the ActiveX controls:

- 1 Download the `vxreplay.cab` file that contains the required files from `http://mycscmrecorder:8080/cabs/vxreplay.cab` (where CRservername is the name of the server on which the Nortel Contact Recorder is installed).
- 2 Save the file to the drive.
- 3 Unzip the file to find:
`csreplay.ocx`

```
csexport.ocx  
dspapi.dll  
csreplay.inf
```

Note: If your browser does not allow you to download the .cab file, see the next section [“A Note About Downloading the .cab file” on page 113](#).

- 4 Copy the dll to a location in the Path (typically \windows\system32).
- 5 Right-click the **csreplay.inf** file and select **Install**.
- 6 Click Start > Run
- 7 In the field displayed enter
`regsvr32 [path]csreplay.ocx`

replacing `[path]` with the full path for the **csreplay.ocx** file.

- 8 Repeat the previous step to register the **csexport.ocx** file.

Note: The files will need to be updated whenever the Contact Recording Server is updated.

A Note About Downloading the .cab file

Some browsers won't let you save a cab file; instead they open and read the file. (It is not in human readable form.) To work around this limitation:

- 1 Create a file that contains the following html:

```
<html>  
<body>  
<a href="http://myCRrecorder:8080/cabs/vxreplay.cab">Right Click  
Here</a> </body> </html>
```
- 2 Save and close the file.
- 3 Use your browser to open the file.
- 4 Right-click the link and select **Save target as**
- 5 Save it as vxreplay.cab.

Modify Default Behavior

You can add or modify lines in the properties file as described in Section 6.1 to change the behavior of the Replay page to:

- limit the number of results returned
- save filter settings from session to session
- restrict access to the export functions:

These settings affect all users and are only updated when the Nortel Contact Recording Service starts.

Limit results returned

Add the following line to the properties file to set the maximum number of calls returned from a query:

```
viewerx.limit=nnnn
```

where nnnn is the maximum number of calls to return. Increasing this maximum over the default of 100 results in more CPU use and higher network traffic if users choose to view or accidentally request a large number of calls.

Save filter settings from session to session

Normally, the entries in the search filter pane are blank when you first access it. If you wish, the application can remember the last used settings and apply these instead. This feature is controlled by a setting in the properties file:

```
viewerx.savesettings=true
```

Restrict access to the Export function

Access to the individual and bulk call export features is controlled by two entries in the properties file:

Allow administrators to export calls (Default = true)

```
replay.export.admin
```

Allow non-admin users to export calls (Default = false)

```
replay.export.all
```

By default, only Administrators can export calls.

Note: The replay.export.all setting overrides the replay.export.admin setting, so if replay.export.admin=false but replay.export.all=true, administrators can use the export feature.

Backup/Restore

Due to the huge volume of new files created every day, a voice recorder is not backed up in the same way as most application servers. This section guides you through the issues around backing up the application, the call details database and the recordings.

Application

A Nortel Contact Recording server's configuration is stored in its database (using PostgreSQL), alongside the details of the call recordings. To preserve the configuration of the server, back up the database frequently as described below.

If you have not installed other applications on the server, there is no need to backup the operating system or the Nortel Contact Recording software. It is faster to reinstall these server components in the event of disk failure. You should therefore retain the installation media and license key that you used.

Backing up the Database

You can back up your Nortel Contact Recording server's database using a command line procedure. The procedure uses the PostgreSQL `pg_dump` command to extract data from the database. It must be executed while the database is running. Do not stop the Nortel Contact Recording service or the Postgresql service before proceeding.

To back up your postgres database:

- 1 Log on as an administrator and open a command window.

Change directory ("`cd`") to the `\etc` folder beneath the installation path.

```
(\Program files\Nortel>Contact Recording\etc )
```

- 2 Create a backup file by entering the command:

```
winbackup backupfile
```

The default location for the backup file is `\Program files\Nortel>Contact Recording\etc`

Note: You should specify a full path name for the backup file. Make sure there is enough space on the target drive for the backup file. Consider copying the backup file to another server, or external media.

```

c:\ Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>d:

D:\>cd D:\Program Files\Nortel>Contact Recording\etc

D:\Program Files\Nortel>Contact Recording\etc>winbackup TestBackup

D:\Program Files\Nortel>Contact Recording\etc>..\jre\bin\java.exe -cp ..\tomcat525\shared\lib\csnmain.jar;..\tomcat525\shared\lib\log4j.jar com.swhh.os.backup TestBackup ..\postgresql\bin
0 [main] DEBUG com.swhh.os.WinBackup - Return code=0

D:\Program Files\Nortel>Contact Recording\etc>_

```

Name	Size	Type	Date Modified	Attributes
backupfile	47 KB	File	10/28/2008 3:17 PM	A
dvdjni.dll	40 KB	Application Extension	3/7/2008 9:01 AM	A
g726jni.dll	48 KB	Application Extension	3/7/2008 9:01 AM	A
g729jni.dll	76 KB	Application Extension	3/7/2008 9:01 AM	A
ndvdjni.dll	52 KB	Application Extension	3/7/2008 9:01 AM	A
osutils.dll	36 KB	Application Extension	3/7/2008 9:01 AM	A
starburn.exe	40 KB	Application	3/7/2008 9:01 AM	A

Restoring data to a new PostgreSQL database

Note: You can only restore data to the Nortel Contact Recording server (or at least one with the same MAC address) from which you dumped it because the dump file stores the software serial number and license key information. The following process erases the default database that exists after a complete re-installation and replaces it with database that you have backed up.

To restore the database:

- 1 Log into server as an administrator.
- 2 Stop Nortel Contact Recording service.

- 3 Locate the pg_hba.conf file in <Install Location>\Nortel\Contact Recording\postgresql\data\
- 4 Make the following modifications to the last lines in the file (below is the BEFORE and AFTER modifications):

Before

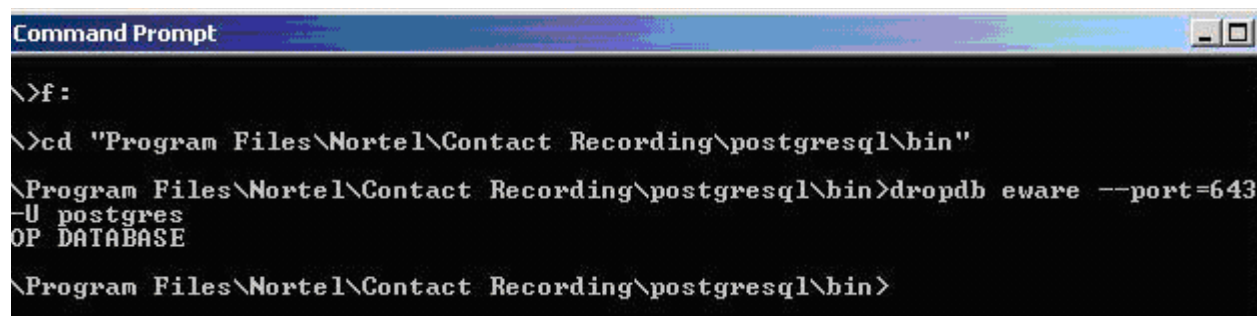
```
# TYPE  DATABASE    USER        CIDR-ADDRESS        METHOD
# IPv4 local connections:
host    all          all         127.0.0.1/32        md5
# IPv6 local connections:
#host   all          all         ::1/128             md5
```

After

```
# TYPE  DATABASE    USER        CIDR-ADDRESS        METHOD
# IPv4 local connections:
host    all          all         127.0.0.1/32        trust
# IPv6 local connections:
#host   all          all         ::1/128             md5
```

- 5 Save the modified pg_hba.conf file.
- 6 Restart PostgreSQL Database service.
- 7 Open a command window and change the directory to <Install Location>\Nortel\Contact Recording\postgresql\bin.
- 8 Drop the existing DB using the command: "dropdb eware --port=6432 -U postgres"

Warning: This step will delete the existing db!! Do not perform without a good backup that can be restored!!



```
Command Prompt

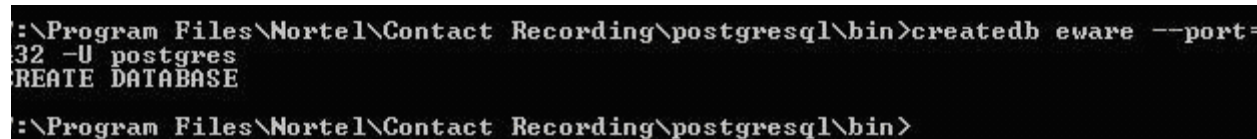
\>f:

\>cd "Program Files\Nortel\Contact Recording\postgresql\bin"

Program Files\Nortel\Contact Recording\postgresql\bin>dropdb eware --port=6432 -U postgres
DROP DATABASE

Program Files\Nortel\Contact Recording\postgresql\bin>
```

- 9 Create eware DB using the command: createdb eware --port=6432 -U postgres



```
Program Files\Nortel\Contact Recording\postgresql\bin>createdb eware --port=6432 -U postgres
CREATE DATABASE

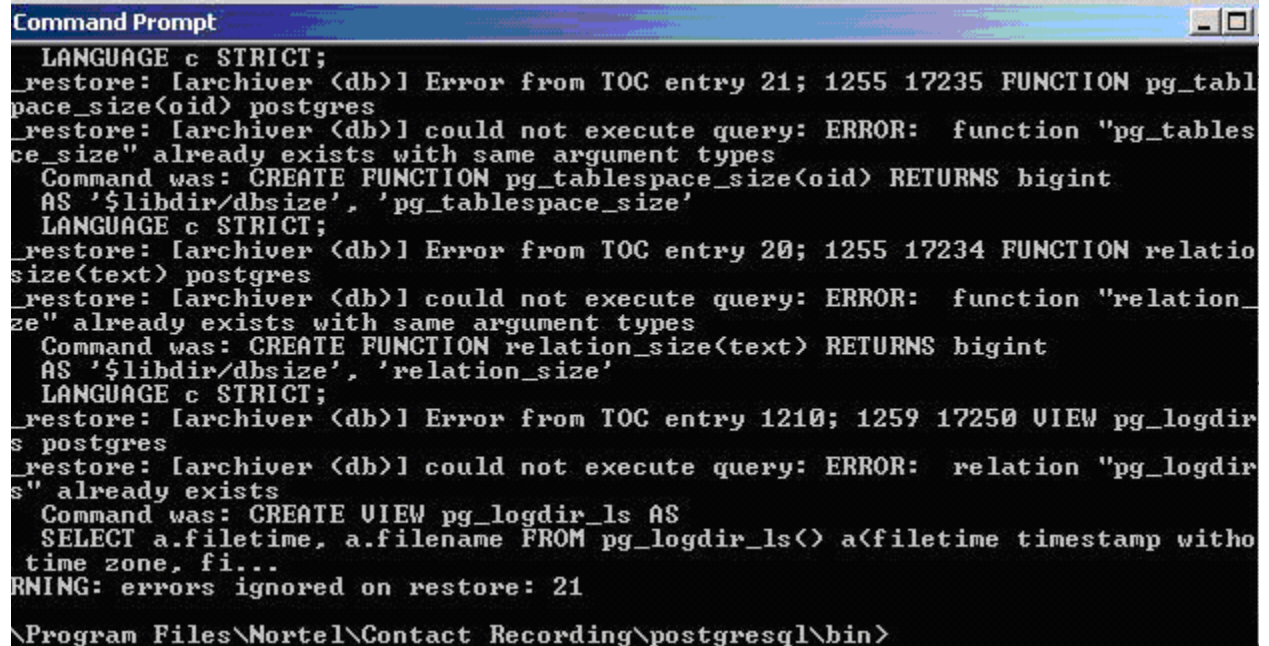
Program Files\Nortel\Contact Recording\postgresql\bin>
```

- 10 Restore backup using the command: `pg_restore --dbname=eware --port=6432 -U postgres --use-set-session-authorization <name of backup file>`

```
:\Program Files\Nortel>Contact Recording\postgresql\bin>pg_restore --dbname=eware --port=6432 -U postgres --use-set-session-authorization backuptest_
```

- 11 The backup will restore with a warning at the end indicating errors ignored.

Note: These errors are OK.



```
Command Prompt
LANGUAGE c STRICT;
_restore: [archiver (db)] Error from TOC entry 21; 1255 17235 FUNCTION pg_tablespace_size(oid) postgres
_restore: [archiver (db)] could not execute query: ERROR: function "pg_tablespace_size" already exists with same argument types
Command was: CREATE FUNCTION pg_tablespace_size(oid) RETURNS bigint AS '$libdir/dbsize', 'pg_tablespace_size' LANGUAGE c STRICT;
_restore: [archiver (db)] Error from TOC entry 20; 1255 17234 FUNCTION relation_size(text) postgres
_restore: [archiver (db)] could not execute query: ERROR: function "relation_size" already exists with same argument types
Command was: CREATE FUNCTION relation_size(text) RETURNS bigint AS '$libdir/dbsize', 'relation_size' LANGUAGE c STRICT;
_restore: [archiver (db)] Error from TOC entry 1210; 1259 17250 VIEW pg_logdir_ls postgres
_restore: [archiver (db)] could not execute query: ERROR: relation "pg_logdir_ls" already exists
Command was: CREATE VIEW pg_logdir_ls AS SELECT a.filetime, a.filename FROM pg_logdir_ls() a(filetime timestamp without time zone, fi...)
WARNING: errors ignored on restore: 21
:\Program Files\Nortel>Contact Recording\postgresql\bin>
```

- 12 Reverse the changes made in step 4 so the hg_hba.conf file is back to original settings (below is the BEFORE and AFTER modifications:

Before:

#	TYPE	DATABASE	USER	CIDR-ADDRESS	METHOD
# IPv4 local connections:					
host	all		all	127.0.0.1/32	Trust
# IPv6 local connections:					
#host	all		all	:::1/128	md5

After:

#	TYPE	DATABASE	USER	CIDR-ADDRESS	METHOD
# IPv4 local connections:					
host	all		all	127.0.0.1/32	md5
# IPv6 local connections:					
#host	all		all	:::1/128	md5

- 13 Save the newly modified pg_hba.conf file.
- 14 Restart PostgreSQL Database service.
- 15 Start Nortel Contact Recording service.
- 16 Test to verify successful restore.

Backing up Voice Recordings

The Nortel Contact Recorder stores voice recordings in the path you specify on the General Setup › Recorder page. This partition quickly fills up with thousands of directories and millions of files. When the partition is nearly full, the Nortel Contact Recording server maintains only a tiny amount of free space on the partition by deleting batches of 100 recordings (and the directory that cataloged them) at a time, as it requires space for new recordings. This causes a huge churn of files every day.

Limitations of full and incremental backup procedures

On a Nortel Contact Recorder server, two issues make it difficult to back up voice files:

- the file size
- the rate of change of the voice recording files

Together these issues make most traditional backup strategies for the voice recordings ineffective. Traditional full backups are required more frequently than normal, which wastes backup media, and incremental backups are larger than expected because of the large churn of creations and deletions. For a backup strategy to be successful, it must be easy to restore the data if necessary.

Traditional “full plus incremental” backup solutions are ineffective because these backup solutions cannot complete fully. In the event of a complete disk failure, the process restores the full backup, then the increments in chronological order. This procedure immediately overflows the disk when the restore program tries to create the increments because the partition holding the call is almost at capacity to begin with. The full plus incremental backup will fail because it runs out of disk space before it has processed the “removals” part of the procedure.

Traditional restore procedures are also ineffective. If you use this solution to review a recording that has been deleted because of age, the Nortel Contact Recording Service immediately deletes any restored file as part of its disk maintenance.

Finally, traditional backup solutions often require locks on the disk while they work. This can seriously disrupt the working of the recorder.

Two suitable strategies for audio backup

DVD+RW archive

This simplest and cheapest strategy is to use the built in DVD+RW archive mechanism. This is not only fully integrated with the workings of the recorder and its search and replay mechanism, but also is well suited to the incremental recording required for a recorder. As recordings are added to the calls path they are copied to DVD in an efficient manner. Even when they have been deleted from the hard disk, the recorder is still able to play them because it knows which DVD they are on and can replay directly from DVD, without an intervening 'restoration' step. Each DVD holds about 4GB, which means it can hold about 150 channel-days worth of recordings from a busy system. For less than dollar a day, even a busy system can have limitless backup.

Archive Manager

The second most effective strategy is to implement the Archive system. This server is a rules-based system. It copies audio files from the Nortel Contact Recorder onto different, centralized disks. The data on these centralized disks is

- organized in a more permanent way
- subject to less "churn"

It is possible to pause the Archive Manager when required, so, if a backup process requires a disk lock, the downtime does not cause a problem with the server's operation. This pause feature, together with the way Archive organizes the audio on disk, makes this data much more appropriate for traditional full/incremental backup solutions.

Chapter 7

Operations, Administration & Maintenance

In this chapter

Introduction	123
Status Monitoring	124
Alarms	129
Audit Trail	130
Local Archive	131
Preventative Maintenance	133
Best Practice: Restarting Servers	136

Introduction

In addition to initial configuration, there are a number of tasks that need to be performed on an ongoing basis. This section discusses:

- the use of the Status monitoring pages
- the Audit Trail
- local archive
- preventative maintenance tasks that should be carried out on a regular basis

Status Monitoring

Recorder status is shown over three pages that are accessed under the Status tab at the top left of the Administration web interface. These show the current:

- Summary – links to other components, local archive and storage status and, if it is the Master, the current and peak concurrent load on all of the recorders in the system.
- (On the Master and Standby only) CTI Monitors – the list of DNs/Position IDs that are being observed via the CTI link.
- (On the Master and Standby only) Channels – the state of each recording channel in the system.

Summary

This page shows summary information about the current state of the recorder and is therefore the default page shown when you first log in as an administrator.

Link to XXX at...

The Master and Standby recorders must receive information over MLS (for CS 1000) or ICM (for CS2x00/DMS systems) in order to control recording. Call tagging and filtering will not work correctly if this link is DOWN.

If the recorder connects to other components, such as Viewer, or Nortel Quality Monitoring, Standby, Slave or TDM recorders, the status of these links should be UP.

Current DVD media

Use this entry to confirm that the DVD drive has sensed, and is using, a valid disk. It will show one of the following values:

- active if it is able to record to the disk
- foreign if it cannot use or recognize the inserted disk
- old if a previously closed disk has been reinserted
- empty if there is no disk in the drive
- unknown if the recorder is still starting up or the archive device has not been specified correctly

Unless it is showing Active, or you are replaying from a previous disk, you should insert a new or the latest partially filled disk so that archiving can continue.

Note: The DVD entries are only shown if you have configured a DVD+RW drive on the General Setup > Recorder page.

Current DVD Label

Use this value to label the current disk. Disks are sequentially numbered. You should label the next disk (with the next available number) before inserting it.

Free Space on current DVD media

Use this value to determine when you will need to change the DVD media. A blank media shows 4 GB free space.

Total call segments recorded to date

This value shows the total number of call segments ever recorded by the system.

