NORTEL

Nortel Contact Center

Server Administration

NN44400-610

Document status: Standard
Document issue: 01.10
Document date: 27 August 2010
Product release: Release 7.0
Job function: Administration
Type: NTP
Language type: English

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT “AS IS” WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Contents

New in this release

The following sections detail what is new in the *Nortel Contact Center Server Administration* (NN44400-610) for Release 01.10.

- Features (page 18)
- Other changes (page 22)

Features

See the following sections for information about feature changes:

- TAPI SP configuration (page 18)
- Security settings (page 19)
- Single Sign-On (page 19)
- Redundancy and resiliency (page 19)
- SIP Contact Center compatibility (page 19)
- Changes to the Communication Control Toolkit Console (page 20)
- Data Management Tool (page 20)
- Dashboard utility (page 20)
- Instant message support on Contact Center Multimedia (page 20)
- Backup and restore procedures (page 20)
- Multiplicity (page 21)
- Instant Experts (page 21)
- Integrated Reporting (page 21)

TAPI SP configuration

The Telephone Application Programming Interface Service Provider (TAPI SP) configuration is embedded in the Communication Control Toolkit administration utility of the Communication Control Toolkit (CCT) Console. As a result, support is no longer available for legacy TAPI SP clients. The following procedure reflects this change:

- Importing address and terminal data from the switch (page 311)

Security settings

The Security Framework applies to Nortel Contact Center Manager Administration only.

Communication Control Toolkit 7.0 uses Windows Communication Foundation (WCF) as the communication layer between the Communication Control Toolkit server and the Communication Control Toolkit clients. This is more secure than Communication Control Toolkit 6.0 and requires no NAT configuration.

Single Sign-On

Single Sign-On (SSO) is part of the identity framework that enables the end user to log on to one application and remain authenticated when navigating to another application. SSO reduces the frequency of re-entering credentials for the same identity.

A session token is required for authentication and therefore enables the SSO after a user logs on to the secured framework.

SSO is only valid through the same Internet Explorer (IE) session. The user must re-authenticate if a new browser window is opened.

Redundancy and resiliency

To provide improved service continuity and data integrity, you can configure Contact Center Manager Server and Communication Control Toolkit with a shadowing process so that a second server is a standby server if the active server goes down. The shadowing process monitors the state of the active server while replicating the Contact Center data to the standby server.

If a communication error occurs, an application fails, or the network or hardware fails, processing automatically switches from the active server to the standby server with no user intervention.

Contact Center Multimedia shadowing operates as it did in Release 6.0, but it now uses the common Redundancy and Resiliency utility for configuration and manual switchover between the primary and redundant server.

SIP Contact Center compatibility

A Session Initiated Protocol (SIP)-enabled environment offers features that enrich customer interaction with the contact center, including inbound voice contacts, video, document sharing, instant messaging, and buddy lists.

Changes to the Communication Control Toolkit Console

Contact Center Release 7.0 contains several minor changes to the Communication Control Toolkit Console. The following section describes changes to the graphical interface:

- Server settings configuration (page 298)

Data Management Tool

In the Communication Control Toolkit, you can export all data from the database to an XML file, and you can import content from an XML file into the Communication Control Toolkit database.

CSV file formats are supported for data imports and exports.

For more information about the data management, see the following sections:

- Importing bulk resources (page 321)
- Exporting resource configuration to a CSV file (page 323)

Dashboard utility

The Contact Center Multimedia Service Control utility is now replaced with a Dashboard utility that tracks resource usage.

Instant message support on Contact Center Multimedia

Contact Center Multimedia for a Microsoft OCS system supports instant messaging using applications such as Instant Messenger.

You can configure settings for an agent such as auto-phrases and initial greetings, and user identification for the conversation.

For more information about instant messaging configuration, see the following sections:

- Creating an automatic phrase (page 398)
- Configuring automatic text (page 402)

Backup and restore procedures

A new common application is available to back up and restore the Caché database on the Contact Center Manager Server, Communication Control Toolkit, and Contact Center Multimedia servers.

For information about backing up and restoring the Caché databases, see the following sections:

- Creating a backup location (page 492)
- Performing an immediate backup of the database (page 494)
- Scheduling a backup of the database (page 496)

- Restoring a backup (page 498)
- Migrating the database (page 500)

Web services

The Web services are a series of SOAP-based Open Interfaces available to third parties to communication-enable applications based on the SOA architecture. With these Web services, you can use the functionality offered by each Web service using a Web Services Data Library (WSDL).

Contact Center 7.0 offers the following Open Interface tools:

- Communication Control Toolkit Open Interface
- Open queue Open Interface
- Open Networking Open Interface
- Contact Center Multimedia Open Interface
- Contact Center Manager Administration (CCMA) Open Interface

Multiplicity

The Multiplicity feature allows agents to manage multiple Instant Message (IM) Web Communications contacts simultaneously with an email contact. You can enable the feature with the Multiplicity settings.

Instant Experts

Unified Communications (UC) Presence has two tabs, My Contacts and CC Contacts. My Contacts tab lists agents that agents in your Contact Center configure with Microsoft Office Communicator (OC).

CC Contacts tab lists Instant Experts groups that you configure. Instant Experts feature allows agents in your contact center to have instant access to centrally-administered lists of IM-enabled experts and other agents. You can create and edit Instant Experts lists with Expert Administration tool.

Integrated Reporting

Contact Center Manager Server (CCMS) has an Integrated Reporting capability for Contact Center Multimedia (CCMM) and Interactive Communications Portal (ICP) statistics.

The CCMS database provides new reporting views for the following statistics:

- CCMM ContactByContact statistics
- ICP Session Detail Record (SDR) statistics
- ICP Collection Status statistics

The CCMA Report Creation Wizard (RCW) can be used to create these integrated reports.

Other changes

See the following sections for other changes in Release 7.0:

- Administration data (page 22)
- No support for pcAnywhere (page 22)

Administration data

All Server Administration information is in a single document, rather than a separate document for each server application for Contact Center as it was in previous releases.

No support for pcAnywhere

Support for pcAnywhere as a remote access tool is removed for Contact Center 7.0. Nortel recommends that you use Microsoft Remote Desktop Client or LogMeIn Rescue for remote support.

Introduction

The Nortel Contact Center Server Administration (NN44400-610) provides you with all information required to perform additional configuration for your Contact Center servers after the initial configuration.

Prerequisites

- Read *Nortel Contact Center Overview* (NN44400-111).
- Read *Nortel Contact Center Fundamentals* (NN44400-110).
- Read *Nortel Contact Center Planning and Engineering* (NN44400-210).
- Complete *Nortel Contact Center Installer Roadmap* (NN44400-310).
- Ensure that you understand which Contact Center features you purchased.
- Install, upgrade, or migrate your Contact Center 7.0 software. See *Nortel Contact Center Installation* (NN44400-311).
- Commission your Contact Center 7.0 software. See *Nortel Contact Center Commissioning* (NN44400-312).

Navigation

- Contact Center Manager Server (page 24)
- Contact Center Manager Server Utility (page 71)
- Contact Center Manager Administration (page 139)
- Security Commissioning (page 232)
- Network Control Center Server (page 268)
- Communication Control Toolkit Server (page 290)
- Contact Center Multimedia (page 325)
- Managing Security (page 451)
- Common server administration (page 484)

Contact Center Manager Server

Contact Center Manager Server fundamentals

This chapter provides an overview of the Contact Center Manager Server tools and utilities.

Navigation

Configuration utility

Use the configuration utility, Nbconfig, to view the local server settings, the address table, and the sites for your Contact Center Manager servers.

If your contact center is in a networked environment, you can use the configuration utility to add sites to the Network Control Center.

The following access levels are available:

- regular access level—Read the information in the Configuration utility.
- administration access level—Change the server settings.

You can view the following information in the Nbconfig dialog box:

- Local Machine Settings—The Local Machine Settings tab lists the local site name and network card IP addresses.
- Address Table—The Address Table tab lists the computer name, IP address, and port information of all servers in the network, including the Network Control Center.

- Site Table—The Site table tab lists information about site names, IP addresses, and flags. When you log on to the Network Control Center in administration mode, use this page to add sites.

For information about working with the Configuration utility, see the following sections:

- Starting the Configuration utility with regular access level (page 35)
- Starting the Configuration utility with administration access level (page 35)

Database Integration service functionality

The Contact Center Manager Server installation automatically installs the Database Integration service. The Database Integration service runs as a Contact Center Manager service when it is enabled by the license manager. When the Database Integration service starts, it

- registers as a service provider to the Host Data Exchange (HDX) service
- registers with the Telephony Application Programming Interface (TAPI) server, if TAPI is enabled in the Database Integration Wizard, and connects to the database as required to run queries and procedures

The connection to the database requires access permissions. Your Contact Center Manager Server Host Application Integration (HAI) service and the Database Integration Wizard must use the correct context to connect to the database.

The Database Integration service and the Database Integration Wizard use the Common Object Request Broker Architecture (CORBA) version of the HDX interface to communicate generically with external databases, TAPI servers, or both.

Interaction of the Database Integration service with HDX

The HDX service maintains connections between registered third-party applications and Database Integration call processing.

The following is an example of the call processing script functions between the HDX service and a registered third-party application:

1. When the call processing script encounters an HDX script command (for example SEND INFO, SEND REQUEST, or GET RESPONSE), it packages the parameters into a message.
2. The HDX service receives and queues the message. A registered third-party application can then use the HDX interface to retrieve the message.
3. The service provider receives the message, unpacks the data it contains, and runs the specified service.

4 If the specified service is a request, the request is run, and the results are packaged into a message and is returned to the HDX.

5 When the HDX receives the message, it routes the data to call processing.

6 Call processing receives the message, unpacks the data, and maps the values to the call variable parameters of the response script function.

The Database Integration service registers with HDX as a third-party application with a unique provider ID. The provider ID is a unique ID that identifies HDX applications to Contact Center Manager. Contact Center Manager scripts use provider IDs to identify HDX applications.

After registering with HDX, the Database Integration service enables the exchange of data between the Contact Center Manager script and any Open Database Connectivity (ODBC) 3.51-compliant database.

You can configure the Database Integration Wizard to register the Database Integration service with the TAPI server. After you register the service with the TAPI server, you can attach data to a call.

The HDX provides a maximum of 10 client application connections. A client application refers to an application written to interact directly with the Contact Center Manager script. The HDX service that provides service to the third-party client applications. The Database Integration Wizard is a client of the HDX service.

Attention: Although the Database Integration Wizard is installed on the Contact Center Manager Server, the Wizard is a separate HDX client application and uses one of the 10 available HDX connections. When the Database Integration Wizard runs, nine HDX client application connections are available. The HDX limit for the size of a data parameter is 80 bytes.

When Contact Center Manager Database Integration is shut down, all existing registrations are released and the open connections to the Data Source Names (DSN) are closed.

Interaction with application commands

After you use the Database Integration Wizard to configure the Database Integration service, you can use call processing script commands for the HDX to integrate with the HAI service.

When the system retrieves a message from the HDX, the system checks the message type:

- SEND REQUEST, GET RESPONSE commands are used for database access and for data retrieval from TAPI.

- SEND INFO is used for database access and for TAPI call data attachment.

The first parameter of SEND REQUEST or SEND INFO is crucial to the operation of Database Integration Wizard. For SEND INFO, the first parameter indicates if TAPI call data attachment is to occur or if database access is required for the Database Integration Wizard. For SEND REQUEST, the first parameter indicates if TAPI is invoked or if the request is for database access for the Database Integration Wizard. For database access (SEND REQUEST or SEND INFO), the first parameter indicates the unique number of the SQL statement to run. For these reasons, at least one parameter is required for SEND REQUEST and SEND INFO.

SEND REQUEST

You can use the SEND REQUEST command to retrieve information from a database or from TAPI. The first parameter of the SEND REQUEST command indicates if the target is database access or TAPI. If the first parameter is %TAPI%, the system requests information from TAPI.

```
SEND REQUEST DIW_PROVIDER_ID "%TAPI%", DATA 1
```

The system checks the parameter to determine if it corresponds to the SQL statements that you constructed using the Database Integration Wizard. If a corresponding SQL statement is found, the statement is selected to run on a Data Source Name (DSN). Stored statements are associated with particular DSNs. If a connection does not exist for the particular DSN, a connection is enabled for it. Connections are maintained for as long as the service runs.

The remaining parameters of SEND REQUEST provide information to the unknown parameters of the SQL statement (you can use up to nine parameters). The unknown parameters are identified by a question mark (?) in the SQL statement identification. Where multiple unknown parameters exist, a question mark (?) appears in the SQL statement for each unknown parameter. The HDX request must send a parameter for each question mark encountered in the SQL statement. Each question mark is replaced, in order, by the parameters in the HDX request as they are encountered. The type of each request parameter must match the data type of the SQL data field.