Total call segments recorded today

Use this value to confirm that recordings are being made today. If you have restarted the server today, this will show the number of call segments recorded since that restart. This includes recordings made on behalf of the Quality Monitoring application.

Date of oldest call held on disk

Until your disk has filled for the first time, you should monitor the available space on the drive. Check that the rate at which space is being consumed is in line with your predictions. You should be able to estimate when the disk will reach capacity and when the first calls recorded will be deleted to make way for new calls.

Once the disk has started to “wrap” and calls are being deleted daily, use this figure to monitor the online retrieval capacity. If the figure starts to fall, recordings are using up your disk space more rapidly than before. The recording volumes are increasing, so you may need to expand the disk capacity before the duration of calls it can hold falls below your minimum requirement.

Load

On the Nortel Contact Recording Master, the table at the bottom of this page shows the current and peak loading levels of the recorder. For each recording mode configured, it shows

- how many channels have been allocated
- how many are currently active
- the maximum number that have been active concurrently since midnight
- the maximum number that have been active concurrently since the date and time shown above the right-hand column

To reset the monitoring period, select the Restart Peak Activity Counts button. For example, if your business has a weekly cycle, you may want to reset the monitoring period at the start of each week. Use this page to predict when to expand your recording capacity.

CTI Monitors

This page is only populated on Master and Standby recorders (not Slaves). It shows each of the DNs or Position IDs that the recorder needs to monitor to perform Bulk Recording and/or Quality Monitoring. (On CS 1000 systems, where a DN appears on multiple telephone sets, each such TN results in a separate row in this display). In all cases, the columns show:

DN or PosID

Shows the Directory number or Position ID being monitored.

TN (CS 1000 Systems only)

Shows the TN that this row relates to. Where a DN appears on multiple phones, each one should have a separate row in this page. If the recorder fails to observe the DN (or has not yet reached it on starting up) this column will show “None Registered.” In the former case, you should check the Alarms page for clues to the problem.

Associated

Shows whether or not this DN or Position ID has been successfully "associated" with the recording application. If not, no CTI events will be received for it and recording will not take place.

Part of Range

This field is used for Bulk Recording only. It shows which DN or Position ID range this particular address is a part of. Any advanced settings that apply to this range will determine how this DN is recorded.

Agent

If an agent has logged on to this position since the recorder started, this field shows that agent's ID. (On CS2x00/DMS systems you must set an Advanced setting to link IDNs to the position ID on which they appear for this to work. See [“Directory Numbers \(DNs\) and/or Position IDs to be recorded” on page 106.](#))

Active Calls

Shows the call ID and parties on each call that this DN or Position ID is connected to. This includes

- whether the call was Incoming (I/C) or Outgoing (O/G) from that party (if known)
- whether that party is an internal (“Int”) or external (“Ext”) party
- the current state of the connection to that party (as best can be determined from the CTI messages received. For example, unless the far end is also being recorded it is not possible to know that the far end has placed the call on hold and it may show as “???” - meaning “unknown”)

If one of the calls listed is shown in bold typeface, it implies that the recorder believes that this particular call is active and therefore may need to be recorded. Other calls must therefore be on hold.

Channel

When a call is active and either needs to bulk recorded or observed by the Quality monitoring application, a channel on a recorder is assigned to it. The recorder name and channel number are shown here. The recorder may be a Nortel Contact Recording IP recorder, a TDM recorder or a Call Recording Card.

Quality

This field shows how the Quality Monitoring application is handling this DN or Position ID. It will show one of three conditions:

- “N/A” - means that this DN or Position ID is not configured within the Quality Monitoring application and hence Quality Monitoring is not available. (Note that the list of DN's and

Position IDs that Nortel Quality Monitoring observes is only updated when the connection to the recorder is established.)

- If a number or pair of numbers is shown (e.g. 1234/5678) this signifies that the Quality Monitoring application is observing this DN or Position ID and sees it as part of the overall “position” that it knows as this string. So for example, both Position ID 1234 and DN 5678 would show “1234/5678” in the previous example.
- A quality monitoring input channel identifier such as “IC:0:”. This shows that the Quality Monitoring application is actively observing (may or may not be recording) this DN or Position ID and is using the channel shown from its channel pool to do so.

Desktop

This shows the PC name where a user has logged into the Contact Recording Desktop and may be controlling recording or tagging calls using the application.

Rec

This column shows whether or not the channel assigned is recording the call at the moment. When Quality Monitoring is used, the recorder must sometimes assign channels even though bulk recording is not required. In such cases this column will show “No”.

Calls

This column shows how many calls have been bulk recorded on this DN or Position ID.

To update the page, click the Refresh button.

Channels

This page is only populated on Master and Standby recorders (not Slaves). It shows the current state and configuration of each channel on each recorder in the system. Note that all channels are dynamically assigned and released as calls come and go. The columns show:

DN/TN

Shows which DN/TN (and hence corresponding row on the CTI Monitors page) is using this port. If a port is not allocated, this column will show “N/A”.

The page is sorted by this column by default so that the (often many) unallocated ports are on later pages and active ports show on the first page.

Channel

The recorder's (or Call Recording Card's) IP address and channel number are shown. The channel number differs slightly according to the type of recorder:

- Nortel Contact Recording IP Recorders show the lower of the two RTP ports used by the channel (and hence there are no odd numbered ones).
- Nortel Contact Recording TDM Recorders show Media channel numbers from 1 upwards
- Call Recording Cards show channel number from 1 upwards.

Rec

Shows whether or not the port has been told to record active calls. This may be “No” due to Quality Monitoring application observing via this port but not recording.

Active

Shows whether a recording is actually in progress or not.

To update the page, click the Refresh button.

Alarms

The Alarms page shows system warnings, alarms and events. The recorder stores alarms in its database. It deletes them when they are more than a month old.

Check the box at the top of the page if you want to see all Alarms, including those that have been cleared. The default is to show only those alarms that have not yet been cleared.

The radio buttons at the top of the page let you select the minimum severity of alarms that are shown. The Alarms page will only show the most recent 1000 alarms (in 20 pages of 50 alarms each). If there are Informational or Warning level messages, you may need to restrict your view to Minor or Major alarms if you want to see further back in time.

Use the buttons above or below the table to refresh the page and to clear some or all alarms.

Note: As long as you have set up mail account information on the System > Email Server page, an email message detailing alarms and events will be sent to the address(es) listed there.

Refer to Appendix C, “Alarms.” for a list of alarms and events that may be generated and what to do about them.

Viewing alarms and events

The default on the page is to show all alarms and events that are uncleared. You can see any new or outstanding issues on first viewing the page. To change the set of events shown:

- 1 Click on the check box and/or radio button to specify your preferences.
- 2 Click on the Refresh button above or below the table.

Clearing specific events

New alarms and events are initially “active”. To clear an individual alarm or event so that it no longer shows:

- 1 Click the check box to the left of the event.
- 2 Click the Clear selected events button.

Clearing all events

Be careful using the Clear All Events button. Clearing an alarm without fixing the problem may lead to system problems being hidden without your knowledge.

Audit Trail

The System > Audit Trail page shows administrator and user actions over a specific period. The default reporting period is the current day. You can also filter this report according to Event Type and Username. To generate a report for a different period, enter the date range in the calendar controls, and click the Refresh button.

The Audit Trail functions track the following user actions:

- Successful user logins
- Failed user logins
- Password changes (although, for security reasons, the actual password is not stored)
- End user searches on the database
- Replay requests

It also tracks all administrator actions that affect recording.

Note: Editing a DN range is logged as a deletion followed by an addition.

The Detail column includes the SQL statement used in searching for calls. It also uses the internal name of a setting rather than the user-friendly, localized name. This avoids any change of meaning that could occur in internationalization.

Each report is restricted to a maximum of 1000 audit records. To report on more, break your reporting period into a number of smaller date ranges.

Use your browser's print, save, or email features to provide a permanent record of the details. To create a summary that presents all results on a single page, click the Show All link at the top. The Show All and Page at a Time links are not shown if the list of audit entries is less than one page long.

Configuration records (which include the audit trail) are retained for three months by default. Set `audit.purgemonths=nn` in the properties file to change this.

Local Archive

This section explains how to use a local DVD+RW drive to archive recordings.

The recorder writes both the audio (WAV) and call detail (XML) files to DVD in batches as calls are recorded. Recording files are copied to the DVD disk when one of the following occurs:

- 14 hours of recordings have been made (equivalent to 100MB when recording in G.726 or 50MB in G.729A mode)
- 24 hours have passed since the last write to DVD

You have the option to record a backup of the calls details database to the end of a DVD. Since DVD+RW disks cannot have multiple small files written separately in the last 0.5GB, this backup file makes efficient use of the otherwise unusable space.

DVD+RW media control and care

To find calls easily and reliably, ensure that all media are labelled, handled and stored correctly. To ensure maximum reliability and consistent high quality recording and playback:

- Follow the drive manufacturer's guidelines for cleaning the drive's lens.
- Follow the media manufacturer's guidelines for storage and handling. Check that the maximum shelf-life of the disks is adequate for your purposes and, if not, plan to copy the contents to new media within this period.

Loading a disk

To load a new disk:

- 1 Insert a blank DVD+RW disk in the drive.
- 2 Wait for it to spin up and be recognized.
Attention: Do not close the rack door as the tray will eject and automatically re-insert during the load process.
- 3 In the recorder Administration application, click on the System Overview link to confirm that the recorder has recognized the disk.

The Current DVD media field shows that the disk has been recognized and is being written to; it also shows the volume label given to the new disk. The Free Space on current DVD media line should show 4GB or more available on a clean disk.

Changing disks

The System Overview page shows when the disk is full and an alarm is raised.

To eject a disk that is still being recorded in order to retrieve calls from another disk:

- 1 Click on the Eject link on the System Overview page.
- 2 Insert the required archive disk.

- 3 When you have finished retrieving calls, replace the partially full disk so recording can continue.

Note: The archival process never writes to disks out of sequence. For example, if you eject a partially full disk, then insert a blank disk onto which the next set of calls is then written, you cannot then reinsert the previous disk.

Labeling a disk

As you eject each disk, label the disk itself using an approved indelible marker. Your label should indicate:

- The identifier of the recorder producing the disk. The identifier is Calls by default; you should change this value on the System Settings > Server page of the System Administration application.
- The sequential serial number of the disk.
- The date that the disk became full.

Verifying recorded disks

While a disk is being recorded, the files on it are not visible to Windows. They only show once the disk has been ejected and reinserted into a non-recording DVD drive.

To verify that the contents of a disks are valid, insert the DVD into a non-recording DVD drive and then open Explorer on the drive. If the contents of the disk are valid, there will be a set of large tar files that contain the wav and xml files of the original recordings.

Be sure to:

- Place the disk back in its protective container.
- Store the disk in a logical order with the other recorded disks.

Preventative Maintenance

This section highlights a number of administrative tasks that should be performed daily, weekly, monthly, and every six months to ensure the system continues to operate smoothly.

Daily

Unless you have fully automated alerting of these conditions, you should carry out the following procedures at the start of each day:

Alarms

Check the Alarms page for new problems.

Disk capacity

Check the available disk space. The disk where recordings are stored will appear to be at or near capacity. However, the system consistently maintains a level of 1 GB of free space by deleting older files. This maximizes the number of recordings that are available online to you. The Nortel Contact Recorder's disk manager thread deletes files on a FIFO (First In First Out) basis. Check the contents of the log files as described in Appendix D and examine any errors logged since the previous check. Look at all error and warning messages, not just those generated by the Nortel Contact Recorder services.

System Status

It is difficult to detect some problems automatically. Check the system status regularly via the Recorder Status › Summary page and verify that all figures are in line with expectations as described in [“Summary” on page 124](#).

Confirm channel status

Use the Recorder Status › Channels page of the Administration application to confirm that the recording channels are in the appropriate states.

Confirm recording and replay

To confirm recording and replay:

- Verify that calls are being uploaded into the database.
- Use the Replay page to select the most recent calls to verify that calls are accessible (IP Recorders only)
- Confirm that the start time of these calls matches expectations. Verify that the start time corresponds to the most recent calls made on the extensions being recorded.
- Confirm that these calls are playable and that audio quality is good.

Archive

If using DVD+RW archive, check the current disk's available capacity. Change the disk when it fills.

Weekly

As you become comfortable with the normal operation of your recorder, you can reduce the frequency of the daily tasks. For example, if you know that the rate at which your disk is filling is not going to fill the available space for several months, you can check it weekly.

Perform the following tasks each week:

Disk capacity: main recording store

When your recorder is first installed, the disk is almost empty. As it gradually fills, you should note the rate at which it is being used (at least weekly) and extrapolate to estimate when the disk will be full. At this point, the Nortel Contact Recorder will begin deleting the oldest calls to make room for new ones. If this happens to calls that are younger than planned, check the configuration of the recorder to ensure that only the anticipated calls only are being recorded. Add additional disk capacity to the partition before it fills.

Disk capacity: other partitions

Check the available space on any other disk partitions. Verify that these other drives have sufficient space. The recorder will warn you if they fall below 500MB of free space. Accumulated temporary files or log files can account for this drop in available space. You may need to purge them manually.

ATTENTION

When you are purging files, remember that files you delete go to the Recycle Bin and that the space they occupy is not freed until you empty it.

Call detail database purging

If you have enabled automatic purging of aged call detail records (as described in [“Retain call details for \(months\)” on page 95](#)) you should still monitor the size of the calls database during the first few months of use. You can then predict how large the database will get by the time old records begin to be purged. Many customers plan never to purge call detail records, but choose instead to add disk capacity every year or two as the database grows. If you do this, you should upgrade your server every few years to compensate for the increasing size of the database and the reduction in search and update speed.

Configuration Backup

Changes to system configuration that affect user access rights are stored in the PostgreSQL database. This means that the system configuration is backed up whenever the call detail records are. See [“Backing up the Database” on page 115](#).

Monthly

Check the following aspects of the system on a monthly basis:

Loading trends

Note the total call volumes recorded every month to be aware of gradually increasing traffic trends. To do this:

- Note the number of calls recorded at the end of each month and compare with previous month's accumulated total.
- Note the age of the oldest call on the disk (only applicable once the disk has filled for the first time)
- Note the CPU load during busy hour

If it appears that the load is increasing, consider purchasing extra licenses if required and/or increasing server specification or disk space.

Every Six Months

The recorder must perform a full vacuum on the database to avoid wrapping transaction identifiers. When six months have passed since the previous vacuum the recorder will automatically perform the maintenance the next time that it is restarted. To remind you to schedule a restart, the system will issue daily warnings that it needs to be restarted. If for some reason you need to restart your system, and would prefer not to have the vacuum process start, you can defer it using the check box on the General Setup › Recorder page. This setting only defers the maintenance once. To defer again, reset the option. However you must allow the recorder to perform this essential maintenance task within 30 days.

Best Practice: Restarting Servers

Occasionally, you will need to restart your Contact Recording servers. In an environment where the Nortel Contact Recording system includes Quality Monitoring, you need to be careful when restarting both Nortel Contact Recording and Quality Monitoring servers.

If you take down both servers at the same time, it is important that you do not get one partially started, then take the other down. This will interfere with the DN registration process on the Nortel Contact Recording Server and can create a situation where the server cannot record calls and no contacts will have the audio icon.

To restart both servers successfully:

- 1 Stop the Nortel Contact Recording service on the Nortel Contact Recording Server. You do not need to reboot the server.
- 2 Restart the Quality Monitoring serve.
- 3 Confirm that the Quality Monitoring services start properly.
 - Quality Monitoring Apache Tomcat
 - Quality Monitoring Command Service
 - Quality Monitoring Naming Service
 - Quality Monitoring Search Service
 - Quality Monitoring BDR Service
 - Quality Monitoring eRecorder Audio Service
 - Quality Monitoring eRecorder Service
 - Quality Monitoring eRecorder Video Service
- 4 After the Quality Monitoring Services have started, start the Nortel Contact Recording service on the Nortel Contact Recording Server.

Note: Do not start the Nortel Contact Recording service until ALL Quality Monitoring Services have started.

- 5 Wait for registration of DNs to take effect with Contact Center 6. This can take up to 45 minutes in some instances. The registration occurs at a measured pace to avoid overload on the switch.

Use the CTI Monitors tab in the Contact Recording Recorder Status screen to verify that the registrations complete successfully.

> CONTACT RECORDING

REFRESH

Help

Change

Operations

Alarms

General Setup

System

Replay

Summary

CTI Monitors

Channels

is : CTI Monitors

the DNs and/or Position IDs being observed via CTI.

TN▼▲	Part of Range▼▲	Agent▼▲	Active Calls▼▲	Channel▼▲	Qual▼▲	Desktop▼▲	Rec▼▲
4-0-0-9	N/A	N/A			3813		No
4-0-0-14	N/A	N/A			3814		No
UNKNOWN	N/A				3815		
152-0-1-4	3914	N/A			3914		No
152-0-1-5	N/A	N/A			3915		No
152-0-1-7	3916	N/A			3916		No
152-0-1-8	3919	N/A			N/A		No
UNKNOWN	4114				4114		
UNKNOWN	N/A				4115		
UNKNOWN	4116				4116		
UNKNOWN	4119				N/A		
4-0-0-9	N/A	N/A			5013		No
4-0-0-14	N/A	N/A			5014		No
UNKNOWN	N/A				5015		
UNKNOWN	N/A				8713		

The relevant DNs/Pos IDs are changing from an unknown state to having a TN assigned.

Important: During the registration period DO NOT reboot or restart the Quality Monitoring server or critical QM services.

- Once all DNs are registered, make a test call.

Note: Remember that all Call Center agents must log out and log back in again to ensure the correct status display in Quality Monitoring. If an agent logs out while the system is restarting, the system will not recognize that they logged out; it will still show them as logged in and as a result, may continue to try and record against that agent.

Chapter 8

Advanced Configuration

In this chapter

Properties File	139
Contact Recording Desktop (CRD)	145
Customizing Search and Replay	155
Installing a Signed SSL Certificate	159
Installing Unlimited Strength Encryption	162

Properties File

A number of system settings can be changed from their default values by placing entries in the properties file as described below and should only be modified if specified by Nortel:

- this is a plain text file, located in the installation path and with filename:
 \properties\cs.properties
- you can edit this file using Notepad or other text editors.
- the Nortel Contact Recording service reads this file as it starts, so any changes made to the file will not take effect until you next restart the service.
- the file is normally empty as all settings default as shown in the table below
- entries are in the form entry=value
- blank lines and lines beginning with a pound (#) are ignored.

Entry (case sensitive)	Default	Meaning
audit.purgemonths	3	Number of months to retain audit trail records.
callid.wrapphours	12	Number of hours after which a call id might be reused - and hence earlier records of this call cannot refer to the current call. If the callids on your switch are wrapping in less than 12 hours, you should consider reducing this parameter to avoid mis-tagging - especially if using "record.persistmode=call"
carrier.ignore.ttt.nn.cc (CS2x00/DMS only)	false	Ignore calls on the trunk connected to PM Type ttt, PM number nn, Carrier number cc.
controllerlistener.localport	8232	TCP Port number the Nortel Contact Recording Master listens on for connections from Contact Recording Desktop applications.
cs.diskmanager	true	Whether to delete oldest calls when needed to create space for new recordings.
cs.forcesecure	false	If true, only https access is allowed. Requests to http port (8080) are redirected to 8443.
cs.logkeepdays	30	How many days to retain log files before they are purged (overnight).
disk.stopatMB	10	Stop writing to disk if free space is less than this many MB
disk.warnAtMB	500	Raise warning if free disk space falls below this many MB.

Entry (case sensitive)	Default	Meaning
dms.alarmlimit	5	Specifies the minimum call duration (in seconds) for which an alarm will be raised if no RTP packets have been received when the call ends. Set to 0 to disable this alarm.
dms.maxchannels	400	Number of duplicate media streaming channels that are created at startup. Reduce for lab systems or if some lower spec machines are used so that load-balancing works effectively.
dnis.mapsize	10000	How many entries to hold in dnis map. Two maps held and alternates between them.
dn.regpersec (CS2x00/DMS only)	10	How many DNs/Position IDs to attempt to Associate per second. Increasing this number speeds up initial startup but will impact the switch more during this period.
email.minalarmlevel	0	Determines minimum severity of alarm/event that is sent by email (if configured). 0=INFO and higher, 1=WARNING and higher, 2=MINOR ALARM and higher, 3=MAJOR ALARM only.
eqb.connecttimeout	60	Seconds that the Nortel Contact Recording Master will attempt to connect to Nortel Quality Monitoring control port on startup before reporting failure.
eqb.inactivitytimeout	30	Seconds of inactivity before the link to Nortel Quality Monitoring's control port is declared faulty.
eqb.maxchannels	160	Maximum number of channels between Nortel Quality Monitoring and Nortel Contact Recording Master/Standby. Should only be changed for lab systems - where it can help reduce the size of log files.
eqb.reconnecttimeout	30	Seconds that the Nortel Contact Recording Master will attempt to reconnect to Nortel Quality Monitoring's control port before reporting failure to reconnect.
eware.password	Not disclosed	Password to use when accessing Viewer database.
eware.recorderhostname	NULL	Name by which the recorder is entered into Viewer rather than its fully qualified IP name. Should not be needed.
eware.user	Not disclosed	Username to use when accessing Viewer database

Entry (case sensitive)	Default	Meaning
execmode.deletedelaymins	0	Minutes to wait after a recording ends for a "retain" command before deleting a call on a DN or Position ID requiring manual retention.
icm.acceptabledelay (CS2x00/DMS only)	350	Milliseconds considered an acceptable delay from ICM feed. Response slower than this will raise a warning.
icm.dnlength (CS2x00/DMS only)	10	The number of digits in a station number. Any number entered with this many digits is assumed to represent a DN. A different number of digits implies it is a position ID.
icm.inactivitytimer (CS2x00/DMS only)	150	Seconds of silence on ICM link(s) after which failure is reported. If no other traffic is present, the recorder will send Application Status message 3 times (at interval given by poll.retry) before this timer expires.
icm.logfile (CS2x00/DMS only)	NULL	The filename (within the /logs folder) to read ICM input from or write it to.
icm.offline (CS2x00/DMS only)	false	If true, read ICM input from the file specified in icm.logfile. Otherwise connect to live ICM/ Linkplexer feed(s).
icm.pollinginterval (CS2x00/DMS only)	120	Seconds between polls to ICM. Specification advises no more frequent than once in 120s.
icm.pollretry (CS2x00/DMS only)	10	Seconds between successive ICM Application Status polls.
log.annotate	false	Set true to have each administration web page display an annotation field and buttons allowing the user to submit entries for insertion into the log file(s) from their browser.
loop.ignore.nn (CS1000 systems only)	false	Ignore calls on loop number nn (1-255). Add one entry for each loop that is not recorded on a partially equipped trunk-side recording system. Otherwise alarms will be generated as the recorder attempts to record calls on these loops.
master.connecttimeout	120	Seconds that a master or standby recorder will wait on startup before reporting a previously known Nortel Contact Recording recorder as faulty.
mls.acceptabledelay (CS1000 systems only)	200	Report warning if response takes longer than this (in milliseconds)
mls.pollinginterval (CS1000 systems only)	20	Time (in seconds) between poll messages with MLS.

Entry (case sensitive)	Default	Meaning
ncr.connecttimeout	60	Seconds that the Nortel Contact Recording Master will attempt to connect to other Nortel Contact Recorders on startup before reporting failure.
ncr.inactivitytimeout	30	Seconds of inactivity before the link to other Nortel Contact Recorders is declared faulty.
postgres.password	Not disclosed	Password to use for vacuumer to access local postgresql database.
qcm.keepwav	false	Whether to retain Quality Monitoring recordings in the recorder's call path.
rec.noip	false	Set true to disable all IP recording - forcing the system to use TDM or Call Recording Card recording as available.
record.alwaysmix	false	If true, mix recordings even if the if these are received in a format that would not normally be mixed. even if the if these are received in a format that would not normally be mixed.
remoteids.localport	1414	TCP Port number the Nortel Contact Recording Master listens on for connections from other Nortel Contact Recording IP recorders
queue.xxx.threads	1	Number of threads to use for job queue xxx.
rec.mincallduration	250	Calls shorter than this many milliseconds are deleted.
record.deletedelaysecs	10	Set the number of seconds the recorder waits between the end of a recording segment and deleting or retaining it.
record.persistmode	dn	Use this setting to choose between “call”, “dn” and “segment” persistence of recording commands. See Section “Contact Recording Desktop (CRD)” on page 145 for further details.
recorder.pool	NULL	Use this to have this recorder form part of a “named pool” of recorders - which will load share and/or provide fault tolerance. Set this property to a short string that is the same on all recorders in this “pool”. Once set, you can specify this name in the “Designated Recorder/Pool(s)” Advanced setting for bulk recording.
replay.export.admin	true	Whether administrators are allowed to export recordings.

Entry (case sensitive)	Default	Meaning
replay.export.all	false	Whether non-administrators are allowed to export recordings.
rtp.lowport	10000	Lowest port number used for IP recording. Note each recording uses FOUR ports.
rtp.highport	20000	Upper limit on ports user for IP recording. Ports up to but not including this port will be used. Note: each recording uses FOUR ports.
rtp.packetlog	false	If true, log details of every RTP packet received.
siu.connecttimeout	60	Seconds that the Nortel Contact Recording Master will attempt to connect to Nortel Quality Monitoring's CTI event port on startup before reporting failure.
siu.ignoreinternal	false	Set to "true" if you have are using TDM trunk-side recording and hence cannot record internal calls. This will suppress messages to the Quality system regarding internal calls. Otherwise these will result in alarms indicating failure to record calls.
siu.ignoreuntappedtrunks	false	Set to "true" if you have are using TDM trunk-side recording but do not have ALL trunks tapped. This will suppress messages to the Quality system regarding calls on trunks that cannot be recorded. Otherwise these will result in alarms indicating failure to record calls.
siu.inactivitytimeout	30	Seconds of inactivity before the link to Nortel Quality Monitoring's CTI event port is declared faulty.
siu.reconnecttimeout	30	Seconds that the Nortel Contact Recording Master will attempt to reconnect to Nortel Quality Monitoring's CTI event port before reporting failure to reconnect.
snmp.port	4161	Port on which recorder listens for SNMP.
sso.dc	NULL	The IP address of the domain controller to use for Single Sign On. (Incompatible with sso.domain.)
sso.domain	NULL	The domain name to use for Single Sign On. (Incompatible with sso.dc.)
sso.wins	NULL	The IP address of a WINS server to use to locate domain controllers. (Mandatory with sso.domain.)

Entry (case sensitive)	Default	Meaning
standby.localconfig	false	Whether the standby is locally configured. If not, it copies config from the Master.
unify.connecttimeout	60	Seconds that the Nortel Contact Recording Master will attempt to connect to external controllers on startup before reporting failure.
unify.inactivitytimeout	30	Seconds of inactivity before the link to an external controller is declared faulty.
unify.reconnecttimeout	30	Seconds that the Nortel Contact Recording Master will attempt to connect to an external controller on failure of a link before reporting failure to reconnect.
usage.reporting	false	Whether to track actual usage to the ConfigHistory table.
viewerx.limit	100	Maximum number of recordings returned for each search.
viewerx.savesettings	false	Whether to save and reuse user's previous entries in search filter pane.

Contact Recording Desktop (CRD)

Overview

The Contact Recording Desktop (CRD) application is a simple application that normally resides as an icon in the tool tray of agents' desktop PCs. You determine which of the following features are available to each user by editing an XML file as described later in this Section.

- Start recording button
- Stop recording button
- Submit/Update button to “tag” call with details the user has entered into the customizable fields shown to him on the form. These can be text fields, selection lists or checkboxes.
- Delete recording button (IP recording only)
- Retain recording button (IP recording only)

The application can be configured to start when a user logs on to the PC. Each application that runs is associated with a single DN or Position ID using one of the following mechanisms:

- The user may log on by entering their AgentID
- The user may log on by entering the Position ID or DN that they wish to control

Note: Recording Position ID and DN at the same time is not supported.

- The user's Windows account name can be entered in a central configuration file and matched to a particular agent ID.
- The PC name can be entered in the central configuration file and automatically matched to a DN or Position ID

Status

The current status of the application and the DN or Position ID it controls is shown as follows:

- the left-hand status panel at the bottom of the main window shows whether or not the application is connected to the Nortel Contact Recording Master
- the third status panel shows whether or not the call is recording and provides feedback when commands have been issued to show whether or not they were successful.
- The right-hand status panel shows the DN or Position ID that the application is controlling.
- The icon in the tool tray also changes to show the current status of the application and the call in progress. Hold your mouse cursor over it to see the pop-up text that explains the current status.

Note: the buttons and menu options will be enabled or disabled according to both the configuration file and the current state of the call in progress.

Note: when the application is running and connected to the recorder, the context menu can be configured to show/hide the options available.

The application running in the tool tray lets the user control recording and tag recordings according to a configuration file that is set on the Nortel Contact Recording Master recorder. This determines which controls and fields are available to the user.

Persistence of Commands

When a user issues a command such as “start”, “stop”, “delete” or “retain” it is important that the user knows whether this relates to:

1. his interaction with this call ever - regardless of whether it is transferred to someone else and then back to him or not.
2. his interaction with this call until he disconnects from it - regardless of how many times he puts it on hold while doing something else
3. his interaction with this call now - and no longer applies if he puts it on hold and retrieves it again. (This latter mode allows him to deliberately return to the default behavior for the call.)

Use the properties file setting `record.persistmode=xxx` to choose between the three (“call”, “dn” and “segment” for (1),(2) and (3) respectively above). The default is “dn”



If using “call” persistence mode, it is the callid that is used to tie commands to calls. If callids wrap on your switch in less than 12 hours, you should set the properties file setting `callid.wraphours` to a value that is lower than the fastest time in which callids are reused. This will, however, limit the maximum duration over which commands can act.

Desktop Layout XML File on Nortel Contact Recording Master/Standby

The configuration of the CRD is primarily controlled by an XML file in the `\properties\desktops` folder in the installation path on the Nortel Contact Recording Master. This determines what options are available to the user and how the user-defined fields are presented to them. A default file, `dcs.xml`, is provided.

You may change this to have all users configured the same way or you can create different XML files and use the Advanced settings for a particular DN or Position ID range to have those addresses use a particular XML file.

Any changes you make to the XML file will be picked up the next time the user logs in to CRD.

Operations › Bulk Recording

The desktop configuration file(s) determine which options show on the application but you must also configure the Operations › Bulk Recording mode to allow the users to perform the operations that you enable. This is necessary because in future releases such operations may be performed directly from the phone rather than solely via the CRD application. As with the XML file, you can specify an overall set of rules (at the top of the Operations › Bulk Recording page) and then override this for specific DNs or Position ID ranges using their Advanced settings.

Client PCs

Either immediately after installation or ideally as part of the installation process, each client PC must be configured with the IP address of the Nortel Contact Recording Master recorder (and any standby) that it is to use. These settings - and others (which you may wish to provide initial values for so as to avoid an inconsistent first login) are held in the Windows Registry as follows:

Under HKEY_LOCALMACHINE\Software>ContactRecordingDesktop

Registry Keys	Type	Default Value	Comment
ServerAddress	String	127.0.0.1	IP address of Nortel Contact Recording Master to connect to.
ServerPort	String	8232	IP port on Nortel Contact Recording Master to connect to.
BackupServerAddress	String		IP address of Nortel Contact Recording Standby to connect to.
BackupServerPort	String	8232	IP port on Nortel Contact Recording Standby to connect to.
LogonBypass	String	True	Whether or not to bypass the login dialog on startup. Will automatically be set to match XML configuration file after first login. ("true" or "false")
RecordingMode	String		Whether to ask for Extension or AgentID on login. Will automatically be set to match XML configuration file after first login. ("true" or "false")
HeartbeatEnable	String	True	Whether or not to send heartbeats to the server.
ConfigPwd	String	admin	Password needed for local configuration changes

Under HKEY_CURRENTUSER\Software\ContactRecordingDesktop

Registry Keys	Type	Default Value	Comment
Extension	String	Last extension this user logged in as	Only used if logonmode= “agent” in XML file
AgentID	String	Last AgentID this user logged in as	Only used if logonmode= “extension” in XML file

Command Line Options

As an alternative to setting the registry entries, you can specify the following options from the command line that runs the application. These are more often used for diagnosing problems e.g. running as if located somewhere else or under a different user account.

Command	Explanation
-a	log in with an agentID rather than extension number
-a <nnnnnn>	log in as agent ID nnnnnn
-x	log in with an extension number rather than an agentID
-x <nnnnnn>	log in as extension nnnnnn
-i <ipaddress>	Use the NIC with this IP address to connect to the server
-u <ipaddress>	connect to server at IP address ipaddress
-p <port>	connect to server using port specified
-h <hostname>	login as running on host name specified
-w <account>	login as running under windows account specified
-l d	login bypass disabled
-l e	login bypass enabled
-h e	heartbeat enabled
-h d	heartbeat disabled
-e e	login using extension rather than agent number
-e d	login using agent number rather than extension

Delayed Delete/Retain

By default, the recorder decides whether to delete or retain a recording segment 10s after the segment is completed e.g. when the Hold key is pressed or when the call terminates. If you wish to delay this decision so that users can click the “Retain” button on their CRD application after the call has completed, you must set the properties file entry “record.deletedelaysecs”. The decision to delete a recording segment is then delayed by however many seconds is specified.

Note that a recording that has been “retained” after the above period can still be deleted at any time up to the call id wrap time. After this time a callid may have been reused and hence it is not safe to perform a deletion using the callid alone to identify the recordings associated with a particular call. The default period in which call ids are assumed to be unique is 12 hours but if your switch is busy, call ids may be reused more frequently than this. Use the property file setting “callid.wraphours” to reduce this time period. You should set it to less than the time in which call ids are reused but longer than the longest call that you need to tag, delete or retain. Note that delete and retain commands use the “owner” field of a recording. A delete command issued by a desktop application will delete the previous recording “owned” by that DN/PositionID. If you override the owner field with the advanced settings, the delete and retain functions will effectively be disabled.

Fault Tolerant Configurations

When using a Standby recorder:

- Set its address in the Configure dialog.
- Copy the configuration files from your \properties\desktops folder to the standby any time you change them on the master.

XML Configuration File Format

The default file provided (dcs.xml) shows all possible options for user defined field entry.

ATTENTION

dcs.xml must not be modified. It is overwritten during upgrades. You will make your changes in files with different filenames (of your choice).

This default is shown below:

```
<?xml version="1.0" encoding="UTF-8"?>
<desktop>
<logon mode="extension" bypass="false" />
<pcs>
  <pc name="cbacer" extension="4114" />
  <pc name="another" extension="1234" />
</pcs>
<users>
  <user name="chrisx blair" agentid="6001" />
  <user name="john doe" agentid="2100" />
</users>
<udfs>
```

```

<udf name="spare1" label="First Field" type="fixed">
  <entry>Fixed Text Entry</entry>
</udf>
<udf name="spare2" label="Second Field" type="text">
  <mask>##/##/####</mask>
  <mask>[abcd]</mask>
  <mask>[!xyz]</mask>
  <mask>##/##/####</mask>
</udf>
<udf name="spare3" label="Third Field" type="list">
  <filename>spare3entries.txt</filename>
</udf>
<udf name="spare4" label="Fourth Field" type="list"
  extensible="false">
  <entry>First Choice</entry>
  <entry>Second Choice</entry>
  <entry>Third Choice</entry>
  <entry>Fourth Choice</entry>
</udf>
<udf name="spare5" label="Fifth Field" type="list"
  extensible="true">
  <entry>First Choice</entry>
  <entry>Second Choice</entry>
  <entry>Third Choice</entry>
  <entry>Fourth Choice</entry>
</udf>
<udf name="spare6" label="Sixth Field" type="checkbox">
  <entry>Checkbox label</entry>
</udf>
<udf name="spare7" label="Seventh Field"
  type="checkbox">
  <entry>First Checkbox label</entry>
  <entry>Second Checkbox label</entry>
</udf>
</udfs>
<buttons>
  <button name="start" mode="enabled" />
  <button name="stop" mode="enabled" />
  <button name="update" mode="enabled" />
  <button name="delete" mode="enabled" />
  <button name="retain" mode="disabled" />
</buttons>
<menu>
  <menuitem name="configure" visible="true" />
  <menuitem name="logoff" visible="true" />
  <menuitem name="exit" visible="true" />
</menu>
</desktop>

```

The individual fields within the XML file are defined as follows:

Logon

The <logon> field determines

- whether the logon form is presented or not (bypass="false" and bypass="true" respectively).
- whether the identifier used in the logon form is treated as a DN or Position ID (mode="extension") or anAgent Identifier (mode="agent")

PCs

If calls are taken on DNs or Position IDs that are fixed and hence are located next to a specific PC, you can list these physical relationships in the <pcs> field.

Rather than have each user specify a particular extension when they log in, simply set the logon bypass option as above and the system will identify the appropriate extension that corresponds to the PC from which the application is run.

Users

If, on the other hand, users log in to position IDs using a particular AgentID, this is often linked to their PC Windows Logon name and this too can be specified in the XML file.

If the user's logon name is found when they start the application, the Nortel Contact Recorder will automatically tie the application to the Agent ID specified in the XML file.

User Defined Fields

As shown above, each user defined field ("udf") is defined inside the outer <desktop> and <udfs> tags. Each such field has:

Name

This is how it will be stored in the XML file associated with the call recording. For compatibility with the Viewer database, you should use "spare1" through "spare7" as shown. Other fieldnames can be used but these will not be uploaded automatically to a Viewer database. Do not include spaces within these names as this is not valid XML.

Label

This is the text that will show on the desktop application to the left of the data entry field. This does not have to be in English but must only contain 8-bit characters.