In the following example, the SQL statement number referenced in HAI_SQLNO_cv runs. This statement expects a single parameter (that is, it has a single question mark [?]), which is replaced by the CLID of the call when the statement runs.

```
SEND REQUEST HAI_AppID HAI_SQLNO_cv, CLID
```

GET RESPONSE

All request messages are accompanied by a GET RESPONSE message. The first parameter of the GET RESPONSE message indicates the status of the SQL statement execution. Returned data from the statement execution populates the remaining message parameters. All remaining parameters of the GET RESPONSE message have a default value of NULL, which is represented within the script as a blank value for a string and a zero for an integer.

The first parameter of the GET RESPONSE is reserved as a string variable to store the status of the SQL procedure. The returned value is one of the following:

- SUCCESS—The SQL statement ran successfully.
- FAILED—The SQL statement failed. Examine the log files to determine the reason for failure (for example, attempting to run an invalid SQL statement results in a FAILED operation).
- NODATA—The SQL statement is of type SELECT; however, no data was returned.

The system packages the returned data in a service completion message, and passes it back to the HDX.

If the GET RESPONSE command returns data from a CCT/TAPI application, each piece of data must be separated by a RECORD_SEPARATOR, defined as follows:

```
#define RECORD_SEPARATOR 0x1E
```

The RECORD_SEPARATOR ensures that each piece of data can be supplied separately in the GET RESPONSE command.

You must check any SQL query configured in the Database Integration Wizard to ensure that it does not use an excessive amount of time to run. By default, the GET RESPONSE command waits 10 seconds for the query to execute before it times out. If the GET RESPONSE command times out, the script continues without the response. Depending on the nature of the query, this can cause call handling to be disrupted.

If an SQL query runs longer than 10 seconds, you can perform one of the following activities:

- Optimize the SQL query so that it takes less time to execute (for example, rewrite the query or use stored procedures).
- Use the optional TIMER parameter of the GET RESPONSE command to increase the timeout value.

In the following example, the executed SQL statement is expected to return a single piece of information, namely the ID of an agent. Use this information for direct queuing to a preferred agent. The status of the SQL execution is stored in the STRING call variable HAI_SQLRESP_cv. Configure the script to check the status of execution and use the information only if the response indicates SUCCESS.

```
GET RESPONSE HAI_AppID HAI_SQLRESP_cv, HAI_AGENTID_cv
```

SEND INFO

Use the SEND INFO command to access script and call data and attach the data to a call by using TAPI. The first parameter of the SEND INFO request identifies whether the target is database access or TAPI. If the first parameter is %TAPI%, the remaining parameters are attached to the call using the IVR/CallData interface provided by TAPI. When attached to the call in TAPI, each data parameter is separated by a RECORD_SEPARATOR.

If the first parameter is not %TAPI%, the SEND INFO command provides database access. In this case, the first parameter is the numeric identifier of the SQL statement to run. The numeric identifier can identify an SQL statement (such as UPDATE) that does not return data to Contact Center Manager. The same principles described for SEND REQUEST apply to SEND INFO when you use it for database access.

The following sample Contact Center Manager scripts illustrate both usages of SEND INFO.

Example 1: SEND INFO for database access

```
/* Execute SQL statement number 5 passing the current callid as
parameter */
ASSIGN 5 TO HAI_SQLNO_cv
ASSIGN "%CALLID%" TO HAI_CALLID_cv
SEND INFO provId HAI_SQLNO_cv, HAI_CALLID_cv
```

Example 2: SEND INFO for TAPI access

```
/* Attach the text 'abandoned' to the call */
ASSIGN "%TAPI%" TO HAI_STRING_cv
ASSIGN "ABANDONED" TO HAI_DATA_cv
SEND INFO provId HAI_STRING_cv, HAI_DATA_cv
```

The previous examples illustrate scripts where the HAI service performs a single action on a voice contact processed by a script. Often, multiple HAI service actions occur sequentially in the script for a single contact. When the result of one action depends on a previous action being completed fully, ensure that the action is fully complete before the next action is executed.

You must change the following registry keys to sequentially run script commands:

\\HKEY_LOCAL_MACHINE\\SOFTWARE\\Nortel\\ICCM\\HAI\\Threads\\WorkerThreads value=1

\\HKEY_LOCAL_MACHINE\\SOFTWARE\\Nortel\\ICCM\\HAI\\Threads \\WorkerThreadsSleep value=60

Stored procedures

The Database Integration service in Contact Center Manager 7.0 supports the use of stored procedures on the database server. Stored procedures are precompiled sets of SQL statements you create in and the system stores on the database server.

The Database Integration Wizard invokes stored procedures by using conventions appropriate to the database vendor.

Creating stored procedures

You can create stored procedures on the database server by using database server software. For instructions to create stored procedures, consult your database vendor documentation.

Using complex SQL statements in Microsoft SQL Server

Executing an SQL statement when the database is configured to return the number of rows affected by that Transact-SQL statement or stored procedure can return invalid results as the number of rows affected is returned as part of the results. To ensure the SQL statement runs successfully, use the SET NOCOUNT ON setting to prevent the counting of the number of rows to be affected.

Using stored procedures that support SELECT...INTO only

When you use stored procedures that support only the SQL construction of SELECT... INTO, invoke the procedures in the following order:

- SEND INFO, to invoke the stored procedure
- SEND REQUEST and GET RESPONSE, to retrieve the data put into the variables by using the SQL construction of SELECT...INTO

The threading model in HAI can make the system process the SEND INFO and SEND REQUEST commands in the wrong order. If this happens, the script receives invalid data. To guarantee the order of the commands, set the value of the following registry key to 1:

HKEY_LOCAL_MACHINE\SOFTWARE\NORTEL\ICCM\HAI\Threads

The default setting has two worker threads, which provides fast performance but does not guarantee order of execution.

If you adjust the worker thread setting, you must also adjust the sleep timer setting. The default value for the sleep timer is 120.

Using stored procedures in Oracle

When a stored procedure must return data to the script, the stored procedure must prepare the data in a form that can be retrieved by HAI. The data must be available to provide information for the parameters of a GET RESPONSE request. Some databases support output parameters where the data is returned in parameters when the procedure is called. This data is not available to HAI and this type of stored procedure is not directly supported by HAI. For example, parameters can be identified as OUT in Oracle. The data passed in the OUT parameter cannot be retrieved by HAI.

Feature report

The feature report provides easy access to the system attributes on the Contact Center Manager server:

- Customer name
- Company name
- Site name
- Nortel Subnet IP address
- Contact Center Manager Server license type
- Contact Center Manager Server version

To access the Feature Report, click Start, All Programs, Nortel, Contact Center, Manager Server, Configuration on the Contact Center Manager server.

Multicast Address and Port Configuration

Use the Multicast Address and Port Configuration utility to change the default data for the optional Real-Time Statistics Multicast (RSM) feature. You can change the following settings:

- the IP multicast address to which each server in Contact Center Manager Server sends real-time statistics

- the ports at which real-time statistics are received
- the multicast Time to Live (TTL) value for RSM
- the default multicast rate for each port at which real-time statistics are received.

Multicast Stream Control

Use this utility to modify settings for applications that require that real-time statistics be turned on manually.

The real-time statistics groups that you need to turn on or off vary depending upon the applications that receive data from the RSM service. Nortel recommends that you review the documentation for each RSM-dependent application in Contact Center Manager Server before you modify the RSM settings.

Server setup configuration

Use the Contact Center Manager Server Setup Configuration utility to modify the data completed during the initial installation of the Contact Center Manager Server. You can change the local settings, the licensing, and the Communication Server 1000 switch information.

For information about working with the Configuration utility, see the following sections:

- Changing the local settings configuration (page 36)
- Changing the licensed features configuration (page 37)
- Changing the Communication Server 1000 switch data (page 40)

Web services

The Open Queue Open Interface delivers existing Open Queue functions to third-party applications that use a Web service. Third-party applications can add and remove contacts of a specific type in the Contact Center.

For more information, see the SDK documentation.

The Open Networking Open Interface enables a third-party application to transfer a call between nodes in a network with any data associated with that call intact. Third-party applications can reserve a Landing Pad on the target node to enable the voice contact to be transferred with data attached. The Web services also provide a function to cancel the reserving of a Landing Pad freeing it for other calls to be transferred across the network.

For more information, see the SDK documentation.

Contact Center Manager Server configuration

This chapter describes how to change the configuration properties for the Contact Center Manager Server software on your server.

The following configuration utilities are available:

- Configuration utility (Nbconfig)—Manage the sites and server information.
- Server Setup Configuration utility—Manage the licensing and default settings for Contact Center.

This chapter also discusses the basic password configuration required for Contact Center Manager Server.

Prerequisites to Contact Center Manager Server configuration

- Install Contact Center Manager Server. See *Nortel Contact Center Installation* (NN44400-311).
- Commission Contact Center Manager Server. See *Nortel Contact Center Commissioning* (NN44400-312).

Navigation

- Starting the Configuration utility with regular access level (page 35)
- Starting the Configuration utility with administration access level (page 35)
- Changing the local settings configuration (page 36)
- Changing the licensed features configuration (page 37)
- Changing the Communication Server 1000 switch data (page 40)
- Changing the NGenDist, NGenDesign, or NGenSys passwords (page 42)

Starting the Configuration utility with regular access level

Start the configuration utility with regular access level to read the information about the local machine settings, the address tables, and the site table for your contact center.

Procedure steps

Step	Action
1	Click **Start, Run**.
2	In the **Run** text box, type **nbconfig**.
3	Click each tab to view the content.
4	Click **OK**.

--End--

Starting the Configuration utility with administration access level

Start the configuration utility with administration access level to change configuration and add sites to your networked contact center.

Procedure steps

Step	Action
1	Click **Start, Run**.
2	In the **Run** text box, type **nbconfig -admin**.
3	Edit the sites.
4	Click **OK**.

--End--

Changing the local settings configuration

Change the local configuration settings of the Contact Center Manager Server, after you install the Contact Center Manager Server software, to change the names and IP addresses required for Contact Center to run.

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Manager Server**, **Server Configuration**.
2	In the **Server Configuration** dialog box, click the **Local Settings** tab.
3	Update the local settings.
4	Click **Apply All** or **OK**.
5	Click **Exit**.

--End--

Variable definitions

Variable	Value
Company Name	The name of the company that uses the Contact Center Manager Server software.
Customer Name	The designated contact person at the company that uses Contact Center software.
ELAN Subnet IP Address	The IP address of the embedded local area network, a dedicated Ethernet LAN that connects the Contact Center Manager Server and the switch. You must select the check box for the ELAN Subnet IP Address if you use an ELAN subnet.
Nortel Server Subnet IP Address	The IP address of the subnetwork that connects the Nortel Contact Center servers (Contact Center Manager Server, Network Control Center, Contact Center Manager Administration, Contact Center Multimedia, and (optionally) CallPilot) are connected.
Real-Time Statistics Multicast IP Address	The RSM IP address of the server to associate with sending real-time data. The IP address must be 224.0.1.0 to 239.255.255.255. The default is 230.0.0.1.
Site Name	The site name for the Contact Center Manager Server. The site name must not contain spaces or non alphabetical characters except for hyphen (-) and underscore (_). The first character must be a letter. The site name must be unique and can consist of any combination of 6 to 15 characters.

Changing the licensed features configuration

Change the licensing configuration of the Contact Center Manager Server, after you install the Contact Center Manager Server software, to update the licensing details.

You can use this application to enable or disable the features of Contact Center including open queue, networking, and predictive outbound.

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Manager Server**, **Server Configuration**.
2	In the **Server Configuration** dialog box, click the **Licensing** tab.
3	Update the licensing details.
4	Click **Apply All.**
5	Click **OK**.
6	Click **Exit**.

--End--

Variable definitions

Variable	Value
CCMS Package	The installation package indicates the licenses that you purchased with Contact Center: • CCS200: The base package for Contact Center on the current supported switching platforms. • CCS300: The networking package. • CCS350: The Network Control Center package for multiple Contact Center Manager Servers
CLAN Subnet IP Address	The IP address of the entire IP network including the ELAN subnet and the Nortel server subnet.
ELAN Subnet IP Address	The IP address of the embedded local area network, a dedicated Ethernet LAN that connects the Contact Center Manager Server and the switch. You must select the check box for the ELAN Subnet IP Address if you use an ELAN subnet.
Optional Packages	You must choose the package you purchased. Some packaged features includes: • Open Queue—Use Contact Center Multimedia to route multimedia contacts to agents by using the existing scripting and skillset routing features available for calls. You must install and license the Open Queue feature for Contact Center Agent Desktop (CCAD) and configure Open Queue on the Communication Control Toolkit server. • Open Interfaces Universal Networking—Use Network Skill-Based Routing to route voice and multimedia contacts between networked sites in a mixed switch environment.
Serial Number	The serial number for the Contact Center suite license manager. You must obtain the serial number from your distributor.

Changing the Communication Server 1000 switch data

Change the Communication Server/Meridian 1 switch data after you install Contact Center Manager Server to enable communication with the Contact Center Manager Server as well as between the Communication Server/ Meridian 1 switch and CallPilot.

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Manager Server**, **Server Configuration**.
2	In the **Server Configuration** dialog box, click the **Switch CS1000** tab.
3	Update the CS1000 Switch Data details.
4	Click **Apply All**.
5	Click **OK**.
6	Click **Exit**.

--End--

Variable definitions

Variable	Value
Alternative Switch Customer Number	The customer number of the switch, if more than one customer is registered for the switch.
Alternative Switch IP Address	The IP address of the switch, if more than one IP address is registered for the switch.
Alternative Switch Serial Number	The serial number of the switch, if more than one serial number is registered for the switch.
CallPilot Alternative IP Address	The IP address of the alternate CallPilot voice connection for the Communication Server 1000/ Meridian 1 switch.
CallPilot Alternative Port	The port number of the alternate CallPilot voice connection type to the Contact Center Manager Server when working with a Communication Server 1000/Meridian 1 switch. The default port number is 5060.
CallPilot IP Address	The IP address of the primary CallPilot voice connection type to the Contact Center Manager Server when working with a Communication Server 1000/Meridian 1 switch.
CallPilot Port	The port number of the primary CallPilot voice connection type to the Contact Center Manager Server when working with a Communication Server 1000/Meridian 1 switch. The default port is 5060.
Switch Customer Number	The customer number for the switch.
Switch IP Address	The IP address of the switch.
Switch Name	The name of the CS 1000/M1 switch. Valid characters for switch names are A-Z, a-z, 0-9, underscore (_), and period (.). Switch names must begin with an alphabetical character and cannot contain spaces. The last character must not be an underscore or period. Switch names must not exceed 80 characters in length.

Changing the NGenDist, NGenDesign, or NGenSys passwords

Change the passwords for the Nortel user accounts NGenDist, NGenDesign, and NGenSys immediately after the installation to protect your system from unauthorized access.

NGenDist and NGenDesign are Windows remote access accounts that the distributor or Nortel customer support can use to remotely log on to the server if requested by the customer. These accounts are created during the server software installation. To ensure server security, change the NGenDist and GenDesign passwords.

Nortel recommends that you change all passwords regularly to maintain system security. If you reinstall the server software, the system recreates default accounts and passwords and you must change the passwords.

Procedure steps

Step	Action
1	Log on to the server as administrator.
2	Click **Start**, **All Programs**, **Administrative Tools**, **Computer Management**.
3	Click **Local users and groups**, and then double-click **Users**.
4	Right-click **NGenDist**.
5	Click **Set Password**.
6	Click **Proceed**.
7	In the **Password** box, type the new password. Ensure that you use a password that contains a combination of numbers and letters.
8	In the **Confirm Password** box, type the same password you entered in the **Password** box.
9	Click **OK**.
10	Click **OK**.
11	Repeat step 3 to step 10 for NGenDesign and NGenSys.
12	Close the **Computer Management** window.
13	Record these passwords and store them in a secure place away from the server.

--End--

Procedure job aid

If you change the NGenSys password, you must apply the same password change to the Meridian Application Server (MAS) Backup and Restore service.

After you change passwords, remember to log on as NGenSys. You must log on as NGenSys to monitor and manage the server.

Configure SNMP on the server

Windows provides a Simple Network Management Protocol (SNMP) agent, which runs as a service on Contact Center Manager Server. You can use this service to forward events to a Network Management System (NMS) on your network.

When you configure the server, you choose the types of events to be forwarded to the NMS. For example, you may choose to forward only Unknown and Critical events. However, you may also be interested in tracking a Minor event, such as 41553. If you configure the server to forward all Minor events, a significant amount of traffic is generated on your Nortel server subnet. To avoid this, but still track event 41553, you can use the Event Preferences feature. This feature allows you to temporarily assign event 41553 a priority of Critical. After you do so, the event is automatically forwarded to the NMS.

Navigation

Attention: You need to reconfigure the existing SNMP if you uninstall Contact Center 6.0, and then upgrade to Contact Center 7.0.

Configuring the Windows SNMP service to forward traps to an NMS.

Install Windows Simple Network Management Protocol (SNMP) agent to forward events to a Network Management System (NMS) on your network.

Procedure steps

Step	Action
1	Log on to the server as NGenSys.
2	Click **Start**, **Programs**, **Administrative Tools**, **Services**.
3	In the **Services** window, select the **SNMP Service**.
4	Click **Action**, **Properties**.
5	In the **SNMP Service Properties** window, click the **Traps** tab.
6	If no community name is defined, in the **Community name** box, type public.
7	Click **Add to list**.
8	Click **Add** to add the IP address of the NMS to which the server sends traps.
9	In the **SNMP Service Configuration** window, type the IP address of the NMS.
10	Click **Add**.
11	In the **SNMP Service Properties** window, click **OK**.
12	In the **Services** window, right-click the **SNMP Trap** Service, and select **Start**.
13	Close the **Services** window.
14	Click **Start**, **All Programs**, **Accessories**, **Windows Explorer**.
15	Browse to the folder **D:\Nortel\bin**, and double-click **SNMPFilterCnfg.exe**.
16	In the **Level of Filtering** box, select the event types to forward to the NMS.
17	Click **OK**.

--End--

Selecting the types of events to be forwarded

Ensure that you use SNMPFilterCnfg.exe to forward all Contact Center Manager Server related events (these events fall between the range 44900 to 51400).

Procedure steps

Step	Action
1	From the **Start** menu, choose **Programs**, **Accessories**, **Windows Explorer**.
2	Browse to the folder **D:\Nortel\bin**, and double-click **SNMPFilterCnfg.exe**.
3	In the **Level of Filtering** box, select the types of events that you want to forward to the NMS.

Attention: All event types that appear and the type that you select are also forwarded. For example, if you select Major, then all Unknown, Critical, and Major events are forwarded.

Step	Action
4	Click **OK**.

--End--

Configuring the NMS

After you configure the server, you must configure the NMS to receive and interpret traps (including identification to the NMS, and the origin and format of the Contact Center Manager Server traps). To do so, you must load or compile the Contact Center Manager Server Management Information Block (MIB) files in the NMS.

The following MIB files describe the format of the traps generated by the server:

- nt-ref.mib (MIB-II)
- nbflt.mib (NGen MIB)
- RR-NORTEL.mib (Resiliency MIHB)

You can use these files on the NMS system. They are SNMP v1 MIB files. The nt-ref.mib and nbflt.mib files are available in Contact Center Manager Server, in the D:\nortel\data, and RR-NORTEL.mib can be found in <InstallDirectory>\Nortel\Contact Center\Common Components\Cache.

For more information about configuring your NMS, see your NMS documentation.

Certificate management for SIP-CCMS

Simple Network Management Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants.

In Contact Center 7.0, SIP-CCMS enables secure communication between the Interactive Communications Portal (ICP) and the Communication Server 1000 (CS 1000) systems.

The Transport Layer Security (TLS) is the technology used to provide this secure communication. The signed security certificates enable the SIP-CCMS to recognize other servers over a network.

Prerequisites

- Install Contact Center Manager Server. See *Nortel Contact Center Installation* (NN44400-311).
- Commission Contact Center Manager Server. See *Nortel Contact Center Commissioning* (NN44400-312).

Navigation

- Obtaining a server certificate (page 47)
- Creating a server certificate (page 48)
- Converting the server certificate for SIP-CCMS (page 50)

Obtaining a server certificate

SIP-CCMS uses batch files to generate a signed security certificate. These batch files are located at D:\Nortel\ICCMM\sgm\TLSCertificates. Within these batch files are two *bat. files:

- certGen.bat—Creates a security key for the certificate used to create a certificate signing request (CSR)

- certConv.bat—Converts the signed identity certificate (CER) to a PEM format that enables SIP-CCMS to secure communication.

Procedure steps

Step	Action
1	Log on to Contact Center Manger Server.
2	Click **Start**, **Run**.
3	In the command window, type **cmd.exe**.
4	Type **D:**.
5	Type the directory location **D:\Nortel\ICCM\sgm\TLSCertificates**.
6	Type **dir**. The necessary batch files are listed.

Attention: Ensure the directories Key and CertCreation are listed. These directories are required to complete the creation process. Contact your administrator if they are not listed.

Step	Action
7	Follow the command prompts as they appear in the command window.

--End--

Creating a server certificate

Create a certificate signing request (CSR) to ask the private Certificate Authority (CA) to sign a certificate that the system can use to configure a trust relationship between parties.

With SIP-CCMS, you must create a CSR with the certGen file before you apply the CSR.

Prerequisites

- Obtaining a server certificate (page 47)

Procedure steps

Step	Action
1	Log on to Contact Center Manger Server.
2	Click **Start**, **Run**.
3	In the command window, type **certGen**. A series of messages appear for informational purposes.
4	Enter **** from the following table.
5	After each command prompt, press **Enter**.

Attention: After you complete this process, the certificate must be signed by a CA. Contact your administrator for the preferred method for obtaining the request.csr signed.

Step	Action
6	After you receive the signed certificate, save the <somename.cer> certificate in the directory location **D:\Nortel\ICCM\sgm\TLSCertificates\CertCreation**.

--End--

Variable definitions

Variable	Value
Organizational Name <company>	The company name.
Organizational Unit Name <department, division>	The department or division within a company.
Locality Name <city, district>	The city or district where the system is located.
State or Province Name <full name>	The province where the system is located.
Country Name <2 letter code>	The country code where the system is located.
Common Name <hostname, IP, or your name>	The Fully Qualified Domain Name (FQDN) of the SIP-CCMS server <computerX.DomainY.com>

Converting the server certificate for SIP-CCMS

After you obtain a CSR from the CA, you must convert the server certificate for SIP-CCMS use.

Prerequisites

- Obtaining a server certificate (page 47)
- Creating a server certificate (page 48)

Procedure steps

Step	Action
1	Log on to Contact Center Manger Server.
2	Click **Start**, **Run**.
3	In the command window, type **D:\Notel\ICCM\sgm\TLSCertificates\CertCreation**.
4	Type **certConv**, and then press **Enter**.
5	Type **Y**.
6	Enter the full name of the file, for example, certSigned.cer.

Attention: You must type the .cer extension; otherwise the process is incomplete.

--End--

Database Integration Wizard configuration

You can use the Database Integration service to exchange call data between Contact Center Manager scripts and any Open Database Connectivity (ODBC)-compliant database and to attach script data to a call or multimedia contact for storage in the database.

Prerequisites to Database integration wizard configuration

- Install Contact Center Manager Server. See *Nortel Contact Center Installation* (NN44400-311).
- Commission Contact Center Manager Server. See *Nortel Contact Center Commissioning* (NN44400-312).

Navigation

Creating and invoking a stored procedure

You can create and invoke a stored procedure (a precompiled set of SQL statements stored in the database) to repeatedly to find information in the database.

Procedure steps

Step **Action**

1 Create a table in the MySQL table editor.

2 Create a stored procedure using MySQL.

3 Test the stored procedure by using the MySQL test tool.

4 Configure the Database Integration Wizard with DSN access.

5 Construct your SQL statements using the Database Integration Wizard.

6 Write and activate the script.

--End--

Example of creating and invoking a stored procedure

Step **Action**

1 Create a table in the MySQL table editor.

2 Create a stored procedure using MySQL.

```
DROP PROCEDURE sp_GetCustomer;
delimiter |
CREATE PROCEDURE sp_GetCustomer(IN __uri VARCHAR(45),
OUT __first VARCHAR(45), OUT __last VARCHAR(45))
BEGIN
SELECT FirstName, LastName INTO __first, __last FROM
test.customers WHERE URI = __uri;
END
delimiter;
```

3 Test the stored procedure using the MySQL test tool.

```
CALL sp_GetCustomer("customer@home.com", @a, @b);
SELECT @a, @b;
```

4 Configure the Database Integration Wizard with DSN access.

5 Construct your SQL statements using the Database Integration Wizard.

6 Write and activate the script.

```
/*
```

```
SQLNO 3 is the number of the stored procedure as seen in
the Wizard
*/
ASSIGN 3 TO HAI_SQLNO_cv
ASSIGN "customer@home.com" TO HAI_FROMADDRESS_cv
SEND INFO HAI_AppId_gv HAI_SQLNO_cv, HAI_FROMADDRESS_cv
SEND REQUEST HAI_AppId_gv HAI_SQLNO_cv
GET RESPONSE HAI_AppId_gv HAI_SQLRESP_cv,
HAI_string01_cv, HAI_string02_cv
```

--End--

Configuring the system data source names

Configure the system data source names (DSN) that you want the Database Integration Wizard to use in Contact Center Manager before you run the Wizard. Use the ODBC Data Source Administrator to configure the system DSNs.

Prerequisites

- Install and configure the software and drivers to enable connection to the external database to access. You can test the database connectivity and the data access capability using the tools and techniques provided by the database vendor.