Type

This will be one of the following:

Fixed - A single "entry" field determines the (fixed) text that will be tagged with the call should the user perform any tagging.

Text - The user may enter a text string to be tagged against the call. Optionally, you may include up to 6 "masks". These follow the syntax for the Visual Basic "like" command and hence can be any of:

- ? Any single character.
- * Zero or more characters.
- # Any single digit (0-9).
- [charlist] Any single character in charlist.
- [!charlist] Any single character not in charlist

List - This results in the user seeing a drop-down list. You can either specify up to seven individual <entry> fields or specify a file from which the entries in the drop-down list will be read. The <filename> specified is assumed to be in the same directory as the desktop application's executable file.

When using <entry> fields, you can also specify whether or not the user is allowed to enter their own text or is restricted to the available list.

Checkbox - One or more checkboxes will be shown, each labeled according to the “<entry>” fields.

Control Buttons

The application provides five command buttons, each of which can be enabled, disabled or completely hidden as shown in the XML file above.

Any button not specified in the XML file will be hidden.

Note: The “Update” button is labelled “Submit” until it has been used on each call.

Menu Items

A menu can be brought up by right-clicking over the CRD's icon in the tool tray. Several of the options on this menu reflect the configuration of the buttons as defined above and perform the same functions as clicking on the corresponding button.

Three additional menu items can be shown if required on this menu. These are:

Configure - If this is made visible, the user can bring up a dialog box allowing them to enter the IP address of the Nortel Contact Recording Master and Standby that the application will connect to. These details are subsequently stored in the Windows registry. If you can configure these details as part of your deployment, there is no need to let the user have access to this dialog. If you do enable the option, the user must still know the password (default is 'admin' but can be changed in the registry as shown in the tables in [“Client PCs” on page 147](#)).

Logoff - If this is made visible, the user can log off. Use this where desks are shared and it is important that a user logs off at the end of a shift or where Agent ID is used to tie the CRD to a specific position.

Exit - If this is made visible, the user can shut the application down. Otherwise it will be running permanently (unless stopped via Task Manager or similar).

User Defined Fields

The recorder can store any number of user-defined fields (UDFs) in its internal PostgreSQL database. You can search on these fields using the Search and Replay web application. The UDF is a customizable feature of Contact Recorder. To implement this feature, contact Professional Services to have a quote generated.

Storing UDFs

Use an external controller to TAG calls using the interface described in Appendix D, “Recorder Control Protocol.” The database automatically notes new UDFs and stores the call's details.

Search and Display UDFs

To search on and display UDFs, copy the browse query (named “browse”) in the postgres database to a new file that you will use to create a new query. Name this “browse2” or something more descriptive.

Use the stored procedure `udf_value(inum, udfid)` to add the chosen UDFs to the new view.

For example, the following fragment of SQL inserted into the SELECT statement's list of fields adds an additional column called `spare1`:

```
... udf_value(calls.inum, 1) AS spare1
```

The `udfid` is determined by searching the `udfnames` table for the relevant `udfname`. The `spare1` column is then available to be used in a customized search and replay view as described in [“Customizing Search and Replay” on page 155](#).

UDF Support in Viewer

UDF support in this recorder compared to UDF support in EWare has the following advantages:

- Unlimited number of user defined fields.
- Unlimited length of each user-defined field.
- User defined search forms created by editing the xml templates rather than the end-user interface available within Viewer.
- Better support for sparsely populated data sets in which there are more user-defined fields, but not every call has every field present.

Viewer Compatibility

If you name your user defined fields `spare1` through `spare7` you can upload them to a Viewer database as well as have them in the local database. The name by which the users see these fields can be set in the template files.

Customizing Search and Replay

By renaming and modifying the layout files provided with the Search and Replay application, you can define search forms and results display list formats. You can also provide alternate language translations for the fields and columns shown.

Default Configuration Files

The default layout is determined by two files located beneath your install directory in \properties\layouts:

- lcs.xml is the default layout
- idefault.xml is the default internationalization file

ATTENTION

lcs.xml and idefault.xml must not be modified. They are overwritten during upgrades. You will make your changes in files with different filenames (of your choice).

Note: The web server picks up changes that result from additional files being placed in this folder within a minute. There is no need to restart. However, it makes sense to make these changes when there are no users on the system.

Custom Layout Files

Layout files are very straightforward. Each file specifies a single “layout”. The filename must be of the form: l<something>.xml. The default, lcs.xml is shown below:

```
<?xml version="1.0" encoding="UTF-8"?>
<layout name="csn" display="ldefault">
<view>browse</view>
<filters>
  <filter type="date"
    dbName="startedat" display="fdate"/>
  <filter type="string"
    dbName="partynames" display="fparty"/>
  <filter type="string"
    dbName="partyagentnames" display="fagent"/>
  <filter type="duration"
    dbName="duration" display="fduration"/>
  <filter type="string"
    dbName="vdn" display="fdnis"/>
  <filter type="number"
    dbName="callid" display="fcallid"/>
  <filter type="callset"
    dbName="csnames" display="fcallset"/>
</filters>

<columns>
  <column dbName="startedat" columnWidth=""
```

```

        formatType="DATE" display="cdate"/>
    <column dbName="duration" columnWidth=""
        formatType="TIME" display="cduration"/>
    <column dbName="partyagentnames" columnWidth=""
        formatType="" display="cagent"/>
    <column dbName="partynames" columnWidth=""
        formatType="" display="cparty"/>
    <column dbName="vdn" columnWidth="" formatType=""
        display="cdnis"/>
    <column dbName="callid" columnWidth="" formatType="ID"
        display="ccallid" enableLikeSearch="true"/>
</columns>
</layout>

```

The outer tag is <layout>, within which the internal name of the layout is given by the “name” parameter and the display name token is given by the “display” parameter.

It makes sense to name the file l<internal name>.xml but this is not mandatory.

The web application presents the layouts in alphabetical order by internal name in the layout name drop list box.

There are 3 inner tags:

- **View:** The name of the query on the database
- **Filters:** The filters for the left panel
- **Columns:** The columns for the grid display

Inside the outer “filters” tag, there are many “filter” tags. Each must have the following:

- a type, which can be a string, number, date or duration
- a column name matching one of those in the specified database view
- a display token which is looked up in the internationalization file.

Inside the outer “columns” tag there are many “column” tags. These must have a column name, width, format and display. They may optionally have an enablelikesearch flag. See the default above for all valid display types.

Widths may be valid HTML table widths (that is, “nnnpx” for pixels or “mm%” for percentages). However, it is better to leave these blank and let the browser decide.

If “enablelikesearch” is “true” the application displays this field as a hyperlink that, when clicked, executes a search for all calls (+/- one day) which have exactly the same data in this column as the call clicked upon.

(The example use of this is for call id – which you can click on to find all recorded segments of this call).

Internationalization

The file “idefault.xml” contains translation strings that allow you to format the output in any language. The current default is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<tokenset>
  <language lang="en">
    <token tid="ldefault">Default Layout</token>
    <token tid="fdate">Call Start Range</token>
    <token tid="fparty">Parties</token>
    <token tid="fagent">Agent</token>
    <token tid="fduration">Length</token>
    <token tid="fdnis">DNIS</token>
    <token tid="fcallid">Call ID</token>
    <token tid="fcallset">Call Set</token>
    <token tid="cdate">Call Start</token>
    <token tid="cduration">Len</token>
    <token tid="cagent">Agent</token>
    <token tid="cparty">Parties</token>
    <token tid="cdnis">DNIS</token>
    <token tid="ccallid">Call ID</token>
  </language>
</tokenset>
```

It has an outer tag <tokenset> with inner tags <language>, which in turn have inner tags <token>.

Note: The naming convention adopted is as follows: the display tokens for layouts begin “l”, for filters “f” and for columns “c”. This is only a convention.

When the application wants to display the name of a layout, it looks up its display token in the internationalization maps by name, according to the user's language preferences set in the browser.

For example, lcs.xml has the display token ldefault, the string for which (in English) is “Default Layout”.

To change/add strings you can supply a file called icustom.xml. This file must contain a tokenset, as described above. It is merged with the tokenset in idefault.xml. Because the file icustom.xml is read after idefault.xml, any duplicates will use your values rather than supplied defaults.

For example, if your French users dislike the default translation of call ID (ID d'appel) and would prefer “ID”, then supply an icustom.xml with the following:

```
<?xml version="1.0" encoding="UTF-8" ?>
<tokenset>
  <language lang="fr">
    <token tid="ccallid">ID</token>
  </language>
</tokenset>
```

This text provides the override of the original value, and the column displaying call id is now labelled ID.

If you are designing additional layouts, you may use any or all of the supplied token ids and these will be translated from the default file.

If you wish to label things differently, you may think of additional token ids, use those in your layouts and provide translations for them in your icustom.xml. You only need to provide translations for your own languages.

However, if you wish to override the default layout, you may create an l<something>.xml file with a valid layout in it, and give that layout the name “cs”.

This file replaces the default layout.

Note: Do not call your file lcs.xml. If you do, your file will be overwritten during upgrades.

Examples

To change the labels shown

Create a icustom.xml file and override the ones you do not like

To change the order of the columns

Copy lcs.xml to lscust.xml. Edit the latter and delete columns or change their order. As you have not changed the name of the layout, it replaces the default one and you still have only one layout.

To create additional layouts

Copy lcs.xml to l<something>.xml. Edit the latter and change the <layout> tag to give it a new name and a new display name. Make other changes as necessary. The new layout appears in alphabetical order by internal name. Create an icustom.xml. Add a translation for the display name token that you gave your new layout.

Installing a Signed SSL Certificate

If you want to install your own SSL certificate, you must replace the certificate distributed with Nortel Contact Recording. Your replacement certificate must be specific to your installed server.

Selecting a Certificate Authority (CA)

If you do not already use a certificate authority, you can use:

- <http://www.freessl.com/startersssl/startersssl.html> - FreeSSL requires that the web server has a fully qualified domain name (e.g. contactrecorder.bigcorp.com or contactrecorder.division.bigcorp.com) and needs to be able to send an E-mail to an address like ssladmin@bigcorp.com or administrator@division.bigcorp.com. The list of addresses can be found on their Web site, and it includes admin, ssladmin, root, and administrator. This provides a free 30 day trial after which you will have to purchase RapidSSL.
- <http://www.instantssl.com> - InstantSSL is more flexible and allows intranet addresses (such as WINS names and IP addresses) as well as fully qualified domain names.

Backing up the Keystore file

In the instructions which follow, replace <installdir> with the location into which you installed Nortel Contact Recorder – for example \Nortel\Contact Recording

The certificates and keys are stored beneath your installation folder in the file:

<installdir>\keystore\keystore.jks

Because this file contains the original, distributed certificate, it is important to make a backup of it. You will delete this file during the remaining steps. Should it be necessary to restore the original certificate, you can copy the backup to the original filename.

Creating the new Certificate

If you would like to test this implementation, you can practice this procedure with a certificate authority's 30-day trial certificate. Then, to implement real certificates, you can start over from this point.

To create a certificate:

- 1 Create a new certificate with the real URL of the Nortel Contact Recorder
- 2 Open a DOS Command window and change directory as follows:

```
cd <installdir>\keystore\conf
```
- 3 Remove the original keystore file

```
del keystore.jks
```
- 4 Run the java keytool utility with

```
..\..\jre\bin\keytool -genkey -keystore keystore.jks -alias tomcat -keyalg RSA
```

- 5 Fill in the Keytool prompts with the following:
Password: Contact5tor3
Note: You must type this password, exactly as shown. It is case sensitive.
 - a. First & Last Name: <enter the FQDN, IP address or intranet name>
 - b. Organizational Unit: <enter your division>
 - c. Organization: <enter your company name>
 - d. City/Location: <enter your location>
 - e. State/Province: <enter your state>
 - f. Country Code: <enter the ISO 2 letter code for your country (for example, GB is the code for United Kingdom)>
- 6 Enter yes if the information is correct.
- 7 Hit enter when prompted for the second password.
- 8 Restart the Nortel Contact Recording service.
- 9 Access the Administration pages via https.
- 10 Check that the certificate matches the information entered.
- 11 Double click the padlock icon. Internet Explorer should warn you that the certificate is unsigned. However, it should no longer display a message that indicates the certificate does not match the web server name.
Tip: If you do get a warning that the certificate does not match, check that the Common Name matches the URL. Double click the padlock, select the details tab, and click the Subject line. This displays the Common Name.

Generating a Certificate Signing Request

You need a Certificate Signing Request (CSR) as the first step of the signing process. When you have it, paste it into the Certificate Authority's web page. To generate a CSR:

- 1 Re-run the keytool command

```
<installdir>\jre\bin\keytool -certreq  
-keystore keystore.jks -alias tomcat
```
- 2 Enter the password – which is Contact5tor3.
- 3 Copy and paste the output into the CA's web page. (Include the BEGIN and END lines.)
- 4 Complete the verification process
- 5 Reply to the verification E-mail and other verification steps until you obtain a signed certificate back from the CA.

Importing the CA's certificates

Before you can import your certificate reply, you need to import the certificate authority's root certificate and any intermediate certificates between their root and your certificate.

To acquire these certificates:

- 1 Download these certificates from the certificate authority's Web site.
- 2 Save the root as rcert.crt and any intermediate as icert.crt.

To import all your certificates:

- 1 Import the root certificate by running keytool:

```
<installdir>\jre\bin\keytool -import  
-keystore keystore.jks -alias root -file rcert.crt
```
- 2 Enter the password - which is Contact5tor3.
- 3 Import the intermediate (if required).

```
<installdir>\jre\bin\keytool -import  
-keystore keystore.jks -alias inter -file icert.crt
```
- 4 Import your signed certificate.
- 5 Save the file the CA sent as cert.crt.
- 6 Import with the keytool.

```
<installdir>\jre\bin\keytool -import  
-keystore keystore.jks -alias tomcat -file cert.crt
```
- 7 Test with the browser.
- 8 Restart the Nortel Contact Recording service.
- 9 Access the administration pages using https.
- 10 Double click the padlock icon and ensure that Internet Explorer no longer displays a message that the certificate is unsigned.

Backing up the keystore file

The keystore file now contains:

- the random private key that is unique to this web server
- the signed certificate you just paid for

These two are linked and cannot be regenerated, so it is important to back up the keystore file. If either one of these components is lost, you must regenerate the certificate and pay again to get it signed.

Installing Unlimited Strength Encryption

To support key sizes larger than 128 bits, you will need to replace the standard Java Jurisdiction Policy Files using the following instructions:

- 1 Using your browser, go to the following link:

http://java.sun.com/javase/downloads/index_jdk5.jsp

- 2 Follow the link entitled:

Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 5.0 at the foot of the page.

- 3 Download and unzip the files.
- 4 Follow the instructions in the readme.txt. (The path for installation is ...jre\lib\security).

Note: You should back up the existing jars that will be replaced

Appendix A

Technical Reference

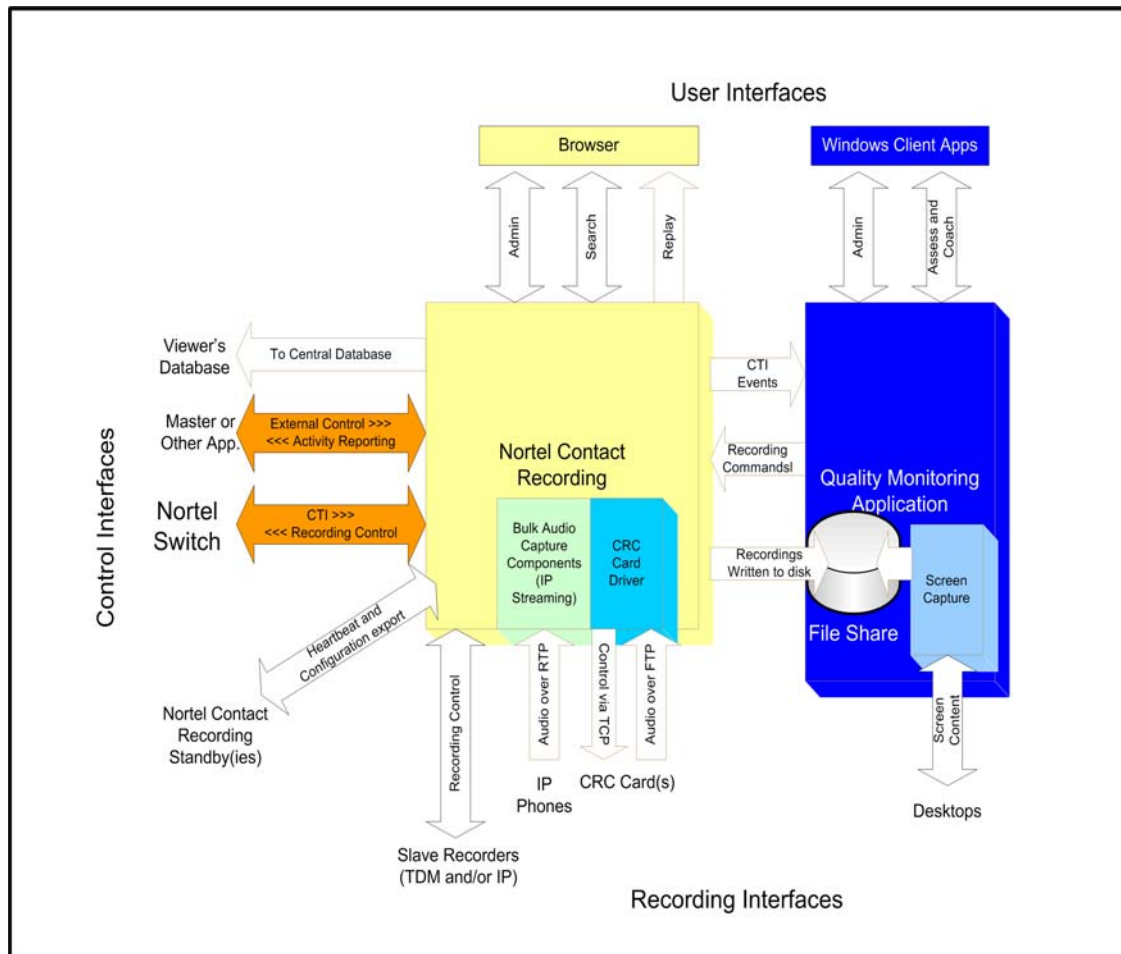
In this appendix

IP Recorder Interfaces

165

IP Recorder Interfaces

The Master recorder in each system determines which calls to record and how to 'tag' these calls for future retrieval. This recorder controls a number of recording channels that may be on the Master recorder itself or on any number of additional 'slave' recorders. The interfaces supported by the recorder are described below (working clockwise round the diagram, starting at top left)



Administration

Administration uses an HTTP and/or HTTPS interface (on ports 8080 and 8443 respectively) that provides administrators with access to configuration and status monitoring pages.

Search

Search uses an HTTP and/or HTTPS interface (on ports 8080 and 8443 respectively) that end users access to search for call recordings that match specific criteria.

Replay

Replay uses an HTTP and/or HTTPS interface (on ports 8080 and 8443 respectively) that end users and other applications (such as Viewer and Archive) access to retrieve the voice content of a specific recording.

CTI Event Interface

The recorder establishes a TCP/IP connection to port 1416 on the Nortel Quality Monitoring server. The recorder passes CTI events on to the Quality Monitoring application.

Recording Command Interface

The recorder establishes a TCP/IP connection to port 1415 on the Nortel Quality Monitoring server. The Quality Monitoring application instructs the recorder to record specific calls and, when using Call Recording Cards, to place telephone calls and perform live monitoring.

Recordings Written to Disk

After the recorder has completed each voice recording that the Quality Monitoring server requests, it queues a job for a background thread to copy the audio to a file share on the Quality Monitoring server.

Audio from Call Recording Cards via FTP (option on CS 1000 only)

When instructed by the recorder, a Call Recording Card passes voice data to the recorder using FTP. The recorder uses TCP/IP ports 11000 and up, 16 ports per card. Data is transferred using Active FTP, so the recorder makes TCP/IP connections back to the card using arbitrary ports at both ends.

Control of Call Recording Cards (option on CS 1000 only)

The recorder establishes a TCP/IP connection to port 6001 on each card. The recorder instructs the card to make recordings, place telephone calls and perform live monitoring of recordings.

Audio over RTP

When the recorder instructs IP phonesets to perform Duplicate Media Streaming, the voice packets are sent using RTP to the recorder. The recorder uses ports 10000 upwards, allocating four ports per recording channel (two for RTP and two for RTCP though the latter is used only for CS2x00/DMS systems).

TDM Slave Recorder Control

The Master recorder can control TDM 'slave' recorders. The Master establishes contact with TCP/IP port 1462 on each TDM recorder.

MLS, ICM or Linkplexer

Master and Standby recorders connect using TCP/IP to the MLS feed from the Nortel Contact Center Manager Server (CS 1000 systems) or to ICM or Linkplexer in CS2x00/DMS systems. These recorders interpret the telephony events occurring in real-time and whichever is active instructs the server to forward call data from the required IP phones to the required ports on the recorder(s) when calls are to be recorded.

External Control Interface

The recorder supports a simple TCP/IP command interface. This allows other applications to control recording directly and/or add further user defined data fields to recordings. This protocol supports START, STOP, TAG and BREAK (seamless stop and start) commands.

Database Upload Interface

The recorder uploads call details to a central Microsoft SQL Server database over this link. The recorder acts as a standard Microsoft SQL Server client application. It uses the TDS protocol, which uses TCP/IP port 1433.

Appendix B

Troubleshooting

In this appendix

Hints and Tips	169
Interpreting Log Files and Alarms (CS1000 systems)	171
Specific Problems	176

Hints and Tips

Where to Look for Clues

When problems occur, check the following:

- Emailed Alarms and Events. If you have been using the E-mail settings to have alarms and events forwarded to one or more E-mail addresses, you should check these carefully. As well as checking the contents of messages that you have received, also check for days when the daily heartbeat message has not been received.
- Alarms Page. This page within the administration application provides a wealth of information on problems that the system has detected. Review the alarms carefully. If the problem is not immediately apparent, consider viewing all alarms, including those that have previously been cleared. It may be that someone has cleared an alarm without addressing it or realizing its significance.
- Log Files. Check for errors being reported in log files within the following directories beneath your installation directory:
 - \logs
 - \tomcat5525\logs

Determining Current Version

When reporting problems you should state precisely which version of software you are running. To determine this, log onto the Nortel Contact Recording Server administration application as an administrator. Access the System > License page and read the exact version number from the row headed “Installed Version”. This provides information on the latest patch whereas the version information held in Control Panel is only to the last Build number.

Application Logs

The Nortel Contact Recorder writes log files to \logs beneath the directory into which it was installed. The current day’s log file is called cs.log. At midnight the current log file is closed, renamed to cs.log.<date>, and a new log file opened. These log files are automatically purged after 30 days.

You can set the level of messages logged by the Nortel Contact Recorder to DEBUG, INFO (the default), WARN, ERROR or FATAL in one of two ways.

To change the level permanently, enter the following line in the properties file cs.properties and restart the Nortel Contact Recording service to have it take effect.