Procedure steps

Step	Action
1	On the Contact Center Manager Server, click **Start**, **All Programs**, **Administrative Tools**, **Data Sources (ODBC)**.
2	On the **ODBC Data Source Administrator** window, click the **System DSN** tab.
3	Click **Add**.
4	On the **Create New Data Source** window, select the appropriate driver. If the required driver is not present, install it using the driver setup program.
5	Click **Finish**.
6	On the driver-specific setup box, in the **Data Source Name** box, type a name for the data source.
7	In the **Description** box, type a description for the data source.

8	Configure the remaining fields for connection to the database.
9	Click **OK**.
10	Click **OK** to close the **ODBC Data Source Administrator** window.

--End--

Configuring HDX and TAPI server settings

Configure HDX and TAPI server settings to configure and test the provider ID that is used to register the Database Integration service with HDX. A single provider ID is used for both database access and TAPI connectivity.

Prerequisites

- Ensure a TAPI server is operational on the network.
- Ensure that you know the TAPI server host name or IP address and the port configured in TAPI for the IVR or CallData interface. Consult your TAPI configuration and TAPI documentation for further information.
- Configure the system DSNs. See Configuring the system data source names (page 53)
- Nortel recommends that you define the provider ID as a global variable in Contact Center Manager. If the provider ID changes, you need not compile the script to obtain the new value.

Attention: If the database requires Domain User authentication instead of database integral user accounts, then the user context running the Database Integration Wizard must be compatible with the assigned database permissions. If the user context and permissions are not compatible, you cannot connect to the database.

Procedure steps

Step	Action
1	On the Contact Center Manager Server, click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Manager Server**, **Database Integration Wizard**.
2	On the **Welcome** window, click **Next**.
3	On the **Configure HDX and TAPI Server Connections** window, in the **HDX Connection** section, in the **Provider ID** box, type the provider ID that is

used to register the Contact Center Manager Database Integration service with HDX. A provider ID of 0 is invalid.

The provider ID is required in the Contact Center Manager script to identify the appropriate provider to which it sends information. Each HDX application must have a unique ID that identifies it to Contact Center Manager. No two applications at the same site can have the same provider ID. The HDX application passes the provider ID to the target server in an attempt to register with the target server software. The developer of the HDX application chooses the provider ID for the application.

4 Click **Test Connection**.

5 Review the information presented in the **Test Output and Result** box to ensure the test is successful.

6 If you do not need to integrate your software with a TAPI server, skip to step 12.

7 In the **TAPI Connection** section, select the **Configure Tapi connection** check box.

8 In the **TAPI Server HostName** box, type the host name or the IP address of the TAPI server.

9 In the **IVR Port** box, type the port number of the IVR/CallData interface.

This port is usually configured for port 5000. However, TAPI configuration allows a port to be specified. Consult your TAPI configuration to determine the actual port.

Attention: If TAPI is co-resident with Contact Center Manager Server, ports 5000 to 5010 are not available for use. You must select another port outside of the 5000 to 5010 range.

10 Click **Test Connection**.

11 Review the information in the **Test Output and Result** box to ensure the test is successful.

Attention: If a failed condition is reported in the Test Output and Result box, check that the TAPI Server HostName and IVR port match the target TAPI server. If required, correct the configuration information and test it again. If the failure persists, ensure that the TAPI Server HostName is accessible and that the IVR port is correctly registered on the TAPI server.

12 Click **Next**.

Attention: To configure the database connections now, see the procedure to configure the database connections.

13 On the **Configure Database Connections** window, click **Next**.

14 On the **Configure Web Services** window, click **Next**.

15 On the **Construct SQL Statements**, click **Next**.

16 On the **Complete** window, click **Finish** to accept the changes and close the wizard.

--End--

Procedure job aid

If a failed condition is reported in the Test Output and Result box, check that the TAPI Server HostName and IVR port match the target TAPI server. If required, correct the configuration information and test it again. If the failure persists, ensure that the TAPI Server HostName is accessible and that the IVR port is correctly registered on the TAPI server.

The following table describes common error messages you may receive when you configure HDX and TAPI server settings.

Error message	Description
Already Connected	Contact Center Manager Database Integration is already connected to HDX.
Authorization Failed	The user details supplied are incorrect. This message indicates that the version of Contact Center Manager Database Integration is different from the HDX version. Contact Nortel Support.
Error	The connection cannot be performed. Contact Nortel Customer Support.
Incompatible Version	The version information supplied is incorrect. This message indicates that the version of Contact Center Manager Database Integration is different than the version of HDX. Contact Nortel Support.
Invalid Object	The HDX server object cannot be found, which indicates the HDX service is not running.
The Host could not be found	A server with the specified host name or IP address cannot be found on the network.
Invalid Provider ID	The provider ID entered is invalid. The valid range for a provider ID is 0 to 1999999999.
Too Many Connections	All HDX connections are used. Deregister another HDX provider to free a connection.

Configuring the database connections

Configure the database connections to configure a user name and password pair for each DSN and to test the connections.

Prerequisites

- Ensure that you have the correct access permissions to the database.
- If you are already on the Configure Database Connections window, skip to step 4.

Procedure steps

Step	Action
1	On the Contact Center Manager Server, click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Manager Server**, **Database Integration Wizard**.
2	On the **Welcome** window, click **Next**.
3	On the **Configure HDX and TAPI Server Connections** window, click **Next**.
4	On the **Configure Database Connections** window, from the **System DSNs Configured** tree, select the DSN to configure a connection to from the tree view.
5	In the **Username** box, type the user name for the selected DSN.
6	In the **Password** box, type the password for the selected DSN.
7	Click **Test Connection**.
8	Review the information presented in the **Test Output and Result** box to ensure the test is successful.

Attention: If a failed condition is flagged in the Test Output and Result box, check the test data and correct it as required.

Step	Action
9	Click **Next**.

Attention: To configure Web services now, review the procedure to configure Web services.

Step	Action
10	On the **Configure Web Services** window, click **Next**.
11	On the **Configure SQL Statements** window, click **Next**.
12	On the **Complete** window, click **Finish** to accept the changes and close the wizard.

--End--

Configuring Web services

Configure Web services to import Web service functionality.

Attention: A limitation exists on the range of Web services that you can import. You cannot use Web service methods that accept a variable number of inputs. This includes methods that take an array or list of variables as a parameter, due to the limitation that an SQL query can only accept a fixed number of simple data types.

Prerequisites

- Ensure that you have access to the Web Service Description Language (WSDL) document that describes the Web service. By providing the Uniform Resource Locator (URL) to the WSDL document, the Database Integration Wizard can generate a corresponding set of stored procedures that use the Web service.
- If you are already on the Configure Web Services window, skip to step 4.

Procedure steps

Step	Action
1	On the Contact Center Manager Server, click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Manager Server**, **Database Integration Wizard**.
2	On the **Welcome** window, click **Next**.
3	On the **Configure HDX and TAPI Server Connections** window, click **Next**.
4	On the **Configure Database Connections** window, click **Next**.
5	On the **Configure Web Services** window, in the **WSDL URL** box, type the address of the Web Service Description Language (WSDL) document that describes the Web service.
6	In the **Package Name** box, type a unique name for the Web service package.
7	If the Web service uses SSL/TLS security (for example, https://), in the **X.509 Certificate (Secure Web Services)** box, type the location of the X.509 certificate. **OR** Click **Browse** to navigate to the X.509 certificate.
8	Click **Import WSDL**. *The import process can take some time, depending on the size of the WSDL document being processed. After you import WSDL, a summary of the imported procedures appears in the Package Summary and Result box. If the import is not successful, the reason for the failure appears in the box.*

9	Click **Next**.

Attention: To configure SQL statements now, review the procedure for Constructing and testing SQL statements or stored procedures.

10	On the **Construct SQL Statements** window, click **Next**.
11	On the **Complete** window, click **Finish**.

--End--

Removing a Web service package

Remove a Web service package that you no longer require by using the Database Integration Wizard.

Procedure steps

Step	Action
1	On the Contact Center Manager Server, click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Manager Server**, **Database Integration Wizard**.
2	On the **Welcome** window, click **Next**.
3	On the **Configure HDX and TAPI Server Connections** window, click **Next**.
4	On the **Configure Database Connections** window, click **Next**.
5	On the **Configure Web Services** window, in the **Web Service Packages** section, select the package to remove.
6	Click **Delete Package**. *A message box appears asking you to confirm the removal of the Web service package.*
7	Click **Yes**.
8	Close the Database Integration Wizard.

--End--

Constructing and testing SQL statements or stored procedures

Construct and test a new SQL statement or stored procedure (or test an existing SQL statement or stored procedure) to ensure the SQL code works to locate content in the database.

Prerequisites

- Ensure that you have the correct access permissions for the database.
- If you are already on the Construct SQL Statements window, skip to step 6.

Procedure steps

Step	Action
1	On the Contact Center Manager Server, click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Manager Server**, **Database Integration Wizard**.
2	On the **Welcome** window, click **Next**.
3	On the **Configure HDX and TAPI Server Connections** window, click **Next**.
4	On the **Configure Database Connections** window, click **Next**.
5	On the **Configure Web Services** window, click **Next**.
6	On the **Construct SQL Statements** window, in the **Edit statement here** box, type the SQL statement or the stored procedure. The statement must contain valid sample data for variable parameters.
7	Select the DSN on which you want to configure an SQL statement from the tree view.
8	Click **Test Execute**.
9	In the **UserName** box, type the user name for the selected DSN.
10	In the **Password box**, type the password for the selected DSN.
11	Click **Test Connection**.
12	If the test is successful, replace the variable parameters of the statement with question marks (?), and then click **Add** to add the statement to the DSN for later selection by the Contact Center Manager Database Integration service.
13	Click **Next**.
14	Click **Finish** to accept the changes and close the wizard.

--End--

Procedure job aid

The results of the execution appear in the Test Output and Result box. If the result is not successful, check the statement for errors, correct it as required, and then test it again.

Updating an SQL statement

Update an SQL statement to correct errors or change the SQL statement.

Procedure steps

Step	Action
1	On the Contact Center Manager Server, click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Manager Server**, **Database Integration Wizard**.
2	On the **Welcome** window, click **Next**.
3	On the **Configure HDX and TAPI Server Connections** window, click **Next**.
4	On the **Configure Database Connections** window, click **Next**.
5	On the **Configure Web Services** window, click **Next**.
6	On the **Construct SQL Statements** window, on the system tree, select the statement or stored procedure. *The selected statement or stored procedure appears in the Edit statement here box.*
7	Edit the statement.
8	Click **Test Execute** to test the statement.
9	If the test is successful, replace the variable parameters of the statement with question marks (?), and then click **Update**.
10	Click **Next**.
11	On the **Complete** window, click **Finish** to accept the changes and close the wizard.

--End--

Deleting an existing SQL statement or stored procedure

Delete an existing SQL statement or stored procedure that you no longer use.

Procedure steps

Step	Action
1	On the Contact Center Manager Server, click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Manager Server**, **Database Integration Wizard**.
2	On the **Welcome** window, click **Next**.
3	On the **Configure HDX and TAPI Server Connections** window, click **Next**.
4	On the **Configure Database Connections** window, click **Next**.
5	On the **Configure Web Services** window, click **Next**.
6	On the **Construct SQL Statements** window, on the system tree, select the statement or stored procedure to delete.
7	Click **Delete**.
8	Click **Next**.
9	On the **Complete** window, click **Finish** to accept the changes and close the wizard.

--End--

Configuring the Contact Center Manager script

Configure the Contact Center Manager script to use the newly enabled function.

Use a Contact Center Manager client to edit the Contact Center Manager scripts. The HDX scripting commands are added using the provider ID, the numerical identifier, and the parameters you identified when you configured your database connections.

Prerequisites

- Use a global variable rather than a call variable for the Application ID. In this example, the call variable is used for testing.
- Use the return value from the database operation only if the operation was successful.

- Assign values to HDX variables before you use them in an HDX command.

Procedure steps

Step	Action
1	Create the call variables for passing data to and for retrieving data from the database.
2	Write and activate the script.
3	Test the script using physical calls. Ensure that the full required behavior is observed. If you do not see the required behavior, examine the trace files for the Database Integration Wizard.

--End--

Backing up the Database Integration Service

Back up the Database Integration Service to back up the current configuration.

Nortel recommends that you manually back up the current configuration and that you refresh the backups after using the Database Integration Wizard to make changes. The Database Integration Wizard backup and restore is not included in the Contact Center Manager backup and restore process.

Prerequisites

- Ensure that you export only the ODBC DSNs created for use with the Database Integration Wizard. Some Contact Center Manager DSNs reference a computer host name or IP address. If you export the entire ODBC folder and restore these DSNs after an IP address or host name change, the server can malfunction.

Procedure steps

Step	Action
1	On the Contact Center Manager Server, click **Start, Run**.
2	In the **Open** box, type **regedit**.
3	Click **OK**.

4	In the Registry Editor, open the key HKEY_LOCAL_MACHINE\SOFTWARE\Nortel\ICCM\HAI
5	From the **File** menu, select **Export**.
6	In the **Export Registry File** dialog box, type a name and location in which to store the configuration file.
7	Click **Save**.
8	In the Registry Editor, open the key HKEY_LOCAL_MACHINE\SOFTWARE\ODBC
9	From the **File** menu, select **Export**.
10	In the **Export Registry File** dialog box, type a suitable name and location to use for storing the ODBC configuration file.
11	Click **Save**.
12	Close the Registry Editor.

--End--

Restoring the configuration

Restore the configuration from a previous backup.

Prerequisites

- Perform an ODBC restore only if the server name and IP address are unchanged, and the ODBC configuration remains unchanged since the ODBC backup operation occurred. If either condition is true, perform a new backup.

Procedure steps

Step	Action
1	On the Contact Center Manager Server, click **Start**, **Run**.
2	In the **Open** box, type **regedit**.
3	Click **OK**.
4	On the **Registry Editor** dialog box, click **File**, **Import**.
5	On the **Import Registry File** dialog box, select a previously saved HAI configuration file.

6 In the **Import Registry File** dialog box, select a previously saved ODBC configuration file.

7 Click **Open**.

8 On the **Registry Editor** message box, click **OK**.

--End--

Contact Center Manager statistics configuration

This chapter describes how to configure Contact Center Manager Server statistics. You can choose to configure the multicast or unicast method of passing statistics from the Contact Center Manager Server to Contact Center Manager Administration server to manage reports.

Prerequisites to Contact Center Manager statistics configuration

- Install Contact Center Manager Server. See *Nortel Contact Center Installation* (NN44400-311).
- Commission Contact Center Manager Server. See *Nortel Contact Center Commissioning* (NN44400-312).

Navigation

Configuring the Multicast controller

Configure the Multicast controller to use the IP Multicast delivery method to send Real Time Reporting data. Multicast is a network addressing method for delivering information to a group of destinations in a one-to-many distribution.

If you plan to use the Unicast delivery method, no configuration of the Contact Center Manager Server is required and you can skip this procedure.

Prerequisites

- Ensure that you know the NGenSys password.

Procedure steps

Step **Action**

1 Log on to the server on which you installed Contact Center Manager Server as **NGenSys**.

2 Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Manager Server**, **Multicast Stream Control**.

3 In the **RTD Multicast Controller** dialog box, select the Moving Window or Interval to Date check boxes for the each Real Time statistics group to enable the setting.

4 In the **Compression** section of the window, select the **RTD Compression** check box.

5 Clear the **RSM Compression** check box.

Attention: Contact Center Manager Administration does not support RSM compression for Contact Center Manager Server.

6 Click **Apply**.

7 Click **OK**.

8 Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Manager Server**, **Multicast Address and Port Configuration**.

9 In the **RTD Multicast Configuration** dialog box, in the **Multicast IP group** box, type the multicast IP address to be used by the Contact Center Manager Server to transmit the RTD.

This is the same address as the Contact Center Manager Administration server receiving IP multicast address.

10 In the **Multicast Time To Live (TTL)** box, accept the default setting.

OR

Type a new value.

11 For the **Interval to Date** and **Moving Window IP Port** and **Multicast Rate** boxes, accept the default values.

Attention: Do not change the default ports

12 Click **Apply**.

13 Click **OK**.

14 Click **Start**, **All Programs**, **Administrative Tools**, **Services**.

15 Scroll down to **CCMS SDP_Service**.

16 Click **Restart**.

--End--

Changing the IP multicast settings

Change the IP multicast settings to configure the applications that receive data from the RSM service. You can change the IP multicast addresses, the Time To Live value for the data, IP ports, and multicast rates for the IP ports that send the real-time statistics.

Prerequisites

- Review the documentation for each RSM-dependent application that uses the RSM service in Contact Center Manager Server.

Procedure steps

Step	Action
1	On the Contact Center Manager Server, click **All Programs**, **Nortel**, **Contact Center**, **Manager Server**, **Multicast Address and Port Configuration**.
2	In the **Multicast IP group** box, type the IP multicast address that is designated as the sending address for IP multicasting in the Contact Center Manager Server.
3	In the **IP Port** boxes, type the IP port for each statistics group.
4	Change the **Multicast time to live (TTL)** value to a value that is appropriate for your network.
5	To increase or decrease the default multicast rate, in the **Multicast Rate** boxes, type a new rate in milliseconds for each port.
6	Click **OK**.
7	To activate new multicast rate settings on Contact Center Manager Server, open the configuration utility, and click **Apply**.

--End--

Variable definitions

Variable	Value
Default value	The values of the Multicast rates provided when you install Contact Center Manager Server.
Registry value	The values of the Multicast rates stored in the registries. You can select this value to cancel changes in the rates boxes.

Procedure job aid

When you change a multicast rate in the configuration utility, you modify the current transmission rate after you click Apply. A delay can occur when the new rate is larger than the existing rate, but the change is immediate from the application perspective.

Configuring the multicast rate equal to 0 (zero) disables the statistic. This is the same as disabling the statistic in the Multicast Stream Control utility by clearing the check box of the matching statistic. The behavior is equivalent because both utilities can read and write to the same portion of the registry.

You can observe the delay when you open the Multicast Stream Control and Multicast Address and Port Configuration utilities at the same time and make the changes. Refresh the settings of each utility using the Registry Value and Get Current States of the Multicast Stream Control and Multicast Address and Port Configuration utilities, respectively.

Disconnecting Terminal Services sessions

Disconnect the terminal services session to use the unicast transmission of statistics from the Contact Center Manager Server to the Contact Center Manager Administration server for reporting purposes.

Prerequisites

- Plan to use unicast transmission for statistics.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Click **Start**, **Administrative Tools**, **Terminal Services Manager**.

3 In the **Terminal Services Manager** window, in the right pane, click the **Sessions** tab.

4 In the right pane, right-click the session to disconnect, and select **Disconnect**.

5 Click **OK**.

6 Close the Terminal Services Manager window.

--End--

Contact Center Manager Server Utility

Access Class operations

Today, much information that is vital to companies is transmitted over networks. These networks must be protected so that only authorized users can access, change, or delete information.

The system administrator establishes and maintains system security. By assigning the appropriate access classes to the appropriate users, the administrator can help ensure system security. For example, you can restrict access to certain Server Utility components to senior administrators.

Prerequisites to Contact Center Manager Server Utility access class operations

- Install and commission Server Utility. See *Nortel Contact Center Installation* (NN44400-311) and *Nortel Contact Center Commissioning* (NN44400-312).

Navigation

- Logging on to Server Utility (page 73)
- Creating an access class (page 73)
- Viewing members of an access class (page 74)
- Modifying access class properties (page 75)
- Previewing the list of access classes (page 76)
- Printing the list of access classes (page 77)
- Deleting an access class (page 77)

Logging on to Server Utility

You must log on to the Server Utility to perform tasks relating to access classes.

The default log on information for the Server Utility is

- User ID: sysadmin
- Password: nortel

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Server Utility**, **Server Utility**.
2	On the **Nortel Contact Center Manager Server Utility Login** dialog box, in the **User ID** box, type the user ID for the Contact Center Manager Server on which to log on.
3	In the **Password** box, type the password for the Contact Center Manager Server on which to log on.
4	From the **Server Name or IP address** list, select the Contact Center Manager Server name or IP address.
5	Click **OK**.

--End--

Creating an access class

Create an access classes from the Server Utility window. You can also add access classes using the Contact Center Manager Administration client. For information about adding access classes in Contact Center Manager Administration, see the Contact Center Manager Administration online Help.

Prerequisites

- Log on to Server Utility. See Logging on to Server Utility (page 73).

Procedure steps

Step	Action
1	In the **Server Utility** window, double-click **User Administration**.
2	Double-click **Access Classes**.
3	In the **Access Classes** window, choose **File**, **New**.
4	In the **New Access Class** dialog box, in the Name box, type a name for the access class. Use a descriptive name to describe the type of user having this access level or the type of privileges available at this access level.
5	In the **Comments** box, type additional optional information about the access class.
6	Click the **Access** tab.
7	On the **Access** tab, select a function to make available to this access class. The selected function appears in the Selected item box.
8	From the **Level of Access** list, select the desired level of access for that function.
9	Repeat step 7 and step 8 for each function to which you want this access class to have access.
10	Click **Save**.
11	To return to the **Server Utility** window, click **File**, **Close**.

--End--

Viewing members of an access class

View the members of an access class from the Server Utility window. If you use Contact Center Manager Administration, you can view the members of an access class by using the Access and Partition Management component. For details, see the application online Help.

Prerequisites

- Log on to Server Utility. See Logging on to Server Utility (page 73).

Procedure steps

Step	Action
1	From the Server Utility window, expand **User Administration**.
2	Double-click **Access Classes**.
3	In the **Access Classes** dialog box, select the access class for which you want to display the members.
4	Click **File**, **Properties**.
5	On the **Access Class Properties** dialog box, click the **Members** tab.
6	On the **Members** tab, click **Cancel**.
7	To return to the Server Utility window, click **File**, **Close**.

--End--

Modifying access class properties

You can modify access class properties if the default properties do not meet your users' needs if you log on as system administrator. You can modify the access permissions and the users for each access class. You cannot modify the name or the description of the access class.

Prerequisites

- Log on to Server Utility as a system administrator. See Logging on to Server Utility (page 73).
- Create the access classes to modify. See Creating an access class (page 73).
- Configure users in CCMA. See *Nortel Contact Center Manager Administration – Client Administration* (NN44400-611).

Procedure steps

Step	Action
1	In the **Server Utility** window, double-click **User Administration**.
2	Double-click **Access Classes**.
3	From the Access Classes window, select the access class to change.

4 Click **File, Properties**.

5 Click the **General** tab.

6 View the name and the description of the access class.

7 Click the **Access** tab.

8 On the **Access** tab, select a function to make available to this access class.

The selected function appears in the **Selected item** box.

9 From the **Level of Access** list, select the level of access for that function.

10 Repeat step 8 and step 9 for each function to which you want this access class to have access.

11 Click the **Members** tab.

12 Add the members to the access class.

13 Click **Save**.

14 To return to the **Server Utility** window, click **File**, **Close**.

--End--

Previewing the list of access classes

Preview the list of available access classes to determine which access class provides a new user with the required level of accessibility.

Prerequisites

- Log on to Server Utility. See Logging on to Server Utility (page 73).

Procedure steps

Step	Action
1	In the **Server Utility** window, double-click **User Administration**.
2	Double-click **Access Classes**.
3	From the Access Classes window, click **File, Print Preview**.
4	Select the **Print Preview Range**.
5	Click **Print Preview**. *A window appears showing the current list of classes and assignments. You can print the list from the Print Preview window.*

--End--

Variable definitions

Variable	Value
Print Preview Range	Choose to print all of the access classes, or only the selected access class.

Printing the list of access classes

Print the list of available access classes for corporate records to determine which access class provides a new user with the required accessibility.

Prerequisites

- Log on to Server Utility. See Logging on to Server Utility (page 73).

Procedure steps

Step	Action
1	In the **Server Utility** window, double-click **User Administration**.
2	Double-click **Access Classes**.
3	From the Access Classes window, click **File, Print**.
4	Select your printer and the printer properties.
5	Click **OK**.

--End--

Deleting an access class

Delete an access class that you no longer use.

Attention: You cannot delete the default access class (AdminGroup, Call Center Admin, or Supervisor) or any access class that has members.

Prerequisites

- Log on to Server Utility. See Logging on to Server Utility (page 73).

Procedure steps

Step	Action
1	In the **Server Utility** window, double-click **User Administration**.
2	Double-click **Access Classes**.
3	From the Access Classes window, select the access classes to delete, and click **File, Delete**.
4	In the Confirmation dialog box, click **Yes**.

--End--

Connected user and user account operations

This chapter describes how to administer users who are currently connected to the server and their user accounts and privileges.

A desktop user account uses the Server Utility application to access Contact Center Manager Server. You must create a desktop user account for each user who requires access to the server. You must also assign each account the access class that gives users the privileges they need to perform their job.

You can use the Server Utility to create desktop user accounts. Users can use these accounts to log on to the Server Utility, to access the server database, or to log on to a wallboard.

For third-party access to the Cache database or real-time data in Contact Center Manager, the administrator can use the Server Utility to create desktop user accounts with permission granted to select all data from the Historical Reporting views or real-time data. The administrator cannot configure desktop users as supervisors.

You can view the system administrator (sysadmin) desktop user, which exists on all Contact Center Manager Servers, in the Server Utility through Desktop Users.

Prerequisites to Contact Center Manager Server Utility connected user operations

- Install and commission Server Utility. See *Nortel Contact Center Installation* (NN44400-311) and *Nortel Contact Center Commissioning* (NN44400-312).
- Log on to Server Utility. See Logging on to Server Utility (page 73).