```
log.level=DEBUG
```

If you change the log level in the properties file, it remains set on subsequent restarts. When logging at DEBUG level, note that the log files grow very quickly and can overflow the disk if left at this level. You may therefore also wish to change the number of days log files are retained. Set this with cs.logkeepdays=nn in the properties file.

To change the level temporarily, without restarting the service, simply use a browser to request the URL:

```
http://myrecorder:8080/log?level=DEBUG
```

replacing myrecorder with the name of your server.

You do not have to stop recording in order to change the logging level. To set it back again, enter the same URL, replacing DEBUG with INFO. The command is case-sensitive. Using this method changes the log level temporarily. It will revert to normal the next time that the system is rebooted.

Tomcat Logs

Nortel Contact Recorder uses the Tomcat web servlet container, which writes log files to `\tomcat5028\logs` beneath the install path.

Obtaining Support

Contact Nortel at the Nortel Networks Support Web site: www.nortel.com/callus

For other support options, please see the Technical Support area of the Nortel Web site: www.nortel.com/support

You may also contact Nortel by phone at either of the following numbers:

U.S. and Canada (toll-free): 800.466.7835

International and domestic (direct): 919.905.4210

Remote Access

You must provide remote access to the server to aid fault-finding.

Interpreting Log Files and Alarms (CS1000 systems)

The following information is helpful in interpreting DEBUG level log files and detailed alarm parameters on CS 1000 systems.

DN Status Codes

Use this table to isolate DN registration problems.

Error Code	Error Meaning
0502	Association table is full
0503	Application table is full
0504	Application already exists
0505	Bad Meridian 1 machine name
0506	Bad host machine name
0507	Requested service unavailable
0508	Bad Password
0509	Polling timeout
050A	Bad Meridian Mail Name
0703	DN for association does not exist
0704	DN table is full
0705	DN already registered
0706	Customer number must be registered to register DN(s)
0707	Cannot remove DN
0708	Bad DN type for DN registration
0709	Route member number out of range
070A	Invalid route
070B	Invalid trunk member
070C	Invalid route state
070D	Invalid trunk state
070E	Invalid device group
1002	Access restricted

Error Code	Error Meaning
1003	Resource unavailable
1004	Invalid customer number
1005	Invalid origination address
1006	Invalid destination address
1007	Invalid manner
2004	Invalid target Position ID
2005	AST is not configured on the agent set
2006	Invalid customer number
2007	The feature could not be invoked
2008	The feature is not configured on the set
2009	The requested feature is out of valid range
200A	The target set is not ACD agent
200B	The target set is a Virtual Agent
200C	The set is maintenance busy
200D	Set is in incorrect state for feature request
200E	Set is already in requested target state
200F	No NRDY/RDY while ACD set is logged off
2010	Package C customer unable to use NRDY with IDN call
2011	Feature IE is missing or invalid
2012	DN IE is missing or invalid
2013	Agent ID IE is missing or invalid
2014	Agent ID is invalid
2015	CFW DN IE is invalid
2016	The Call Forward DN is too long
2017	The Call Forward DN is invalid
2018	User is invoking Call Forward
2019	MSB/MSI not supported for 500/2500 sets
201A	500/2500 ACD agent already changed status

Error Code	Error Meaning
201B	500/2500 ACD agent set is being rung
201C	User is manually logging on 500/2500 ACD set
201D	Meridian Link Server Option 209 is not equipped
201E	The agent has not been acquired
201F	The agent is already logged on
2020	The resource is already acquired by another application
2021	The resource is already acquired by this application
2022	The resource is not released
2023	The application is unable to acquire all the resources
2024	The resource type is unknown
2025	The AML is down
2026	The resource table is full
2027	The CDN is not configured to operate in controlled mode
2028	The Poll timer is out of range
2029	The resource ID length is too long
202A	Device disabled by administration
202B	No response to operation request
202C	Logon tries exceeded
2030	This release of the Meridian 1 software is not equipped to operate this feature
2031	The resource is not acquired by the application
2032	Registration not set up for request
2033	Internal error
2034	Bad resource ID
2035	No internal resource available
2036	Service not available on device
2037	Device not available
3457	The content of the 1st and 2nd SFI Start Record request on this TN does not match

Error Code	Error Meaning
3516	Feature cannot be invoked on a PBX set
3540	User_ID (TN+DN combination) is not valid
3541	The DN is not configured on supported terminal
3542	VTN is not registered with any IP hardware
3543	The set is configured with ICRD CLS
3545	The requested user is an IVR ACD agent
3546	The B1/B2 IE is in invalid format

Stop Record Reason Codes

Use this table to determine recording problems:

Error Code	Error Reason
2	Invalid FW on the IP Phone
3	Signalling Server Failure
4	CLS changed from ICRA to ICRD
5	AST configuration is removed
6	IP Phone is rebooting or deregistered with TPS
7	DACR commands are executed
8	Host Application de-acquired the User_ID

MLS Link Status

Use this table to determine the state of the MLS link:

Link Status	Meaning
1	Initializing
2	Waiting to be configured
3	Disabled
4	Temporarily out of service while associated link is being configured

Link Status	Meaning
5	Enabled but not connected. This means that the link is enabled on the Meridian Link Protocol. However, the far end is either physically not connected or not ready for communication
6	Connected. The link is established
7	Link pending verification

MLS Call States

Use this table to determine call states:

State	Meaning
0	UNKNOWN
1	ON_HOOK
2	OFF_HOOK
3	RINGING
4	ANSWERED
5	DISCONNECTED
6	UNRINGING
7	RETRIEVE
8	CALL_ID_CHANGED
9	TRANSFER_COMPLETED_TO
A	CONFERENCE_COMPLETED_TO
B	CONFERENCE_TO_SIMPLE
C	IVR_TRANSFER
D	HOLD
E	TRANSFER_INITIATION
F	CONFERENCE_INITIATION
10	CONSULT_INITIATION

Specific Problems

System Administration page problems

You may encounter problems as you access and use the System Administration application. This section lists those problems and suggests steps to take to correct them.

Cannot access the System Administration pages

If you cannot access the System Administration pages, try the following:

- Ping the server to confirm that connectivity is possible. If not, trace the network connections between client and server and double-check the server's IP address, default gateway etc.
- Use the numeric dot notation IP address instead of the hostname. If this works, then the hostname is wrong or cannot be translated by your DNS services. You may need to use a fully qualified node name, such as recorder.bigco.com.
- Use the browser installed on the server itself to access the application at `http://localhost:8080`.

If this works, then the problem is in the network between server and client. If it does not work, then the problem may be with the Tomcat web server.

Cannot log in

If you have trouble logging in, check the state of the Caps Lock key and make sure the username and password are being entered with the correct case.

If you can log in under another account, reset the password of the account having problems.

If nothing happens when you click the OK button, check that your Internet Explorer settings allow javascript to run. See [“ActiveX Control Download” on page 111](#).

Web pages appear “untidy”

If the forms on the System Administration pages and/or Search and Replay page appear to be out of alignment, or fields are truncated, check your desktop properties. If set to Large Fonts (120dpi), this will impact all Web site accesses not just the Nortel Contact Recorder pages.

To correct display issues:

- 1 Right-click on your desktop and select Properties.
- 2 On the Settings tab, click Advanced and set the DPI Setting to 96dpi.

On new laptops, especially those with 1400x1050 resolution screens, the DPI is often set to 120dpi. Using too small a window or too large a type (View > Text Size in Internet Explorer) can make the columns and headings on the web pages wrap where they would not normally.

Connectivity

E-mail alarm problems

Invalid entries in any one of the parameters used to define the E-mail settings will result in errors. To check this:

Try the settings you are using in a standard mail client, such as Outlook. Send a message using the account specified to prove that the settings are valid.

If E-mail messages have been working and then stop without any of the settings changing, verify that nothing has changed on the mail server. This problem occurs, for example, if your password has been reset or changed on the mail server.

If the Nortel Contact Recorder is not sending E-mail messages, it may be because it is not able to access the SMTP server. Check the network connections to the recorder.

CTI Link Connection Problems

Nortel Contact Recorder communicates constantly with the Contact Center Manager Server over the MLS link (CS1000) or the ICM/Linkplexer (CS2x00/DMS). If this link fails, alarms are raised.

If these problems are accompanied by other alarms that indicate a failure to send E-mail messages, then the problem is more likely to be with the recorder's network connection than with the CTI interface itself.

Nortel Contact Recorder to Quality Monitoring server problems

If the problems reported include mention of the file share:

- 1 Verify that the Quality Monitoring server is running.
- 2 Verify that the username and password previously in use are still valid. Try to access the fileshare from another machine using the username and password provided to the Nortel Contact Recorder.
- 3 You may need to change the NTLM settings of the Quality server. Set the LmCompatibilityLevel to 3. This key is located in the Windows Registry at HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

Nortel Contact Recorder to Viewer server problems

If you have problems connecting to the Viewer server:

- 1 Verify that the Viewer server is running.
- 2 Verify that the SQL Server is active on it.

Search and Replay problems (IP Recording only)

For most problems with Search and Replay, consider the following diagnostic approaches to narrow down the cause of the problem:

- 1 Search for a different call, for example, one that is more recent or older, shorter or longer.
- 2 Log in as a different user with different replay restrictions

Cannot access the replay application

If you cannot get to the login page, try accessing the page from a different machine:

- 1 From the same side of any firewalls.
- 2 On the same LAN if you are having problems with WAN access
- 3 From the same sub-net, if having problems from a different sub-net
- 4 From the recorder itself, if having problems from the same sub-net.

User replay restrictions do not work

If you have given a user account replay rights over a number of addresses but the calls from these stations are not listed when you enter a valid search that should include them, check the recording ownership. When an agent has logged on to a station that is being recorded, the calls recorded are “owned” by the agent number not the underlying Position ID or DN. Give the user replay rights to the range of agent IDs who have been using the Position IDs in question. In fact, in most cases, you should restrict access to a set of Agent IDs rather than station numbers.

Problems downloading ActiveX control

If you see error messages relating to ActiveX controls being downloaded-or blocked from being downloaded, your security settings may be too restrictive. See [“ActiveX Control Download” on page 111](#) for more information.

Problems displaying ActiveX control

If the ActiveX control downloads but displays a red cross on white background at top of page, upgrade to Internet Explorer 6.0. These symptoms have been seen on Internet Explorer 5.0.

Cannot log in

If you see the login page but cannot get past it:

- 1 Verify that Caps Lock is off and that you are entering the password with the correct case.
- 2 Log in as a different user
- 3 Confirm the spelling of your log in name with the system administrator and check that your account is still configured in the administration pages.
- 4 Ask the system administrator to reset your password. Log in with a blank password and change your password when redirected to the Change Password page.

Search returns no calls

If you get to the search page but no calls are returned when you perform a search:

- 1 Broaden your search criteria to confirm that you can at least find some calls. Start by requesting calls from any parties for today. If that shows no calls, extend the time period.
- 2 Try setting the date range back to at least the time you know you have seen call records for in the past.
- 3 Check that the system administrator has given you access to the correct calls. Your search and replay restriction may be wrong or too narrow for the search you are attempting.
- 4 Confirm that calls are being recorded. Follow the troubleshooting guidelines for recording problems if you suspect that the system is not actually recording or processing any calls.

Calls listed but cannot play them

If you can see the list of calls that matched your search criteria, but cannot actually play them, look at the area at the top of the browser page where the “graph” of the audio normally shows and match your symptoms to one of the following:

No Audio “graph”

This means that the call has not been retrieved from the recorder or DVD disk or has not reached the client PC.

- 1 Check the server logs for errors.
- 2 Note the call's 15 digit reference number (shown if you hold the mouse pointer just to the right of the radio button that you click to retrieve the recording. Search for that wav file in the calls path to confirm that the recorded file exists.
- 3 Check connectivity and available bandwidth to the client PC.

Audio graph stops in mid call

This implies that the transfer of data from the Nortel Contact Recorder to your client PC has been stopped or interrupted.

- 1 Request the same call again. There may have been a temporary network problem.
- 2 Request a different call. If the problem is only with one call, you may have a corrupt file on your hard disk.
- 3 Request the problem call from another PC on the same network. If the other PC can retrieve it successfully, assess the differences between the two client PCs; the problem is most likely at the client end.
- 4 Request the problem call from different sub-nets, ideally working closer to the Nortel Contact Recorder.
- 5 Request the call from the recorder server's own browser. If this works and the others don't, then the problem is likely to be in the network between server and clients.

Audio graph appears but no sound

The audio file has reached the client PC successfully; the problem is most likely to be with the PC's multimedia setup or current settings.

- 1 Verify that the PC has a sound card.
- 2 Play a wav file through Media Player or similar application to verify that the sound card is set up correctly.
- 3 Adjust any hardware volume and/or mute controls on the speakers/headphones.
- 4 Double-click on the icon in the system tray at the bottom right-hand corner of the screen to verify that the PC's software volume controls are not set to mute or very low.
- 5 Ensure you are not running any other programs that may be locking the sound card exclusively. If in doubt, shut down all other programs.
- 6 Try another similar PC. If that works, look for differences in the multimedia setup of the two PCs.

No New Recordings Playable

If you can replay old recordings but not newly made calls, there may be a problem with the recording and/or storage components of the system. Follow these steps:

- 1 On the Status › Summary page of the Nortel Contact Recorder's System Administration application, look at the counts for total calls recorded and calls recorded today.
- 2 Use Bulk recording mode to make a test recording.
- 3 Complete the recording and hang up.
- 4 Return to the Status › Summary page and note the Total call segments recorded today and Total call segments recorded to date (or since restart, if today). These counts should have increased by at least one, the recording that you just made. If the counts have increased, the Nortel Contact Recorder is processing recordings. This is probably a search/replay problem. See earlier sections for help.

Note: If these counts have not increased, the recording has not been successfully compressed and stored on the Nortel Contact Recorder or inserted into the call details database. Do the following:

- 5 Look for alarm messages that indicate problems with the recording channel or with file read/write or rename functions. The error message should indicate whether disk space or a directory access problem is the cause. Check that .wav files are appearing in the latest folder beneath the calls path as recordings are made.
- 6 Check disk space in all partitions. If any of these is 0 or less than 50MB, this may be the problem. Check for build up of log files. Check that the call details database hasn't exceeded the available space. Consider reducing the number of months of calls kept-use the "retain call details for (months)" setting on the Server configuration page to adjust this.
- 7 Look for alarm messages that indicate licensing problems. The recorder will not process any new calls if you have changed the MAC address, tampered with license settings or are running on a time-expired license. In all cases, you should obtain a new license key.
- 8 Check that the Tomcat server is running (Nortel Contact Recorder service).
- 9 Check for messages in the log files.
- 10 Reboot the server and watch for error messages on startup.

Partial recording problems

Since no hardware component in the system is dedicated to specific ports, any hardware problem is likely to affect all recordings equally. Therefore, if some calls are being recorded and are playable but others are not, the problem is probably in the configuration.

- 1 Recording Mode versus Recording Channel? Determine whether your problems relate to all channels of one or more recording modes or just to certain ports.
- 2 Check the configuration pages for the affected recording mode(s).
- 3 Calculate the range of stations carefully. For example, 11000 to 11010 is a range of 11 addresses, not 10.
- 4 Use the Status › Channels page to observe the ports on the recorder during your test calls. The port status should switch between ready and active (though never idle).

Appendix C

Alarms

In this appendix

Alarms	183
Alarms Table	184

Alarms

The Nortel Contact Recording system may generate the following Alarm or Event notification messages. These events are:

- shown on the Alarms › View Alarms page
- sent in E-mail messages as specified on the General Setup › Email Server page
- reported via the SNMP MIB
- logged to the recorder's log file cs.log

Alarms Table

Within messages, the strings XXX and YYY represent a specific parameter such as a DN number, an IP address etc. The table shows both the English text of the message (that appears on the Alarms page) and the underlying resource string that appears in the log file.

Entries within the table are sorted according to the text of the message.

Severity	Log File Entry	English Text on Alarm > View Alarms	Comments	Recommended Action
Major	alarms.callspath.invalid	Call storage path is invalid. Please change it under General Setup > Recorder.	When initially installed, this path is blank.	Specify the path the recorder should use to store recordings.
Major	alarms.cti.badinitalsend	IO Exception on initial transmission.	Could not transmit over the socket connection.	Check far end is listening. Check network connection is up.
Major	alarms.cti.cannotconnect	Cannot connect.	Could not establish a TCP/IP link.	Check address. Check server is up.
Major	alarms.cti.clientrelease	Link dropped by far end.		Check far end for problems or manual shutdown.
Warning	alarms.cti.configchanged	CTI Configuration changed. Dropping previous connection.	System is responding to change in configuration.	Nothing.
Major	alarms.cti.connectionfailed	Connection failed.	An established link has been dropped.	Check for neighboring events at each end of the connection.
Major	alarms.cti.error	Link to CTI on XXX reporting error: YYY	A problem occurred between the recorder and the Nortel Contact Center server.	Depends on error YYY reported.
Major	alarms.cti.heartbeatfailed	CTI link failed. Heartbeat lost.	No activity on the link for an unacceptable period.	Check network connectivity. Check health of component at far end.

Severity	Log File Entry	English Text on Alarm › View Alarms	Comments	Recommended Action
Major	alarms.cti.ioexception	IO Exception.	A socket error occurred on the link.	Check network integrity.
Major	alarms.cti.invalidparams	Invalid CTI Address: XXX	You have not specified an address for the Nortel Contact Center server. (CS 1000) or ICM/Linkplexer (CS2x00/DMS)	Enter a valid address on the General Setup › Contact Center Interface page.
Info	alarms.cti.providerok	CTI Services on XXX UP	Connection to CTI link server has been established.	Check earlier error message to determine why link failed earlier.
Major	alarms.cti.shutdown	Service shut down	The link has been shut down.	If not planned, check for reasons preceding this in the event log.
Warning	alarms.cti.slowresponse	Slow response from CTI link. DN XXX reg/unreg took YYYms.	Registration or unregistration of an address took longer than expected.	Check the recorder is not overloaded. Check the MLS link is not overloaded.
Major	alarms.cti.timeout	Connection timed out. Far end not responding.	The component specified has not responded; has not connected or reconnected within the expected time.	Check the network connectivity and the state of the component specified.
Major	alarms.database.cannotinsert	Cannot insert details of recording XXX into database.	Local postgresql database could not be updated with recording details.	Check log file for further detail. Catch XML file of the recording for analysis.
Major	alarms.disk.full	Disk full on partition 'XXX'.	Recording has stopped	Clear some disk space or add more space.

Severity	Log File Entry	English Text on Alarm > View Alarms	Comments	Recommended Action