Navigation

- Viewing a list of connected users (page 80)
- Printing a list of connected users (page 80)

- Logging off a user (page 81)
- Setting privileges for a user (page 82)
- Adding desktop user accounts (page 87)
- Preventing users from accessing the server (page 89)
- Restoring access to the server for a user (page 89)
- Resetting desktop passwords (page 90)
- Changing the properties of a desktop user (page 91)
- Printing a list of users (page 92)
- Deleting a desktop user (page 92)

Viewing a list of connected users

Check the status of a connection to the server for a desktop user.

Procedure steps

Step	Action
1	From the **Server Utility** window, click **System Administration**, **System Configuration**.
2	Double-click **Connected Sessions**. *The Connected Sessions window appears. This list displays the desktop users who are logged on to the server, their user IDs, their location (network address), and the time of their last activity on the system.*
3	To return to the **Server Utility** window, choose **File**, **Close**.

--End--

Printing a list of connected users

Print a list of users connected to the Contact Center Manager Server to produce a hard copy of the list recorded in the Contact Center.

Procedure steps

Step	Action
1	From the **Server Utility** window, click **System Administration**, **System Configuration**.
2	Double-click **Connected Sessions**.
3	In the **Connected Sessions** window, choose **File**, **Print**.
4	Choose the options for your printer.
5	Click **Close**.

--End--

Logging off a user

Immediately disconnect and log off a user. The disconnected user is not warned.

Procedure steps

Step	Action
1	From the **Server Utility** window, click **System Administration**, **System Configuration**.
2	Double-click **Connected Sessions**.
3	In the Connected Sessions window, select the PC User ID of the user to disconnect.
4	Choose **File**, **Disconnect Session**.
5	In the message box that appears asking you to confirm your choice, click **Yes**. *You return to the Connected Sessions window. The user is no longer on the list.*
6	Click **File**, **Close**.

--End--

Setting privileges for a user

You can assign a variety of privileges to certain functions to provide users with the accessibility they need to successfully perform their job.

Procedure steps

Step	Action
1	For each access class, select the Contact Center Manager Server functions that members of that class can use in Server Utility.
2	Create desktop user accounts for users who require access to Contact Center Manager Server functions.
3	Assign access classes to user accounts, giving users the privileges they need to perform their jobs.

--End--

Procedure job aid

The following table describes the privileges assigned to functions in Server Utility.

Function	Privilege	Description
Access Classes	View	View the properties for any access class.
	Edit	View and modify properties for any access class.
	Create/Delete	View, modify, add, or delete access classes.
Activity Codes	View	View the properties for any activity codes.
	Edit	View and modify properties for any activity codes.
	Create/Delete	View, modify, add, or delete activity codes.
Agent Threshold Classes	View	View the properties for any agent threshold class.
	Edit	View and modify properties for any agent threshold class.
	Create/Delete	View, modify, add, or delete agent threshold class.

(1 of 6)

Function	Privilege	Description
Agent to Skillset Assignments	View own agents only	View the properties for the agents configured in your group.
	View and assign own agents only	View the properties and assign skillsets for the agents configured in your group.
	View all agents	View the properties for all agents configured in the contact center.
	View and assign all agents	View the properties and assign skillsets for all agents configured in the contact center.
Agent to Supervisor Assignments	View own agents only	View the properties for the agents configured in your group.
	View and assign own agents only	View the properties and assign supervisors for the agents configured in your group.
	View all agents	View the properties for all agents configured in the contact center.
	View and assign all agents only	View the properties and assign supervisors for all agents configured in the contact center.
Alarm Monitor	View	View event details for system alarms.
	Create/Delete	View event details for system alarms, clear and acknowledge system alarms.
Application Threshold Classes	View	View the properties for any application threshold classes.
	Edit	View and modify properties for any application threshold class.
	Create/Delete	View, modify, add, or delete application threshold classes.
Applications	View	View the properties for any application.
	Edit	View and modify properties for any application.
Backup Scheduler	View	View the list of available backup schedules.
	Edit	View and modify the properties of backup schedules.
	Create/Delete	View, modify, and delete backup schedules.
Call Presentation Classes	View	View the call presentation classes.
	Edit	View and modify the call presentation classes.
	Edit, Create/Delete	View, modify, and delete the call presentation classes.
CDNs	View	View the call distribution numbers.
	Edit	View and modify the call distribution numbers.
	Edit, Create/Delete	View, modify, and delete the call distribution numbers.
Connected Sessions	View	View the connected sessions window.
	Create/Delete	View the connected sessions and log off any connected users.

(2 of 6)

Function	Privilege	Description
DNISs	View	View the dialed numbers.
	Edit	View and modify the dialed numbers.
	Create/Delete	View, modify, and delete the dialed numbers.
Emergency Help	View	View the emergency help configuration.
Event Browser	View	View all Informational, Critical, Minor, or Major events in the Event Browser.
Event Preferences	View	View event preferences configured for event codes.
	Edit	View event preferences and increase or decrease the severity.
	Create/Delete	Create event preferences, increase or decrease the severity, and delete event preferences.
Formulas	View	View formulas for statistical reports.
	Edit	View and modify formulas for statistical reports.
	Create/Delete	Create and delete formulas for statistical reports.
Historical Statistics	View	View historical statistics.
	Edit	View and modify historical statistics.
IVR ACD-DN Threshold Classes (CS 1000/ Meridian 1)	View	View IVR ACD-DN Threshold Classes
	Edit	View and modify IVR ACD-DN Threshold Classes
	Create/Delete	Create and delete IVR ACD-DN Threshold Classes
IVR ACD-DNs (CS 1000/ Meridian 1)	View	View IVR ACD-DNs.
	Edit	View and modify IVR ACD-DNs.
	Create/Delete	Create and delete IVR ACD-DNs.
Network Communication Parameters	View	View Network Communication Parameters.
	Edit	View and modify Network Communication Parameters.
Network Historical Statistics (NCC)	View	View Network Historical Statistics.
	Edit	View and modify Network Historical Statistics.
Network Skillsets (NCC)	View	View network skillsets.
	Edit	View and modify network skillsets
	Create/Delete	Create and delete network skillsets.
Nodal Threshold Class	View	View nodal threshold classes.
	Edit	View and modify nodal threshold classes.

(3 of 6)

Function	Privilege	Description
Phoneset Displays (CS 1000/Meridian 1)	View	View phoneset displays
	Edit	View and modify phoneset displays.
Phonesets	View	View phonesets.
	Edit	View and modify phonesets.
	Create/Delete	Create and delete phonesets.
Real-Time Displays	View own agents	View your agents in real-time displays.
	View own agents–create displays	View your agents in real-time displays and create displays.
	View all agents	View all agents in real-time displays.
	View all agents–create displays	View all agents in real-time displays and create displays.
Real-time Statistics	View	View real-time statistics.
	Edit	View and modify real-time statistics.
Reports	Create and run any report	Create and run any report.
Reports–Agent Performance	Create and run any report	Create and run Agent Performance reports.
Reports–Call by Call	Create and run any report	Create and run Call by Call reports.
Reports–Other	Create and run any report	Create and run Other reports.
Route Threshold Classes (CS 1000/Meridian 1)	View	View route threshold classes.
	Edit	View and modify route threshold classes.
	Create/Delete	Create and delete route threshold classes.
Routes (CS 1000/ Meridian 1)	View	View routes.
	Edit	View and modify routes.
	Create/Delete	Create and delete routes.
Scheduler	View	View the scheduler.
	Edit	View and modify the scheduler.
	Create/Delete	Create and delete the scheduler.
Script Variables	View	View script variables.
	Edit	View and modify script variables.
	Create/Delete	Create and delete script variables.

(4 of 6)

Function	Privilege	Description
Scripts	View	View scripts.
	Edit	View and modify scripts.
	Create/Delete	Create and delete scripts.
Serial Ports	View	View the Serial Ports window and properties for all serial ports.
	Edit	View the Serial Ports window and view and modify properties for all serial ports.
Server Performance Monitor	View	View the Server Performance Monitor.
Server Settings	View	View detailed information about the server, such as the software release and the serial number.
Sites (NCC)	View	View sites on the NNC.
	Edit	View and modify sites on the NCC.
	Create/Delete	Create and delete sites on the NCC.
Skillset Threshold Classes	View	View skillset threshold classes.
	Edit	View and modify skillset threshold classes.
	Create/Delete	Create and delete skillset threshold classes.
Skillsets	View	View skillsets.
	Edit	View and create skillsets.
	Create/Delete	Create and delete skillsets.
Switch Resource	View	View the Switch Resource properties for the telephony switch type.
	Edit	Users can view and modify the Switch Resource properties.
Table Routing Assignments (NCC)	View	View table routing assignments.
	Edit	View and modify table routing assignments.
	Create/Delete	Create and modify table routing assignments.

(5 of 6)

Function	Privilege	Description
Users	View reporting agents only	View the Users window and view properties for reporting agents.
	View and edit reporting agents only	View the Users window and view and modify properties for reporting agents.
	Edit all agents–create agents only	View the Users window and view, modify, create, and delete any agents.
	View all users	View the Users window and view properties for all desktop users, supervisors, and agents. Users require this access privilege to generate call-by-call reports.
	Edit all users	View the Users window and view and modify properties for all desktop users, supervisors, and agents.
	Edit all users–create any type	View the Users window and view, modify, add, and delete desktop users, supervisors, and agents.
Voice Ports	View	View the Voice Ports window and view properties for all voice ports.
	Edit	View the Voice Ports window and view and modify properties for all voice ports.
Voice Prompt Editor	View	Log on to the Voice Prompt Editor and view voice files and voice segments.
	Edit	Log on to the Voice Prompt Editor and view and modify voice segments and voice files.
	Create/Delete	Log on to the Voice Prompt Editor and view, modify, add, and delete voice files and voice segments. In CallPilot, use Application Builder to work with voice prompts.
	(6 of 6)	

Adding desktop user accounts

Add a desktop user account to the server utility to configure the permissions, and accessibility to the features of the Contact Center Manager Administration application.

Prerequisites

- Create at least one access class. See Creating an access class (page 73)

Procedure steps

Step	Action
1	On the **Server Utility** window, double-click **User Administration** and then double-click **Users**.
2	In the **Users** dialog box, choose **File**, **New**.
3	In the **New User** dialog box, on the **General** page, enter the contact information for the user.
4	Click the **Desktop** tab.
5	On the **Desktop** page, in the **User ID** box, type a user ID.

Attention: The desktop user uses this to log on to the server. You cannot change the user ID after you save the user account.

Step	Action
6	Click **Set Password**.
7	In the **Set Password** dialog box, in the **New Password** and **Confirm Password** boxes, type the password. If you open an existing desktop user, this button appears as Reset Password.
8	Click **OK**. The Set Password window closes.
9	Select the **Password Expires** check box to indicate that the password expires in 180 days. For special users, such as wallboard displays used with third-party software, you can leave the check box clear so that password never expires. The administrator password does not expire.
10	From the **Access Class** list, select the access class to which to assign the user.
11	Click **Save** to save your settings and return to the **Users** window.
12	Click **File**, **Close**.

--End--

Preventing users from accessing the server

Prevent users from accessing the server to restrict access for the desktop users. You can restrict the access for desktop users who do not have the authority, knowledge, or responsibility to update the server settings.

Prerequisites

- Log off the desktop user. See Changing the properties of a desktop user (page 91).

Procedure steps

Step	Action
1	On the **Server Utility** window, double-click **User Administration**, and then double-click **Users**.
2	In the **Users** dialog box, double-click the user name.
3	In the **User Properties** dialog box, click the **Desktop** tab.
4	On the **Desktop** page, click **Lock Out**. *The user desktop status changes to Locked out by an administrator. This continues to be the current status of the user until an administrator restores it to OK. The Lock Out button changes to Restore.*
5	Click **Save**.
6	Choose **File**, **Close**.

--End--

Restoring access to the server for a user

Restore or grant access for a desktop user on the server. You can grant access for specific periods of time, or provide access to desktop users who have authority to change settings on the server.

Perform this procedure when a user is locked out of the system after exceeding the password retry count or after an administrator manually locks out a user.

Procedure steps

Step	Action
1	On the **Server Utility** window, double-click **User Administration**, and then double-click **Users**.
2	In the **Users** dialog box, double-click the user name.
3	In the **User Properties** dialog box, click the **Desktop** tab.
4	On the **Desktop** page, click **Restore**. The user desktop status changes to OK. The Restore button changes to Lock Out.
5	Click **Save**.
6	Choose **File**, **Close**.

--End--

Resetting desktop passwords

Reset desktop passwords when users forget their desktop password or if the desktop password expires.

By resetting the password, you can create a new password for the desktop user.

The desktop user password expires after 180 days unless the user changes the password within that time. Seven days before the expiry of the password, the Server Utility displays a warning message during the user logon.

If users want to change their password, they can log on to the server and click Utilities, Change Password.

Prerequisites

- Log on to Server Utility as sysadmin.

Procedure steps

Step	Action
1	On the **Server Utility** window, double-click **User Administration**, and then double-click **Users**.
2	In the **Users** dialog box, double-click the user name.
3	In the **User Properties** dialog box, click the **Desktop** tab.
4	On the **Desktop** page, click **Reset Password**.
5	On the **Reset Password** dialog box, In the **New Password** and **Confirm New Password** boxes, type the new password.
6	Click **OK** to close the **Reset Password** window.
7	Click **Save**.
8	Click **File**, **Close**.