Warning	alarms.disk.nearlyfull	Disk nearly full on partition 'XXX'. Only YYYYMB free.	Recording will stop if disk fills.	Clear some disk space or add more space.
Minor	alarms.dn.notobservable	Cannot observe DN/Position ID XXX. CTI Cause Code YYY	The recorder was not able to register for CTI events on the address shown.	CS 1000: Check the AST flag is set on the DN/Position ID. Check that the Meridian1 Machine name and number are correctly set. Check the MLS specification for specific cause codes CS2x00/DMS: Check that the DN has EMC set. Check that the address is in the same Business Group as the recorder.
Minor	alarms.dn.regdropped	Observation of DN/Position ID XXX dropped.	The recorder is no longer receiving CTI events for the position ID shown.	CS 1000: Check that the AST flag has not been removed. Check the MLS specification for meaning of each cause code. CS2x00/DMS: Check that EMC has not been removed from the DN.
Major	alarms.eware.diskload	Error advising Viewer database of disk insertion. Reason: XXX	Could not update the media tables within the central database.	Check the database is online and can be reached by the recorder.
Major	alarms.eware.linkdown	Viewer database server Link DOWN. Reason: XXX	Recorder cannot access the SQL server for central database upload.	Check server, SQL server instance and network connectivity.

Severity	Log File Entry	English Text on Alarm > View Alarms	Comments	Recommended Action
Info	alarms.eware.linkup	Viewer database server Link UP.	Recorder has accessed the SQL server for central database upload.	Check previous link down error message and address root cause.
Major	alarms.eware.tar	Error adding archive details to Viewer database. Reason: XXX	Could not update the central database with details of the archive file being prepared.	Check the central database is online and accessible to the recorder.
Minor	alarms.file.deletefailed	Failed to delete file XXX. Reason: YYY.	Could not delete uncompressed file or XML file.	Depends on reason code.
Minor	alarms.file.compressfailed	Failed to compress audio file for recording XXX. Reason YYY.	G.711 recordings are mixed and compressed at the end of a recording. This process could not complete.	Depends on reason given.
Major	alarms.file.xmlwritefail	Failed to write XML file XXX. Reason: YYY.	Could not write the XML file containing details of the call with unique reference number XXX.	Depending on the reason shown, check disk space; permissions on the folder etc.
Warning	alarms.file.notin db	XXX recordings up to and including YYY were not stored to database on last shutdown.	The recorder should truncate all active recordings and store them to the database on shutdown. This indicates that it failed to do so.	May be a quality recording (these do not get stored to the recorder's database) but if truncated, may be misinterpreted as "missing" on next startup.
Info	alarms.info.heartbeat	Daily heartbeat. System still running.	Only appears in E-mail notification not in Alarms page.	Nothing.

Severity	Log File Entry	English Text on Alarm > View Alarms	Comments	Recommended Action
Minor	alarms.dn.startrec	Recording Start failed on DN/TN XXX. Cause Code (hex):YYY	Could not start Duplicate Media Streaming.	Check the specific cause code against the list in Appendix A.
Minor	alarms.dn.stopnotif	Recording stopped on DN/TN XXX. Reason Code (hex):YYY	Duplicate Media Streaming stopped unexpectedly.	Check the specific cause code against the list in Appendix A.
Minor	alarms.dn.stoprec	Recording Stop failed on DN/TN XXX. Cause Code (hex):YYY	Failed to stop Duplicate Media streaming.	Check the specific cause code against the list in Appendix A.
Warning	alarms.dn.starttimeout	Timeout on recording start on DN XXX TN YYY	Did not receive prompt confirmation of Duplicate Media Streaming stopping.	Check recorder is not overloaded. Check CTI is not overloaded. Check network connectivity.
Warning	alarms.dn.stoptimeout	Timeout on recording stop on DN XXX TN YYY		Check recorder is not overloaded. Check MLS is not overloaded. Check network connectivity.
Minor	alarms.eqb.mix	Error mixing halves of recording XXX: YYY	Recording made for Quality monitoring cannot be decompressed and/or mixed into a single file.	Depends on reason YYY given.
Major		Licensed bulk recording capacity reached. Cannot record call on XXX.	Cannot record a call on the address shown. The recorder is already operating at its maximum licensed capacity.	Purchase and/or install additional capacity.

Severity	Log File Entry	English Text on Alarm > View Alarms	Comments	Recommended Action
Minor	alarms.license.quality	Quality Monitoring agent station license exceeded. Cannot record XXX.	You have attempted to record more agent stations in the past 30 days than your license permits.	Increase licensed capacity.
Major	alarms.master.linkerr	Error establishing link to Slave recorder on XXX: YYY	A previously identified slave recorder is no longer connected.	Check slave recorder is up and network connection viable.
Major	alarms.master.timeout	Slave recorder timed out: XXX at address YYY	The slave recorder specified has not responded; has not connected or reconnected within the expected time.	Check the network connectivity and the state of the slave recorder.
Major	alarms.master.serversocket	Error creating socket for slave recorder on port XXX. Reason: YYY.	Implies no network connectivity at all.	Check network cables and TCP/IP stack.
Major	alarms.primary.linkerr	Error establishing link to Standby recorder on XXX: YYY	A previously identified standby recorder is no longer connected.	Check standby recorder is up and network connection to it is viable.
Major	alarms.primary.serversocket	Error creating socket for standby recorder on port XXX. Reason: YYY.	Implies no network connectivity at all.	Check network cables and TCP/IP stack.
Major	alarms.primary.timeout	Standby recorder timed out: XXX at address YYY	The standby recorder specified has not responded; has not connected or reconnected within the expected time.	Check the network connectivity and the state of the standby recorder.

Severity	Log File Entry	English Text on Alarm > View Alarms	Comments	Recommended Action
Major	alarms.properties.notanumber	Property XXX in properties file is non numeric (YYY). Using default value instead.	An entry in the properties file, which should be numeric, is not a valid number.	Correct the specified entry in the properties file.
Major	alarms.queue.copy	Failed to copy to XXX. Reason: YYY.	NOTE: Further errors with the same root cause on the same path will only show here once every 24 hours. Check the log file if in doubt. Will cache files until problem is resolved then copy all outstanding.	Determine why recorder cannot write to the share.
Warning	alarms.queue.slowjob	XXX Job Queue individual slow job - took YYYms.	This activity took longer than expected.	May occur under startup conditions. If occurring later, check recorder is not overloaded.
Warning	alarms.queue.tooslow	XXX Job Queue backlogged. Delay currently YYYms but may go higher.	The recorder cannot process these jobs as quickly as is should.	May occur under startup conditions. If occurring later, check recorder is not overloaded.
Minor	alarms.rtp.packetloss	Unacceptable packet loss from XXX.	More than 1% of packets from this IP address were lost.	Check network between this address and the recorder for packet loss.
Minor	alarms.rtp.nopackets	Unable to receive audio packets from XXX to YYY	No RTP packets received during a recording.	Check network route between this address and the recorder. Check the IP address shown is the expected NIC on the recorder.

Severity	Log File Entry	English Text on Alarm > View Alarms	Comments	Recommended Action
Major	alarms.slave.call slost	Unable to reallocate XXX recordings on failure of slave YYY	There was insufficient capacity to reallocate these recordings.	Check why the slave failed. Consider increasing the capacity of this slave pool to avoid losses in future.
Warning	alarms.slave.call sswitched	Reassigned XXX recordings on failure of slave YYY	These recordings have been restarted on a different slave recorder.	Check why the slave failed.
Major	alarms.slave.ove rflow	Call failed to record XXX due to overload on slave YYY	The slave recorder (or pool of slaves) had no spare capacity to record this call.	Increase the capacity of the slave(s) or rebalance recording across the recorders to reduce the peak load on this slave.
Info	alarms.slave.port savailable	XXX or more ports available on slave YYY	The available capacity on the slave recorder(s) specified exceeds the warning threshold.	Nothing
Warning	alarms.slave.port slow	Less than XXX ports available on slave YYY	The available capacity on the slave recorder(s) specified is below the warning threshold.	Increase the capacity of the slave(s) or rebalance recording across the recorders to reduce the peak load on this slave.
Minor	Alarms.softphon e.callstopped	Port XXX. Call dropped as it exceeded maximum permitted duration.	May be genuine very long call or a “zombie” recording.	Check log file at start of recording as well as at this point.
Info	alarms.softphon e.inservice	Port XXX restored.	A failed recording port has been restored.	Check the previous port failure message.

Severity	Log File Entry	English Text on Alarm > View Alarms	Comments	Recommended Action
Minor	alarms.softphone.invalidtarget	Port XXX - Invalid target for recording: YYY	The Quality Monitoring system has attempted to record a DN that has a non-numeric address.	Check the Quality Monitoring application setup.
Minor	alarms.softphone.processfailed	Error processing file XXX. Reason YYY.	Could not compress file or insert into database.	Check log file for further details. Neighboring event may show root cause.
Minor	alarms.softphone.timedout	Port XXX. Timed out when in state YYY.	The recording channel timed out e.g. did not complete recording start within 30s.	Check log file from the time at which the port entered this state until the time of the alarm.
Major	alarms.standby.goinginactive	Standby recorder taking over.	The standby recorder has determined that the Master recorder has failed or has requested that the Standby take over.	Check the alarms on the Master to determine the root cause of the problem.
Major	alarms.standby.notviable	Recorder fatal error.	The recorder has detected a major problem that means it cannot record.	Check the alarms preceding this one for the root cause of the problem.
Major	alarms.standby.primarynotok	Master recorder requests that Standby(s) take over.	The Nortel Recording Master has decided that it cannot record and requests that the standby recorder should take control.	Check the alarms preceding this one for the root cause of the problem. This may be that a disk partition is full or the recorder cannot communicate with the CTI link.

Severity	Log File Entry	English Text on Alarm > View Alarms	Comments	Recommended Action
Info	alarms.stnbulk.p ortsavailable	Bulk Recording now has XXX channels available.	The number of channels available for bulk recording has returned to or above the warning threshold.	
Warning	alarms.stnbulk.p ortslow	Bulk Recording has less than XXX channels available.	The number of channels available for bulk recording is below the warning threshold set.	Increase licensed capacity or relax the warning threshold.
Minor	alarms.unify.ioe xception	File I/O error updating call details of XXX. Reason: YYY.	A post-call tagging operation was attempted and failed.	The recording file may have been deleted (or not retained) since it was recorded. Manual command or minimum call length not being reached could cause this.
Minor	alarms.unify.par seerror	Parsing error updating call details of XXX. Reason: YYY.	The message received from Master or external controller is invalid.	Check the syntax of messages being sent to the recorder.
Major	alarms.url.badpo rt	Invalid IP port number for recording mode: XXX, Set to: YYY	The port number is not a valid integer.	Check you have specified the correct port number.
Major	alarms.url.gener al	Error on link to 'XXX': YYY		Depends on reason YYY
Info	alarms.url.linku p	Link established with XXX server on 'YYY		'Check previous error report.

Severity	Log File Entry	English Text on Alarm > View Alarms	Comments	Recommended Action
Major	alarms.url.nourl	Ports are allocated to XXX recording but no url is set to communicate with the server.	You are attempting to use a recording mode that requires connection to another server - such as the Nortel Quality Monitoring application.	Provide a valid url for connection to the required server.
Major	alarms.url.socket	Error connecting to 'XXX'. YYY		Depends on reason YYY.
Info	crc.card.up	Call Recording Card at XXX is connected.	The recorder has established a session with the specified Call Recording Card.	Check previous error condition.
Major	crc.card.conn	Call Recording Card at XXX disconnected. Reason: YYY	The recorder cannot establish a session with the specified Call Recording Card.	Depends on reason reported. Check Call Recording Card manual for specific cause codes. Check IP address and security code are correct.
Major	err.archive.baddisk	Bad or wrong type of archive disk inserted.	The disk in the local DVD drive must be a DVD+RW disk. Other formats are not supported.	Enter a blank DVD+RW disk or the latest, partially filled disk.
Major	err.archive.error	Unable to write to archive file YYY. Reason: XXX. Check Troubleshooting Guide.	The recorder could not write to the local DVD drive.	Check the media is good. Confirm the drive is working.
Major	err.archive.nodisk	No disk available for calls archive.	The recorder is ready to write files to disk but the drive is empty.	Insert a blank DVD+RW.

Severity	Log File Entry	English Text on Alarm > View Alarms	Comments	Recommended Action
Major	err.archive.wrongdisk	An old archive disk (XXX) is inserted, but archiver needs the current disk (YYY) or a blank disk.	The recorder is ready to write files to disk but the drive contains a previous disk.	Insert a blank DVD+RW or the most recent, partially filled disk.
Minor	err.eqb.1002	Port XXX: Invalid Parameter: YYY	Invalid message parameter received from Nortel Quality Monitoring application.	Check Quality Monitoring application log files.
Minor	err.eqb.1006	Port XXX: Invalid state. Currently YYY	Nortel Quality Monitoring application attempted to perform an operation on a recording port that was in an invalid state for this operation.	Check for earlier errors that may have caused the port to be in the incorrect state.
Minor	err.eqb.1007	Port XXX Out of Service	The Nortel Quality Monitoring application attempted to use a recording port that was not available.	Check for earlier errors that may have caused the port to go out of service. Check it recovered shortly afterwards.
Minor	err.eqb.1008	CTI Down	Could not complete operation requested by Nortel Quality Monitoring application because the CTI link was down.	Restore CTI link. Check for alarms indicating why this has failed.

Severity	Log File Entry	English Text on Alarm › View Alarms	Comments	Recommended Action
Minor	err.eqb.1009	Port XXX: Local file I/O error on 'YYY', error:{2}	Could not read or write the recording file being made locally on behalf of the Nortel Quality Monitoring application.	Depends on DOS file error code given.
Minor		Invalid E-mail address: XXX	The E-mail address shown is not a valid E-mail address.	Correct this address on the General Setup › Email Server page.
Minor	err.mail.send	Error sending E-mail XXX.	The system was unable to send an E-mail.	Check E-mail settings. Confirm that the E-mail account is correctly set up.
Major	err.mail.authentication	Authentication failed attempting to send E-mail.	Cannot use the SMTP account provided.	Check user account details. Try using account manually from Outlook or similar.
Major	err.mls.notconfigured	CTI Link not yet configured.	You have not yet provided the IP address of the Nortel Contact Center server.	Specify the address of the Nortel Contact Center server.
Warning	err.system.restart	System restarting.	The Nortel Contact Recording service has started.	If not a planned shutdown, check for reason why it failed.
Info	err.system.shutdown	System shut down.	The Nortel Contact Recording service was started.	If not a planned shutdown, check for reason why it failed.
Info	info.archive.errorcleared	Wrote to archive disk correctly.	The previous archiving error has been cleared and a file has been written to disk successfully.	Check the previously reported error.

Severity	Log File Entry	English Text on Alarm > View Alarms	Comments	Recommended Action
Info	info.archive.righ tdisk	Correct archive disk now inserted.	The correctly numbered (or new) disk has been inserted.	Nothing
Info	info.archive.ewa reok	Viewer database connection OK.	Connection to the Viewer database has been restored.	Check for earlier alarms indicating that connection had been lost.
Info	info.mail.sent	Mail sent successfully.	E-mail alarms are now being sent successfully after one or more failures to send them.	Check reason for previous failure.
Info	info.standby.goi ngstandby	Standby recorder returning to idle.	The standby recorder is returning to standby mode because the Master has asked it to or it has detected that the Master is active again.	Check why the standby was active in the first place. This will interrupt recordings. You should bring the master back online out of hours.
Info	info.standby.pri maryok	Master recorder requests Standby(s) go idle.	The Nortel Contact Recording Master is resuming control and requests that the standby recorder give up control.	The problem that led to the standby recorder taking over may have been resolved. For example, disk space may have been freed on the Master.
Info	info.standby.via ble	Recorder fatal error resolved. OK to record.	The problem that was blocking the recorder from functioning has been resolved.	Check earlier alarms for details of the specific problem.
Major	err.database.pur ge	Error purging database. Reason: XXX.	Failed to purge old audit trail records, call details or alarms	Check log file for further details.

Severity	Log File Entry	English Text on Alarm > View Alarms	Comments	Recommended Action
Major	link.master.linkerr	Error on link to Slave recorder at XXX: YYY	The Master recorder has lost contact with the slave recorder specified.	Depends on reason YYY.
Major	link.primary.linkerr	Error on link to Standby recorder at XXX: YYY	The Master recorder has lost contact with the standby recorder specified.	Depends on reason YYY.
Major	standby.reason.connecttimeout	Initial connection timed out with XXX	Standby recorder could not make contact with the Master	Check Master recorder. Check network between Master and Standby.
Major	standby.reason.reconnecttimeout	Connection dropped and reconnection timed out with XXX	Standby could not re-establish contact with Master when link dropped.	Check Master recorder. Check network between Master and Standby.
Major	standby.reason.inactivity	Heartbeat failure via <nnn.nnn.nnn.nnn>	Standby recorder did not hear heartbeat from Master.	Check Master recorder. Check network between Master and Standby.

Appendix D

Recorder Control Protocol

In this appendix

Introduction	201
Java API Toolkit	202
TCP/IP Protocol Overview	203
TCP/IP Message Sequences	206

Introduction

This appendix describes the interface used to control the recording behavior of a Nortel Contact Recorder. You may integrate directly to the TCP/IP socket using the protocol described or by using the Java package provided for this purpose. An example application that uses the Java interface is also provided for reference.

When to Use External Control

The Nortel Contact Recording system includes sophisticated CTI interfaces and recording control but there are still occasions when additional flexibility or further data tagging is required. You will require an “external controller” in the following cases:

Complex Recording Rules

If your “record/do not record” requirements are more complex than the administration interface supports. For example, if you wish to start and stop recording at specific points within a call.

Additional Tagging

To “tag” recordings with details not available directly from the Nortel CTI feed connected to the recorder.

Hybrid Systems

If your Nortel system is controlled by another application (e.g. Genesys) then it may be appropriate to control recording as a result of the events occurring on this other CTI feed.

This Appendix

The remaining sections of this appendix provide:

- an overview of the underlying TCP/IP control protocol
- a reference guide for the message sequences exchanged between recorder and controller
- a brief overview of the Java interface classes. For detailed information refer to the JavaDocs for this package.

Java API Toolkit

Rather than write directly to the socket level interface described below, you may use the Java language API provided. This contains the following components:

Packages

com.swhh.cti.ncr.lang	Provides a high-level API for controlling the Nortel Contact Recording Master.
com.swhh.cti.ncr.msg	Provides Nortel Contact Recording message classes and interfaces as well as classes that implement the java.io.Reader interface for reading Nortel Contact Recording messages from streams.
com.swhh.cti.ncr.service	Provides a low-level API for communication with the Nortel Contact Recorder.
com.swhh.cti.ncr.tools	Contains two debugging tools as well as examples of applications that use the low-level API.
com.swhh.cti.ncr.ui	Contains a test harness for the Nortel Contact Recorder with a graphical user interface that also serves as an example application built on top of the high-level API classes.

JavaDoc for these classes is available on request. To view the JavaDoc without a Java IDE, unzip the contents and double-click `index.html` for a top-down view. For a comprehensive reference index, double-click `indexall.html`.

TCP/IP Protocol Overview

Connection Method

An external controller can drive the Nortel Contact Recording Master via a TCP/IP socket using the protocol described below.

You configure the Master recorder with the IP address and socket number of the controller(s) to which it should connect. Connection defaults to port 1415 but you can specify an alternate port. The recorder creates a socket and attempts to connect to the specified address. If it fails to connect, it will try again every 60s.

You can use multiple, independent controllers connected to a single recorder.

The controlling application should open and bind a server socket and accept incoming connection requests.

General Protocol Specification

Messages take the form:

```
<protocol version number> <command> (<command specific data>) '\x1b'
```

When sending messages, follow these rules:

1. Transmit messages in ASCII 8-bit encoding. Wrap any 16-bit XML content in CDATA blocks.
2. All messages and responses are terminated with an escape character (27 / 0x1b).
3. Separate fields with space characters.
4. Enclose field contents in double quotation marks where the field needs to contain a space - as, for example, with filenames. Always enclose filenames in double-quotes.
5. Delimit sub-fields with colon characters ":".
6. Apart from HELLO messages (see below) and responses, all messages must be responded to in the form:

```
<protocol version number> <error code> <channel identifier> <error  
qualifier> <additional info> '\x1b'
```

Where

<error qualifier> is typically "DESC:xxxxxxx:"

and

<additional info> may be 0 or more instances of "PARAM:pppppp:"

The response to a successful command is therefore:

```
1 0 DN:nnn: TN:mmm: \x1b
```

and a typical error response is

```
1 -1 DN:1234: TN:1000: DESC:"Invalid Parameter": PARAM:DN \x1b
```

7. Ignore unexpected or malformed responses.
8. Send commands in uppercase, but test for them case insensitively.

Channel Identification

In most messages below, the recorder's channels are identified by Directory Number ("DN:nnnnn:") and by Terminal Number ("TN:mmmm").

Where "nnnnn" can be 1 to 7 digits long and may include leading zeroes. The Directory Number passed is that of the DN (or Position ID) being monitored by the recorder. The TN (1-5 digits) is that of the specific terminal on which this DN is present. Note that the TN value must be in decimal even though the CTI Monitors page shows these in hex format.

Note: This scheme allows recording of MARP/MADN multiple appearance DN's on CS 1000 IP media streaming phonesets in knowledge worker environments. See ["Limitations of this release" on page 36](#).

Note: In a CS2x00/DMS system, there can only be one call active on a set

Note: of MADN appearances so any command received will be assumed to apply to the currently active station.

XML Tagging

All tagging information is passed straight through the recorder into the XML file associated with the recording. The recorder only looks for an escape character to delimit each command. The intention is that the controlling application will pass through valid XML tags which the recorder will insert into the body of the call's XML file. These may include valid expansions of control and other characters (e.g. %20 etc). The entire XML string will be inserted between opening and closing "taglist" tags. E.g. the command

```
1 TAG DN:1234: TN:1001: INUM:800369000000009: <spare1>some data</spare1><spare4>John Doe</spare4>\x1b
```

will result in call reference 800369000000009, which is currently being recorded on DN 1234 at TN 1001 being tagged with the additional fields:

```
<taglist>
  <spare1>some data</spare1>
  <spare4>John Doe</spare4>
</taglist>
```

The recorder supports seven user-defined fields, labelled "spare1" to "spare7". These can be relabelled for end user viewing as part of the query design using Contact Viewer. You may use other fields but the recorder only uploads the seven "spare" fields automatically.

Fallback Mode

When a Nortel Contact Recorder starts, it automatically runs in locally controlled mode - where CTI events it detects cause it to start/stop recording. This is also known as “fallback” mode.

If an external controller wishes to start/stop recordings itself rather than respond to decisions made inside the recorder, it can instruct the recorder to turn this Fallback mode OFF for a specific channel (or all channels).

If the heartbeat to that controller is subsequently lost, the channel(s) will revert to fallback mode and recording will continue as if the controller had never been present.

TCP/IP Message Sequences

Note: In all of the following examples, the TN parameter is only sent for CS1000 systems. It is absent in CS2x00/DMS systems. In CS2x00/DMS systems, MADN appearances each send identical ONLINE messages. However, because only one can be active at a time, these should be treated as a single recording channel and any commands sent will refer to the currently active line appearance.

The following table shows all supported message sequences:

Controlling Application Sends	Dirn	Nortel Contact Recording Master Sends	Comments
On recorder first establishing connection with controller's socket (default port = 1415)			
	<<<	2 HELLO NortelCapture nnnn	Where nnnn is the recorder's unique reference number (1 to 9999) as shown on the Licensing page.
2 HELLO XXXX nnnn	>>>		Where XXXX is the application's name and nnnn a unique identifier for this instance of the application. The recorder does not parse beyond "HELLO". Recorder writes the full message to the log file but does not act on the name given. The recorder will also accept the older "1 HELLO xxxx" message.
	<<<	1 ONLINE DN:nnnnn: TN:mmmm:	For each recordable occurrence of a DN or Position ID configured and available, the recorder sends this message. This allows the controlling app. to build a table of available recording channels on the fly. The app may wish to respond immediately with a START or STOP message to enable/disable recording of that channel. A burst of these messages will be sent as the external controller connects to the recorder. Thereafter, this message is sent when additional DNs are configured. When a DN is removed from the recorder, an ERROR message is sent for it.

Heartbeat – exchanged every few seconds to allow rapid failure detection

Controlling Application Sends	Dirn	Nortel Contact Recording Master Sends	Comments
	<<<	1 PING	Recorder initiates.
1 PINGACK	>>>		Confirmed. If >5 heartbeats are missed (assuming local area connection between recorder and controller) report error.
To request notification of call details on a channel			
1 REQUEST ACTIVITY ON DN:nnnn: TN:mmmm:	>>>		The controller can ask that it is advised of full call details in addition to basic started/stopped messages. To avoid looping, the recorder does not advise of tagging submitted by external controllers, only the tagging information that the recorder itself applies at the start of a recording.
	<<<	1 0 DN:nnnn: TN:mmmm:	Confirmed
Start Recording			
2 START DN:nnnn: TN:mmmm: <xml data>	>>>		Start recording on DN/TN specified and tag with optional data supplied.
	<<<	1 0 DN:nnnn: TN:mmmm:	Confirmed
Stop Recording			
2 STOP DN:nnnn: TN:mmmm: <xml data>	>>>		Stop recording on DN/TN specified and tag with optional data supplied.
	<<<	1 0 DN:nnnn: TN:mmmm:	Confirmed
On recording starting			
	<<<	1 STARTED DN:nnnn: TN:mmmm: INUM:nnnnnnnnnnnnnnnn :	The controller can note the INum to ensure subsequent tag commands go to the right segment even if that call has finished. It can also parse out the DN/TN if it wants to check for orphaned records hanging around from this station which are obviously now in error.

Controlling Application Sends	Dirn	Nortel Contact Recording Master Sends	Comments
On recording stopping			
	<<<	1 STOPPED DN:nnnn: TN:mmmm: INUM:nnnnnnnnnnnnnnnn :	Sent by the recorder when recording stops – due to hold or hangup/transfer.
On recording getting new or changed info (and the controller has requested ACTIVITY ON for this port)			
	<<<	1 UPDATE DN:nnnn: TN:mmmm: INUM:nnnnnnnnnnnnnnnn : <xml data>	Info available for call specified on station specified. Controller may need to interpret some of the XML to determine recording action. Will send all call info on each update so controller can cache single string.
On controller wanting to tag call			
1 TAG DN:nnnn: >>> TN:mmmm: INUM:nnnnnnnn nnnnnnnn: <xml data>			This allows tagging to be sent for the current and previous calls on a channel. The recorder will use nnnnnnnnnnnnnnnnn to determine whether the tagging is for the current call or an earlier one. In the latter case, it will open the XML file and append the details given. Additional tagging should currently be confined to the 7 pre-defined fields spare1 to spare7. i.e. <xml data> should be of the form <spare1>some data</spare1>.
	<<<	1 0 DN:nnnn: TN:mmmm:	Confirmed
Call Break – controller initiated			
1 BREAK DN:nnnn: TN:mmmm: <xml data>			Recorder breaks the call seamlessly. The optional tag data is applied to the stopped call. Send further TAG command to tag new call.
	<<<	1 0 DN:nnnn: TN:mmmm:	Confirmed
	<<<	1 STOPPED DN:nnnn: TN:mmmm: INUM:nnnnnnnnnnnnnnnn :	(Only if there was actually a call active)

Controlling Application Sends	Dirn	Nortel Contact Recording Master Sends	Comments
	<<<	1 STARTED DN:nnnn: TN:mmmm: INUM:nnnnnnnnnnnnnnnn :	Only if a call is in progress and hence can be recorded.Same DN/TN but different INum obviously
Call Break at recorder due to max segment duration exceeded			
	<<<	1 STOPPED DN:nnnn: TN:mmmm: INUM:nnnnnnnnnnnnnnnn :	
	<<<	1 STARTED DN:nnnn: TN:mmmm: INUM:nnnnnnnnnnnnnnnn :	Same DN/TN but different INum
	<<<	1 UPDATE DN:nnnn: TN:mmmm: INUM:nnnnnnnnnnnnnnnn : <xml data>	Only sent if ACTIVITY ON previously requested. Controller can identify this as a broken call from the “nostart” field being “true”.Externally tagged data will have been rolled over from the previous call and included in this call’s data already.
On shutdown			
	1 BYE <reason>	>>>	<reason> is logged but not acted upon. The recorder does not respond and closes the socket.
On a recording channel reporting an error			
	<<<	1 ERROR DN:nnnn: TN:mmmm:	Channel is unusable e.g. the DN is not present on this TN, cannot be monitored, has been removed from the list of recorded stations etc.Controller should mark this port faulty and not attempt to use. Hopefully, an ONLINE message will follow shortly as the recorder recovers the port.
On a recording channel being restored			
	<<<	1 ONLINE DN:nnnn: TN:mmmm:	Channel is available

Controlling Application Sends	Dirn	Nortel Contact Recording Master Sends	Comments
To take control of a channel (i.e. recorder will no longer start recordings itself)			
2 FALLBACK OFF DN:nnnn: TN:mmmmm	>>>		Recorder will stop recording as result of locally detected CTI events. Will only start when controller tells it to. Stop will still occur on timeout of stream but controller would normally instruct it to stop before timeout expires (though note that far-end placing call on hold can generate an unsolicited STOPPED. If DN and TN are not specified, the command applies to all channels and the response does not include the DN/TN parameters.
		<<< 1 0 DN:nnnn: TN:mmmm:	Confirmed
To relinquish control of a channel (i.e. recorder will now start recordings itself)			
2 FALLBACK ON DN:nnnn: TN:mmmmm	>>>		Recorder will resume control of recording as result of locally detected CTI events. If DN and TN are not specified, the command applies to all channels and the response does not include the DN/TN parameters.
		<<< 1 0 DN:nnnn: TN:mmmm:	Confirmed

Appendix E

Auto-dialer Integrations (only available with 6.5.1 update)

In this appendix

Introduction	213
Configuration	215
Avaya PCS/PDS Dialer	223

Introduction

When agents log in to dialers using “nailed up” sessions, the whole session of customer calls appears to the recorder as a single “call” and hence recordings are concatenated. These can be broken up and tagged with the outbound call details using CTI integration to the dialer.

One or more dialers can be supported. These may be of the same or mixed types.

Currently supported dialers are:

- Davox/Concerto
- SER
- Avaya PCS/PDS

Functionality

Dialer integrations allow calls made over “nailed up” sessions (usually on the secondary DN of a position) to be split into individual customer calls. Without the dialer integration, such calls are recorded as a single recording for the duration of the session, tagged only with the identification of the dialer port – not the numbers of the customers actually called.

When an agent logs in to a dialer, the nailed up call is recognised as such and recording stops. This recording may include an initial greeting or login dialogue. If it is very short it may be automatically deleted but typically results in a 0 or 1s duration call. If the agent subsequently drops this call by releasing at the phone set or otherwise, the dialer will re-establish the nailup with a new call. This will be recorded unless the dialer sends an agent not ready event as it does this. In either case, when a customer is next connected to the nail-up, a new recording will begin.

When the agent is presented with a call, the dialer tells the recorder and it starts recording. Information provided by the dialer at this time is used to tag the call. This typically includes campaign information and identification of the party being called.

At the end of a call, the dialler tells the recorder and it stops recording.

Optionally:

- Agent logon/logoff from the dialer can be used to determine the agent number and name (but the default is to use the CC6 agent login information).
- Events for nailups on the positionID can be passed through (but the default is to block events on the position id as this can impact normal operation i.e. where the positionID is not “nailed” up).

Detailed functionality varies from dialer to dialer and from installation to installation. See below for more details.

How it Works

The recorder starts an additional thread to monitor the CTI activity from each dialer. This picks up Agent Logon/logoff and start/stop events as the agent takes each call. The details vary from dialer to dialer. Each dialer is implemented as a specific Java “class” and can be configured via the normal cs.properties file.

Status Monitoring

The status of the CTI link to each dialer is shown on the Status > Overview page alongside all the other interfaces.

Alarms are generated whenever a link fails or is restored.

Nailup calls which do not have a customer connected to them will show as if the call were on hold.

Errors, warnings, informational and debug messages are written to the cs.log file along with all other messages generated by the recorder.

Configuration

Dialer configuration is done via the cs.properties file.

Licensing

To interface to e any dialer other than the Nortel/SER dialer, you must purchase and install a license key containing this option.

Dialer List

First, specify how many dialers you have and what they are called by adding the following line to the properties file cs.properties:

```
cs.dialerlist=<dialer1name>,<dialer2name>,...
```

Choose the dialer names to reflect not just the make of dialer but also its location or identity if you have more than one dialer of a given type.

For example:

```
A single, Davox dialer:  cs.dialerlist=Davox
Two SER Dialers and one Davox dialer:
cs.dialerlist=SER_London,SER_NewYork,Davox_Dublin
```

Generic Dialer Configuration

For every dialer name given in the cs.dialerlist, you should include the following lines in your properties file. Each begins with the name of the dialer to which it refers.

Mandatory Fields

You MUST include this for each dialer so the application knows which Java class to use:

```
<dialer1name>.class=<java classname for the type of dialer>
```

Optional Fields

The following fields need only be added if you wish to override the default settings.

By default, only calls on the secondary DN are passed to the recorder. If you wish to pass on any messages relating to calls taken on the position Id, add

```
<dialer1name>.blockposmessages=false
```

By default, agent logon/logoff messages are not passed on to the recorder (i.e. it is assumed that the agent logon to the position id is sufficient to tag the call). To change this, add

```
<dialer1name>.blockagentids=false
```

This will allow the dialer's view of agent ids and names to be included in call tagging.

Tagging of Calls

Recordings split by dialer instructions are tagged as follows:

Recording Data Field	Type	Max Length	Recommended Use	Search and Replay View	Available in QM?
DN	Numeric	50	The DN used to take the call	Appears in the Parties field	Yes
AgentID	Numeric	50	Dialer login id (or Nortel login id if dialer agent ids blocked)	These two fields are shown combined in the "Agent" field e.g. "1234 (Mary Smith)"	Yes
AgentName	Alphanumeric	50	Dialer login name (or Nortel lead CDN if dialer agent ids blocked)		Yes
Party Number	Numeric	50	The number dialled	These two fields are shown combined within the Parties field. E.g. "02081234567 (Mr John Smith 54670045)"	Yes
Party Name	Alphanumeric	50	The customer identifier. Some dialer interfaces allow you to combine multiple fields into this one. Try to include the customer name and your unique identifier for that customer e.g. account number.		No
Service Number	Numeric	16	Skill number or "treatment code"	These two fields are shown combined within the Service field e.g. "200 (BadDebts)"	Yes
Service Name	Alphanumeric	50	Campaign or database used		No

Note: Where a dialer integration allows multiple fields to be concatenated, don't forget to count the space character between these when assessing total field length. Any fields longer than permitted will be truncated.

Configuring NQM

If NCR is used with NQM, the dialer integration makes the same agent logon/off, call boundaries and tagging visible to NQM.

It can be helpful to turn up the logging of the IFConnector using the registry key below – though this level of logging must NOT be left set on production systems.