--End--

Changing the properties of a desktop user

Change the properties of a desktop user if the default properties are not sufficient.

Prerequisites

- To change the access class of a particular user, ensure that the user is not logged on.

Attention: If the user is logged on, the server logs the user off when you make the change.

Procedure steps

Step	Action
1	On the **Server Utility** window, double-click **User Administration**, and then double-click **Users**.
2	In the **Users** dialog box, double-click the desktop user to change.
3	In the **User Properties** dialog box, make any required changes.

Step	Action
4	Click **Save** to save your changes.

--End--

Printing a list of users

Print a list of users to keep as an easy reference in company records.

Procedure steps

Step	Action
1	On the **Server Utility** window, double-click **User Administration**, and then double-click **Users**.
2	From the **Users** window, choose **File**, **Print**.
3	Select the printer and the printer options.
4	Click **OK**.

--End--

Deleting a desktop user

Delete a desktop user if that user no longer requires access to the server.

Prerequisites

- Ensure the user to be deleted is logged off; otherwise, the user is immediately logged off without warning.

Procedure steps

Step	Action
1	On the **Server Utility** window, double-click **User Administration** and then double-click Users.
2	From the **Users** window, select the desktop user to delete.

3 Click **File**, **Delete**.

--End--

Serial port configuration

Serial ports are input/output devices used to connect external equipment, such as CD-ROMs or modems, to your computer. Serial ports transmit data from these external devices one bit at a time.

You can use the Serial Ports window to view, print, or edit serial port settings. From this window, you can modify a serial port baud rate, data bits, stop bits, parity, and flow control. You can also use the Serial Port Properties page to edit serial port settings.

Prerequisites to Contact Center Manager Server Utility serial port configuration

- Install and commission Server Utility. See *Nortel Contact Center Installation* (NN44400-311) and *Nortel Contact Center Commissioning* (NN44400-312).
- Log on to Server Utility. See Logging on to Server Utility (page 73).
- Connect to a Communication Server 1000/Meridian 1 PBX server.

Navigation

- Viewing port settings (page 95)
- Printing port settings (page 95)
- Editing port settings (page 96)

Viewing port settings

View the Serial Ports window to ensure the accuracy of the port settings.

Procedure steps

Step	Action
1	In the **Server Utility** window, expand **System Administration**.
2	Expand **System Configuration**.
3	Double-click **Serial Ports**.
4	On the Serial Ports window, select a configured serial port.
5	Click **File**, **Properties**.

--End--

Printing port settings

Print the port settings to file in the company records.

Procedure steps

Step	Action
1	In the Server Utility window, expand **System Administration**.
2	Expand **System Configuration**.
3	Double-click **Serial Ports**.
4	Click **File**, **Print**.
5	Select the printer and the printer options.
6	Click **OK**.

--End--

Editing port settings

You can use the Serial Ports window to modify serial port settings, such as baud rate, data bits, stop bits, panity, and flow control.

Procedure steps

Step	Action
1	In the Server Utility window, expand **System Administration**.
2	Expand **System Configuration**.
3	Double-click **Serial Ports**.
4	From the Serial Ports window, click **File**, **Edit**.
5	On the Serial Ports window, select a configured serial port.
6	Click **File**, **Properties**.
7	Configure the changes to the properties of the Serial Port.

--End--

Server settings

This chapter describes how to view and print server resources.

Detailed information about server resources is saved to the server database during installation or you can retrieve it for technical support purposes.

Prerequisites to Contact Center Manager Server Utility server settings

- Install and commission Server Utility. See *Nortel Contact Center Installation* (NN44400-311) and *Nortel Contact Center Commissioning* (NN44400-312).
- Log on to Server Utility. See Logging on to Server Utility (page 73).

Navigation

- Viewing server resources (page 97)
- Printing server resources information (page 98)

Viewing server resources

You can view detailed information about the server resources, such as the software release number and the serial number. You can also view a list of services and features installed on your system.

Procedure steps

Step	Action
1	Log on to the server where the Server Utility is installed.
2	On the **Start** menu, click **All Programs**, **Nortel**, **Contact Center**, **Server Utility**, **Server Utility**.
3	On the Server Utility window, expand **System Administration.**

4	Expand **System Configuration**.
5	Double-click **Server Settings**.

--End--

Printing server resources information

Print server resource information to document in paper format the system configuration of your contact center for company records.

Procedure steps

Step	Action
1	Log on to the server where the Server Utility is installed.
2	On the **Start** menu, click **All Programs**, **Nortel**, **Contact Center**, **Server Utility**, **Server Utility**.
3	On the Server Utility window, expand **System Administration.**
4	Expand **System Configuration**.
5	Double-click **Server Settings**.
6	Click **File**, **Print**.
7	Select the printer and the printer options.
8	Click **OK**.

--End--

Switch configuration

You can record information about a Communication Switch 1000/Meridian 1 after initial software installation.

Switch resources are not available when you connect to a Media Application Server (MAS).

Prerequisites to Contact Center Manager Server Utility switch configuration

- Install and commission Server Utility. See *Nortel Contact Center Installation* (NN44400-311) and *Nortel Contact Center Commissioning* (NN44400-312).

Navigation

- Recording switch information (page 99)

Recording switch information

Record switch information using the Switch Resource property sheet after the initial software installation. You can record the switch type, subtype, and release number. Depending on the switch type, some fields may not be applicable and therefore be blank.

Procedure steps

Step	Action
1	Log on to the Server Utility.
2	From the Server Utility window, double-click **System Administration**.
3	Double-click **System Configuration**.
4	Double-click **Switch Resource**.

5 Ensure the **Switch Type** and **Switch Subtype** are correct.

6 Record the **Customer Number**, **Name**, and **IP Address**.

7 Enter an optional **Description**.

8 Click **Close**.

--End--

Alarm and event configuration

The Event Browser and Alarm Monitor show events that occur on the server. These programs provide many common features for viewing events. For more information about the features, see Event Browser versus Alarm Monitor features (page 103).

To view client events, such as successful logon or logoff or failure to connect, use the PC Event Browser, which provides many features for viewing events.

Events are log entries that record activities in Contact Center Manager Server, such as sending or receiving messages, opening or closing applications, and errors. Some events are for information only, while others can indicate problems. You can filter events by several categories, such as severity and event code range. You can also limit the display to the most recent events.

The main advantage of the Alarm Monitor is that it automatically appears in the foreground of the desktop when an event occurs, thus immediately alerting you to problems. You can specify whether the Alarm Monitor appears in the foreground for only critical events, major and critical events, or all events, or whether it stays in the background.

In the Alarm Monitor, you can filter events by severity only. The Alarm Monitor does not display information events.

Prerequisites to Event Browser configuration

- Install and commission Server Utility. See *Nortel Contact Center Installation* (NN44400-311) and *Nortel Contact Center Commissioning* (NN44400-312).
- Log on to Server Utility. See Logging on to Server Utility (page 73).

Navigation

- Starting the Event Browser (page 102)
- Starting the Event Browser from Server Utility (page 103)
- Sorting events in the Event Browser (page 104)

Starting the Event Browser

Start the Event Browser to view a history of events that occurred on the server.

Procedure steps

Step	Action
1	Click **Start, All Programs, Nortel, Contact Center, Server Utility, PC Event Browser**.

--End--

Procedure job aid

Event Browser versus Alarm Monitor features

Feature	In Event Browser?	In Alarm Monitor?
View events	Yes	Yes
View online Help for an event	Yes	Yes
Sort events by category	Yes	Yes
Save a list of events	Yes	No
Print a list of events	Yes	Yes
View minor, major, critical events	Yes	Yes
View information events	Yes	No
Filter events by code, type, severity, most recent events	Yes	No
Filter events using Event Preferences graphical user interface	Yes	Yes
Automatically show the graphical user interface in the foreground when an event occurs	No	Yes
Clear an event	No	Yes

Starting the Event Browser from Server Utility

You can start the Event Browser from the Server Utility.

Prerequisites

- Log on to Server Utility. See Logging on to Server Utility (page 73).

Procedure steps

Step	Action
1	On the Server Utility window, expand **System Administration**.
2	Expand **Alarms & Events**.
3	Double-click **Event Browser**.

--End--

Sorting events in the Event Browser

You can sort events based on time, event code, event type, severity, and object ID.

Prerequisites

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 103).

Procedure steps

Step	Action
1	On the Event Browser window, click the header of the column by which you want to sort.

--End--

Viewing online Help for an event

View online Help for a selected event. The online Help displays the code, severity, description, impact, and recovery action of the event. The listed recovery actions can provide a recommended action to correct the problem or additional information about the event.

Prerequisites

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 103).

Procedure steps

Step	Action
1	In the Event Browser, double-click the event to investigate.
2	Click **Help on Event**.

--End--

Saving a list of events

Nortel recommends that you save relevant sections of the event log in the event of a problem with your system. The log helps technical support representatives to thoroughly analyze your system.

Prerequisites

- Ensure the filter settings are configured to show the type and number of events to save. See Changing the filtering criteria for events (page 106).
- Open the Event Browser. See Starting the Event Browser from Server Utility (page 103).

Procedure steps

Step	Action
1	From the Event Browser window, click **File, Save Event Log**.
2	In the **Save As** dialog box, click a save range.
3	Click **OK**.
4	In the dialog box that appears, enter a recognizable file name and location.
5	Click **Save**.
6	In the Confirmation dialog box, click **OK**.

--End--

Printing a list of events

Print a record of events for technical support.

Prerequisites

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 103).

Procedure steps

Step	Action
1	On the Events Browser window, click **File, Print**.
2	Select the printer and printer options.

3	Click **OK**.

--End--

Changing the filtering criteria for events

Change the filter criteria for events so that you can either view every single event that arises or specify which event types to view. By changing the filtering criteria, you can reduce the number of events shown at one time and force the Event Browser to display only the events in which you are interested.

You can configure the event log filter to display the following:

- a specific number of most recent events, or all events (all events available on or retrieved from the system)
- events of a certain severity (critical, major, minor, information)
- a specific event code range or all event codes
- a specific type of alarm (alarm set, alarm cleared, or message)
- events that occurred during a specific date and time interval

Prerequisites

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 103).

Procedure steps

Step	Action
1	Click **File, Change Filter criteria**.
2	In the **Set Event Filter Properties** dialog box, select the **All events** or **Latest** option.
3	If you select the **Latest** option. indicate the number of most recent events you want to view.
4	Select the Severity check boxes that indicate the type of events you want to view: **Critical, Major, Minor**, **Information**.
5	Click the **Code and Type** tab.
6	On the **Code and Type** page, select the **All Codes** or **Code Range** option.
7	If you select the **Code Range** option, indicate the minimum and maximum code range to view.

8 Select all of the **Type** check boxes that interest you: **Alarm Set, Alarm Cleared,** and **Message**.

9 Select the **Interval** tab.

10 To view all events, enable **First Event** and **Last Event**. To filter events, select a **Start Time** and **End Time**.

11 Click **OK** to change the filter.

--End--

Adding an event preference

Add an event preference to override the default severity or throttling parameters of any event code. For example, you can change the preferences of an event to one of the following:

- Increase the severity of an event (for example, from Information to Minor). By increasing an event severity, you ensure that the event appears in the Alarm Monitor when it occurs.
- Reduce the severity of a recurring alarm to Information. By reducing an event severity, you prevent it from appearing in the Alarm Monitor.
- Configure the limiting parameters to reduce the frequency with which an event is logged.

Previous occurrences of the event are not affected. You can revert to the default event definition at any time by deleting the event preference for that event code.

Prerequisites

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 103).

Procedure steps

Step	Action
1	On the Server Utility window, expand **System Administration**.
2	Expand **Alarms & Events**.
3	Double-click **Event Preferences**.
4	From the Event Preferences window, click **File, New**.

5 In the **New Event Preference Properties** dialog box, in the **Event Code** box, type the event code number for the event to add.

Attention: Contact Center Manager does not accept unrecognizable event codes. For a complete list of valid event codes, see to the Event Browser and select Event Code Reference from the Help menu.

6 From the **Severity** list, select the severity to assign to the event.

7 In the **Interval** box, type the throttling interval.

8 In the **Threshold** box, type the number of instances of the event that can be logged during the specified interval.

9 Click **Save** to return to the Event Preferences window.

10 Click **File, Close**.

--End--

Variable definitions

Variables	Value
Interval	The time interval during which the event can be logged a specified number of times. For example, in 30 minutes (the interval), log the event a maximum of 10 times (the number)

Throttling all events

Use event throttling to control the frequency with which events are recorded by the server log. You can limit all events to prevent the log from becoming overcrowded. If too many instances of each event are recorded, the log might have insufficient space to record more important events. Too many instances of the same event can distract users, causing them to overlook other important events.

Prerequisites

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 103).