```
HKEY_LOCAL_MACHINE > SOFTWARE > Witness > Tracing > IFConnectorAdapter >
TraceLevel = 12 (dec)
```

Some of the attributes passed to QM are standard ones but you will need to configure it for the additional attributes as follows:

Under System Administration > CTI Adapters > Custom Properties set the following:

Custom Property Name	Customer Property Name
DNISNAME	Contact.DNISNAME
CounterPartyName	Contact.CounterPartyName

Note: You must specify “Contact.” before the name of the attribute passed into the IFConnector.

Now add the following Custom Attributes under System Administration > Additional > Custom Attributes.

System Name:	DNISNAME	CounterPartyName
Visible	Yes	Yes
Business Rule Editable	Yes	Yes
Display Name	DNISNAME (or change to more closely match the data field your dialer provides here)	CounterPartyName
ToolTip	DNISNAME (or change to more closely match the data field your dialer provides here)	CounterPartyName
Renderer	String	String

ANI and DNIS are already built into the Custom Properties at the CTI Adapter level, so there is no need to add these.

To make the fields visible in the Contacts View you need to right click in the grid and select Customize Columns and move the following entries into the Selected Columns:

- CTI ANI
- CTI DNIS
- CTI Number Dialed

- CTI Call Direction
- DNISNAME
- CounterPartyName

Finally, restart the QM System to make sure the changes take effect.

SER Dialer

Set the .class property to “com.swhh.cti.sercon.SERDialer”. For example:

```
SER_Chicago.class=com.swhh.cti.sercon.SERDialer
```

HostName

Specify the IP host name of the dialer to which the recorder should connect:

```
<dialer1name>.hostname=<hostname>
```

For example:

```
SER_Chicago.hostname=10.100.205.23
```

Use a numeric IP address if the host name cannot be resolved or is not known.

Port

Specify the port number to which the recorder should connect:

```
<dialer1name>.port=<portnumber>
```

The default is set to port 40000 but you may need to change this to suit your dialer. For example,

```
SER_Chicago.port=9000
```

SwitchName

An SER dialer can be connected to more than one switch. You must specify the name that has been set in SER for the Nortel switch that this recorder is recording. In most cases, the default of “switch1” will be correct.

```
<dialer1name>.switchname=<switchname>
```

For example:

```
SER_Chicago.switchname=switch2
```

FieldMappings

A standardised set of mappings is provided from the SER fields to the recording tagging fields as described on the following page:

SER Field Name	Notes	Mapping to Recording XML and Database Field (NB. Fields shown in search pane are derivatives of these not 1:1 mappings)	User will see information in this search field and column in the Default Search Layout	Example Value seen on Galway V&V system
N/A	Only outbound calls go through SER	Direction=Outbound on all calls including consult as no way to determine if target is internal v external?		N/A
Campaign	Dial plan and strategy	Service number (where DNIS is stored on inbound calls and can be alphanumeric). NB. Truncated to first 16 chars.	Service	nd400k
Group	The skill set from which agents are selected to service the campaign	Agent name of party 1 on call – where lead ACDDN shows at present i.e. in parentheses after agent ID as part of compound agent field	Agent	PR_TestSk1
UserName	SHOULD match the CS1K logged on Agent ID	AgentID of Party 1	Agent	3508
Extid	The extension we asked to observe – actually the secondary DN on the Position	Party Number of Party 1	Parties	8900
Telnum	Dialled number	Party Number of Party 2	Parties	3006

SER Field Name	Notes	Mapping to Recording XML and Database Field (NB. Fields shown in search pane are derivatives of these not 1:1 mappings)	User will see information in this search field and column in the Default Search Layout	Example Value seen on Galway V&V system
RetKey	Unique reference for this record in the dialling list (Portfolio). Often is customer identifier e.g. a/c number	Party Name of Party 2 hence customer will show with this in parentheses after their number e.g. 07767791590 (00001234)	Parties	0000001255
Portfolio	Set of numbers i.e customer list and their phone numbers. Mapping of fields, import file, which wrapup codes etc.	Service Name – will show in same field as DNIS but in parentheses after the number e.g. campaign “Bad Debts” run against portfolio “Gold Customers” will show as “Bad Debts (Gold Customers)” in service field	Service	ND400k
RE_segnum	A numeric identifier that uniquely identifies the contact. Reused upon system restart – i.e. starts at 1 again.	Overrides the Nortel CallID. Has an offset (default 1000000) added so as not to overlap with Nortel callids. Property file callid.offset=nnnn to override this should it clash with the Nortel Call IDs in use on that switch	Call ID	16

Davox Dialer

Set the .class property to “com.swhh.cti.davcon.DavoxDialer”. For example,

```
Davox_Dublin.class=com.swhh.cti.davcon.DavoxDialer
```

HostName

Specify the IP host name of the dialer to which the recorder should connect:

```
<dialer1name>.hostname=<hostname>
```

For example:

```
Davox_Dublin.hostname=10.100.205.23
```

Use a numeric IP address if the host name cannot be resolved or is not known.

Port

Specify the port number to which the recorder should connect:

```
<dialer1name>.port=<portnumber>
```

The specification uses an example of 4252 so try this is in doubt! For example,

```
Davox_Dublin.port=4252
```

FieldMappings

The standard Davox integration for Verint Impact 360 recorders can be used. This provides user defined fields in the CTI output as DATA1 through DATA16. You can choose how to map these into the partynumber, partynumber, servicenumber and service name fields as described below.

These fields are passed on from the various campaign files – and hence there may be more than one mapping required if campaigns’ fields are not uniformly labelled. You can specify multiple strings for cases where only one of each is present in any given campaign or where you want to store multiple fields in one e.g. title, firstname and surname. Individual fields will be separated by a space character. In each case below, start with n=1 and do not skip any.

```
<dialer1name>.partynumber.<n>=<fieldname>
```

(Normally used to hold the phone number dialled. Maximum length = 50 characters).

```
<dialer1name>.partynumber.<n>=<fieldname>
```

(Normally used to hold the name or other identifier of the customer dialled e.g. account number. Maximum length = 50 characters).

```
<dialer1name>.servicenumber.<n>=<fieldname>
```

(This field is stored where DNIS is stored on inbound calls. Normally used to store the “campaign” identifier. Maximum length=16 characters.)

```
<dialer1name>.servicename.<n>=<fieldname>
```

(This field appears in parentheses after the servicenumber and is normally used to store the name of the database list being used on the campaign. Maximum length = 30 characters.)

For example:

```
Davox.partynumber.1=DATA1  
Davox.partyname.1=DATA2  
Davox.partyname.2=DATA3  
Davox.partyname.3=DATA4  
Davox.partyname.4=DATA5  
Davox.servicenumber.1=DATA6  
Davox.servicename.1=DATA7
```

You can check that all fields have been specified correctly by looking for the corresponding INFO level messages in the log file after startup e.g.:

```
2008-10-30 17:04:29,896 [Dialer Manager thread] INFO  
com.swhh.cti.davcon.DavoxDialer - starting davox dialer: Davox  
2008-10-30 17:04:29,896 [Dialer Manager thread] INFO  
com.swhh.cti.davcon.DavoxDialer - Found keyword [DATA1] for partynumber  
Etc.
```

Agent IDs

Note that the Agent IDs sent from the Davox dialer are normally alphanumeric names rather than numbers. These can be entered into QM as if they were additional CS1000 agent IDs.

Avaya PCS/PDS Dialer

Set the .class property to “com.swhh.cti.pcscon.PCSDialer”. For example,

```
PCS_Boston.class=com.swhh.cti.pcscon.PCSDialer
```

Versions Supported

The recorder interfaces to “Hard” dialers only (as opposed to “Soft” dialers) running the following versions of software, each of which has a corresponding “personality file” as shown below:

Dialer Type and Version	Personality File	Notes
PDS V12	pds12_idl.jar	
PCS V3.0	pcs30_idl.jar	
PCS V4.0	pcs40_id.jar	Secure connection can be enabled

Limitations

When using multiple PCS or PDS dialers, they must all be of the same major version as only one personality file can be loaded at a time.

Configuration

- 1 All three personality files can be found in the “etc” folder beneath the installation path. Copy the appropriate one into the /tomcat5525/shared/lib folder beneath the install path.
- 2 Ensure you have a license key installed that includes the optional dialer license.
- 3 Edit the properties\cs.properties file as described below
- 4 Restart the Nortel Contact Recorder service to have your configuration take effect.

Address

Specify the IP host name and port number of the dialer to which the recorder should connect and, optionally (mandatory if using multiple PCS dialers) the IP address and port to be used for the return connection :

```
<dialer1name>.hostname=<hostname>
<dialer1name>.port=<portnumber>
<dialer1name>.myhostname=<hostname>
<dialer1name>.myport=<portnumber>
```

For example:

```
PDS_Boston.hostname=10.100.205.23
PDS_Boston.port=4711
```

Use a numeric IP address if the host name cannot be resolved or is not known.

Credentials

Set the username and password that the recorder should use when registering as a client:

```
<dialer1name>.username=<username>  
<dialer1name>.password=<password>
```

For example:

```
PDS_Boston.username=NCR1  
PDS_Boston.password=secret
```

Encryption

When using PDS 4.0 you can force the recorder to use a secure connection to the dialer by setting:

```
<dialer1name>.secure=true
```

For example

```
PDS_Boston.secure=true
```

Name Service IOR (Optional)

This parameter is optional but if not provided, the recorder attempts to look up the Name Service using corbaloc (and must be able to resolve the IP address of the dialer by name – make sure it is in DNS).

```
<dialer1name>.NSIOR=mynsior
```

For example

```
PDS_Boston.NSIOR=xyz
```

FieldMappings

The dialer's "job name" is stored as the "Service" number (normally used for DNIS on inbound calls hence normally unused on outbound calls)

Glossary

A

ACD

Automatic Call Distribution. This is a feature offered by the Meridian 1 that queues and distributes incoming calls to waiting agents. Calls are queued until an agent is available. If multiple agents are available, calls are distributed on an equitable basis. ACD has many additional features, including recorded announcements (RAN), music while queued, night treatment, overflows, statistics/reports, and networking with ISDN.

ACD DN

The DN associated with an ACD group. Calls made to an automatic call distribution directory number are distributed to agents belonging to the group, based on the ACD routing table on the switch.

AGENT Logon ID

An unique identification number assigned to a particular agent. The agent uses this number when logging on to his/her phone. The agent ID is not associated with any particular phoneset

ANI

Automatic Number Identification (Service). The provision of calling party information (typically, telephone number or billing/account number) to the called party.

C

Call Recording Card

A circuit board that can be used within the Meridian switch to record calls being made through the switch and to allow other phonesets to monitor these calls.

CDN

Controlled DN. A CDN is similar to an ACD queue with no agents, a “holding place” for calls. Calls are queued in a CDN, and while in the queue, calls can receive treatment commands from a controlling application (for example, host application giving treatments such as music, ringback, or silence, or routing the call). CDNs can operate in controlled or default (uncontrolled) mode. An active application controls calls in a CDN when the CDN is in controlled mode. In default mode, calls entering a CDN are immediately given the default treatment (for example, routed to an ACD DN and receive RAN, music, and so on), as specified in the default configuration in Overlay 23).

Controlling Recorder

In any Nortel Contact Recording system, there will be one, and only one active Controlling Recorder. This is the server that is connected to the MLS link and is actively controlling recording channels on itself and/or other recorders.

CRD

Contact Recording Desktop

CTI

Computer Telephony Integration – typically an interface through which a computer system can be advised of events occurring within a telephony system and/or control the telephony system. MLS is an example of such a link.

CUSTOMER

The Meridian 1 supports multitenant operations. The PBX can be partitioned into multiple, independent systems known as customers. Within each customer, DNs are unique and routes are private. Meridian Link is a system feature: that is, it covers all customers in the Meridian 1 PBX. However, when an application registers over Meridian Link (Application Registration message), it selects the customer it wants to work with.

D**DID**

Direct Inward Dialing. An attribute of a trunk. The CO passes the extension number of the called party over a DID trunk to the PBX when offering a call to the PBX. The PBX is then able to automatically route the call to that extension without requiring operator/attendant assistance. In this way, a single trunk can terminate calls for many different extensions (but not simultaneously).

DN

Directory number. The number that identifies a phoneset on a PBX or in the public network. It is the number that a caller dials to establish a connection to the addressed party. The DN can be a local PBX extension (local DN), a public network telephone number, or an ACD-DN—the pilot or group number for an ACD queue.

Duplicate Media Streaming

A means of recording telephone calls by having the phoneset duplicate the packet streams it is receiving and transmitting – sending the copies to a specified IP address (the recorder).

DVD+RW

Digital Versatile Disk + Read/Write. One of several competing optical storage standards, supported by a wide range of manufacturers.

E**E1**

E-carrier level 1. A European telecommunications standard for 2 Mbps trunks.

H**HFS**

Hierarchical File Storage system. Typically a combination of hard disk and tape drives plus controlling software that automatically migrates little used files to cheaper storage media.

I**IDN**

Individual DN. ACD agents using BCS sets can have additional DNs (in addition to their ACD key) configured on their phonesets. Key 0 is used to receive incoming ACD calls; other keys can support other DNs. IDNs are treated just like any other DN. 500/2500 set ACD agents can also have a (single) IDN configured.

Internet Protocol

The Internet Protocol (IP) is a data-oriented protocol used for communicating data across a packet internetwork.

IVR

Interactive Voice Response. A system/facility that plays voice menus to callers, and acts upon user input (typically, DTMF digits from a touch tone phone). It is sometimes called VRU (Voice Response Unit).

M**MADN**

Multi-Appearance Directory Number. Meridian Link only supports monitoring one appearance of a Multi-Appearance DN.

Meridian Link (ML)

Meridian 1's host interface. Meridian Link supports X.25 and LAPB communication protocols for host connectivity.

MLM

Meridian Link Module. The MLM supports the Meridian Link Protocol to host processors. It is packaged within the Application Equipment Module (AEM), which itself is packaged in the Meridian 1 Universal Equipment Module (UEM).

N**NACD**

Network ACD. Meridian 1's networked ACD offering. With NACD, it is possible to have calls queued in multiple queues at different locations. The call is presented to the first agent that becomes available, at any of the locations where the call is queued. This can greatly improve operations, particularly where time zone differences can be exploited. ISDN is used as the base network transport.

NAS

Network Attached Storage. A term used for RAID, tape and other mass storage systems which have an integral network connection such as Ethernet or fibre-channel.

NIC

Network Interface Card. An expansion board that you insert into a computer so the computer can connect to a network. Most NICs are designed for a particular type of network, protocol, and media, although some can serve multiple networks.

O

OA&M

Operations, Administration and Maintenance. The tools, typically software, that enable a crafts person to configure, administer, and maintain a system.

P

POSITION ID

A unique identifier for the phoneset, used by the switch to route calls to the phoneset

Primary Controller

A Nortel Contact Recorder that is being shadowed by one or more Standby Controllers. The Primary will default to “Active” on startup but will ask a Standby to take over its role if it determines that it cannot record e.g. a disk fills.

Q

QoS

Quality of Service

R

RAID

Redundant Array of Inexpensive Disks. RAID controllers use two or more hard disk drives together for fault tolerance and enhanced performance. RAID disk drives are used frequently on servers.

RTP

The Real Time Protocol (RTP) defines a standardized packet format for delivering audio and video over the internet.

S

SAN

Storage Attached Network. A high-speed network that is typically part of an overall network of computing resources for an enterprise, in which the software knows the characteristics of storage devices and the quantity and value of the data stored in those devices.

Slave Recorder

A Nortel Contact IP Recorder, Passive Tap IP recorder or Passive Tap TDM recorder being controlled by the active Controlling Recorder. i.e. recording what it is told to record.

Standby Controller

A Nortel Contact Recorder that shadows a Primary Controller and takes over its role (“goes active”) should the primary fail or appear to fail (e.g. the standby loses contact with it).

T

T1

T1 is a T-carrier signalling system devised by Bell Labs. It is a widely used standard in telecommunications in North America and Japan to transmit voice and data between devices.

Tagging

Adding details to the database of call recordings so that recordings can later be retrieved by searching through the available data fields.

TDM

Time Division Multiplexing. The traditional means of transmitting large numbers of voice calls over circuit switched networks – as distinct from VoIP.

TN

Terminal Number. The physical address of a device (for example, a phoneset, a trunk, an attendant) on the Meridian 1 PBX. The TN is composed of the loop, shelf, card, and unit IDs.

TRUNK

A communications link between a PBX and the public central office (CO), or between PBXs, or between COs. There are various trunk types that provide services such as Direct Inward Dialing (DID trunks), ISDN, and Central Office connectivity (CO trunks). Digital trunks use A/B signaling, or D channel signaling in the case of ISDN. Trunks are configured on the Meridian 1 in Overlay 14.

V**VAS/VSID**

Value added Server/Value Added Server Identifier. Identifies the ELAN link on which the CCMS is connected.

VoIP

Voice over Internet Protocol. A means of transmitting telephone calls over the packet-switched IP network – as distinct from TDM.

VRU

Voice Response Unit. A device that plays voice menus to a caller and responds to caller instructions entered on a touch tone phone. Also known as Interactive Voice Response (IVR).

Nortel Contact Recording

Planning, Installation and Administration Guide

Nortel Networks
Mervue Business Park
Galway, Ireland

Copyright © 2008-2009 Nortel Networks. All Rights Reserved.

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

Any other use of the data and the transmission process is a violation of the user license unless specifically authorized in writing by Nortel Networks prior to such use. Violations of the license by alternative usage of any portion of this process or the related hardware constitutes grounds for an immediate termination of the license and Nortel Networks reserves the right to seek all allowable remedies for such breach.

Publication number:	NN44480-300
Product release:	6.5
Document release:	Standard 01.15
Date:	October 2009

Nortel, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

To provide feedback or report a problem with this document, go to
www.nortel.com/documentfeedback.