Procedure steps

Step	Action
1	From the Server Utility window, expand System Administration.
2	Expand **Alarms & Events**.
3	Expand **Event Preferences**.
4	From the Event Preferences window, click **File, Default Throttling**.
5	In the **Set Default Throttling Properties** dialog box, select the **Enable** check box.
6	In the **Interval** box, type the interval for which you want to configure throttling.
7	In the **Number** box, type the number of instances of each event that you want logged.
8	Click **Save** to return to the Event Preferences window.
9	Click **File, Close**.

--End--

Changing an event preference

Change an event preference if one is already defined for the event. You can change the event severity.

Prerequisites

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 103).

Procedure steps

Step	Action
1	From the Event Browser window, select the event preference to change.
2	Click **File**, **Event Details**.

--End--

Printing the list of event preferences

Print the list of event preferences for your records.

Prerequisites

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 103).

Procedure steps

Step	Action
1	From the Event Preferences window, click **File, Print**.
2	Configure the printer and print settings.
3	Click **OK**.

--End--

Deleting an event preference

Remove an event preference from the system. The event settings for severity and throttling revert to default values.

Prerequisites

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 103).

Procedure steps

Step	Action
1	From the Event Preferences window, select the event preference to delete.
2	Click **File, Delete**.

--End--

Changing the classification of an event

Change the default classification of particular events. For example, you can choose to treat a major event as a minor event if you are aware that the event is being resolved.

Prerequisites

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 103).

Procedure steps

Step	Action
1	Click **File, Change Filter criteria**.
2	In the **Set Event Filter Properties** dialog box, select the desired criteria on all tabs.

--End--

Opening the Alarm Monitor

Open the Alarm Monitor appears in the foreground when a critical, major, or minor event occurs. If you cannot see the Alarm Monitor or if it is closed, follow this procedure to open the Alarm Monitor.

Prerequisites

- Log on to Server Utility. See Logging on to Server Utility (page 73).

Procedure steps

Step	Action
1	On the Server Utility window, expand **System Administration**.
2	Expand **Alarms & Events**.
3	Double-click **Alarm Monitor**.

--End--

Refreshing the Alarm Monitor

Refresh the Alarm Monitor window any time to ensure you view the most complete list of alarms.

Attention: After you refresh the Alarm Monitor, the number of alarms can decrease. Alarms cleared by other processes are removed from the Alarm Monitor.

Prerequisites

- Open the Alarm Monitor. See Opening the Alarm Monitor (page 111).

Procedure steps

Step	Action
1	From the Alarm Monitor window, click **View, Refresh**.

--End--

Sorting events in the Alarm Monitor

Sort events in the Alarm Monitor to review particular timestamp, severity, or information level.

Prerequisites

- Open the Alarm Monitor. See Opening the Alarm Monitor (page 111).

Procedure steps

Step	Action
1	From the Alarm Monitor window, click the header of the column by which to sort.

Attention: By default, events are sorted by timestamp in reverse chronological order.

--End--

Specifying when the Alarm Monitor appears in the foreground

The Alarm Monitor appears in the foreground when any event occurs (that is, it takes the focus from the currently active window). You can configure the severity of alarm that forces the Alarm Monitor to appear in the foreground.

Prerequisites

- Log on to Server Utility. See Logging on to Server Utility (page 73).

Procedure steps

Step	Action
1	On the Server Utility window, click **Utilities**.
2	Select the menu item that meets your criteria for when you want to be alerted about new alarms.

--End--

Procedure job aid

In the Server Utility window, from the Utilities menu, choose one of the following options:

- Alert All Alarms: show the Alarm Monitor window every time an alarm is registered or updated.
- Alert Major and Critical Only: show the Alarm Monitor window every time a Major or Critical alarm is registered or updated.
- Alert Critical Only: show the Alarm Monitor window every time a Critical alarm is registered or updated.

Configuring the Alarm Monitor to appear in the background

If you do not want to see the Alarm Monitor every time it receives and updates a new alarm, you can force it to appear in the background.

Prerequisites

- Log on to Server Utility. See Logging on to Server Utility (page 73).

Procedure steps

Step	Action
1	On the Server Utility window, click **Utilities, Alerting Off**. *The Alarm Monitor moves to the background. When a critical alarm is registered, the Alarm Monitor window taskbar flashes until you move the Alarm Monitor window to the foreground.*

--End--

Obtaining more information about an alarm

Obtain additional details about a specific alarm at any time after it appears in the Alarm Monitor window.

Prerequisites

- Open the Alarm Monitor. See Opening the Alarm Monitor (page 111).

Procedure steps

Step	Action
1	On the Alarm Monitor window, double-click an alarm entry.
2	In the **Events Details** dialog box, click **Help on Event**.

--End--

Manually clearing an alarm

Clear an alarm to remove the selected alarm (but not the event that raised it) from the event log. This action also removes the selected alarm from the list in the Alarm Monitor. If the event occurs again, however, the alarm reappears in the Alarm Monitor.

Attention: Contact Center Manager automatically clears alarms when the alarm condition changes.

Prerequisites

- Open the Alarm Monitor. See Opening the Alarm Monitor (page 111).

Procedure steps

Step	Action
1	On the Alarm Monitor window, select the alarm to clear it.
2	On the Alarm Monitor, choose **File, Clear Alarm**.
3	In the **Clear Alarm** dialog box, click yes to confirm to clear the selected alarm.

--End--

Provider configuration

The Provider application receives Contact Center script information over the Host Data Exchange (HDX) interface between the Contact Center Manager Server (provider.exe host) and the Contact Center Manager Administration server (scripts).

Navigation

Starting Provider

Start Provider.

Prerequisites

- Ensure that you have administrative privileges on the server on which Server Utility is installed.

Procedure steps

Step	Action
1	Log on to the server on which Server Utility is installed.
2	Select **Start**, **All Programs**, **Nortel**, **Contact Center**, **Server Utility**, **Provider**.

--End--

Connecting to the Contact Center Manager Server

You can configure Provider to return information to the Contact Center script. The receiving side receives both SEND INFO and SEND REQUEST information from the Contact Center script. Configure the sending side to send a variety of information to the Contact Center script. The Contact Center script command GET RESPONSE receives the information sent by Provider.

Prerequisites

- Ensure that you know the Contact Center Manager Server IP address.
- Ensure that you know provider ID. The provider ID must match the ID in the Contact Center script.

Procedure steps

Step	Action
1	In the **Server Site IP Address** box, type the IP or computer name of the Contact Center Manager Server. If Provider and the Contact Center Manager Server reside on the same computer, you can use the IP address 127.0.0.1.
2	Click **Connect to Server**. *The Register button is enabled.*
3	In the **Enter Register ID** box, type the provider ID of the application.
4	Click **Register** to assign the value.

--End--

PC Event Browser configuration

Use the PC Event Browser to view events that occur on the client computers. You cannot view events that occur on the server in PC Event Browser.

Prerequisites to PC Event Browser configuration

- Ensure that you have administrative privileges on the server on which you installed Server Utility.

Navigation

- Starting the PC Event Browser (page 118)

Starting the PC Event Browser

Start PC Event Browser.

Procedure steps

Step	Action
1	Log on to the server on which Server Utility is installed.
2	Click **Start**, **Nortel**, **Contact Center**, **Server Utility**, **PC Event Browser**.

--End--

Contact Center Service Monitor configuration

You can use Service Monitor to monitor the state of services at the Network Control Center (NCC) and across multiple Contact Center Manager Servers on the NCC.

Services are divided into two categories:

- Core Services
    - Agent Skillset Manager (ASM)
    - Telephony Services Manager (TSM)
    - Meridian Link Services Manager
    - Task Flow Executor (TFE)
    - Voice Services Manager (VSM)
- Database Services
    - Operations, Administration and Maintenance Auditing (Audit)
    - Event Broker (EB)
    - Event Server (ES event server is not on every computer so this is not checked against the monitor lights)
    - Historical Data Collector (HDC)
    - Historical Data Manager (HDM)
    - Intrinsic Server (IS)
    - Operations, Administration, and Maintenance (OAM)
    - NCC Operations, Administration, and Maintenance (NCCOAM)
    - Nodal Operations, Administration, and Maintenance (NDLOAM)
    - Real-Time Data Collector (RDC)
    - Real-Time Statistics Multicast (RSM)
    - Statistical Data Manager Configuration Administrator (SDMCA)

- — Server Data Propagator (SDP)
- — Task Flow Access (TFA)

On the NCC, the services that can be running and monitored are limited to the following:

- Audit
- HDM
- OAM
- TSM
- NCCOAM

Prerequisites to Contact Center Service Monitor configuration

- Install and commission the Network Control Center. See *Nortel Contact Center Installation* (NN44400-311) and *Nortel Contact Center Commissioning* (NN44400-312).

Navigation

- Starting Contact Center Service Monitor (page 120)
- Changing the site to monitor (page 121)
- Exiting Networking Service Monitor (page 121)
- Refreshing the service status (page 122)
- Configuring the default site information (page 122)

Starting Contact Center Service Monitor

Start Contact Center Service Monitor.

Procedure steps

Step	Action
1	Log on to the server on which Server Utility is installed.
2	Click **Start**, **Nortel**, **Contact Center**, **Server Utility**, **Service Monitor**.

--End--

Changing the site to monitor

Monitor the service status of other servers in the network.

Prerequisites

- Start Contact Center Service Monitor. See Starting Contact Center Service Monitor (page 120).

Procedure steps

Step	Action
1	In the left pane, double-click **Other Sites**.
2	In the expanded list, double-click the site to monitor.

--End--

Exiting Networking Service Monitor

Exit the application to close the Service Monitor icon in the system tray.

Prerequisites

- Start Contact Center Service Monitor. See Starting Contact Center Service Monitor (page 120).

Procedure steps

Step	Action
1	In the **System** tray, right-click the **Contact Center Service Monitor** icon.
2	From the menu, select **Exit Contact Center Service Monitor**.

--End--

Refreshing the service status

Refresh the status of services.

Prerequisites

- Launch Contact Center Service Monitor. See Starting Contact Center Service Monitor (page 120).

Procedure steps

Step	Action
1	Click **Refresh Service Status**.

--End--

Configuring the default site information

Configure the default monitored site.

Prerequisites

- Start Contact Center Service Monitor. See Starting Contact Center Service Monitor (page 120).

Procedure steps

Step	Action
1	Click Set Site.
2	In the **Set IP Address of Server** dialog box, in the **CLAN IP** address box, type the IP address of the site to configure it as the default site.
3	Click **OK**.
4	Restart **Contact Center Server Monitor** for the changes to take effect.

--End--

Voice Prompt Editor configuration

To create and manage voice files and voice prompts for Contact Center Voice Services, you must log on to the Voice Prompt Editor. When you finish using the Voice Prompt Editor, you can log off and exit.

The Voice Prompt Editor is available only if you use one of the following applications:

- Contact Center Voice Services on CallPilot
- Application Builder to manage your voice prompts

Prerequisites to Voice Prompt Editor procedures

- Ensure that you are connected to Communication Server 1000/ Meridian 1.

Navigation

- Lengthening or shortening a voice segment (page 133)
- Removing all silence from a voice segment (page 134)
- Removing or adding a specified length to all voice segments (page 135)
- Removing all silence from all voice segments (page 136)
- Deleting a voice segment (page 137)
- Restoring a deleted voice segment (page 137)

Logging on to the Voice Prompt Editor

Log on to the Voice Prompt Editor to create and manage voice files and voice prompts.

Prerequisites

- Log on to Server Utility. See Logging on to Server Utility (page 73).

Procedure steps

Step	Action
1	From the **Server Utility** window, expand **System Administration**, **System Configuration**.
2	Double-click **Voice Prompt Editor**.
3	In the **Account** box, type the mailbox containing the voice prompts with which to work.
4	In the **Password** box, type the password for that mailbox.
5	In the **Telephone No.** box, type the telephone number of the phone to use to record or play back voice segments.
6	Click **Login**.

--End--

Logging off the Voice Prompt Editor

Exit the Voice Prompt Editor.

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 124).

Procedure steps

Step	Action
1	To log off the Voice Prompt Editor, choose **File**, **Logoff**.
2	Click **OK** to confirm that you want to log off. *You are logged off the current session, open voice files are closed, and the Voice Prompt Editor Login window appears.*
3	To exit completely, choose **File**, **Exit**.

--End--

Creating a voice file

Organize your voice segments into a voice file.

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 124).

Procedure steps

Step	Action
1	From the **Voice Prompt Editor** window, choose **File**, **New**.
2	In the **File Name** box, type the name of the new voice file. Voice file names are case-sensitive. When you reference voice files in scripts and variables, make sure the file name matches the name you create here.
3	In the **Subject** box, type an optional description of the new voice file.
4	To save the file, click **File**, **Save**.

--End--

Opening a voice file

Open a voice file to display a list of voice segments stored in the selected voice file.

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 124).

Procedure steps

Step	Action
1	From the **Voice Prompt Editor** window, choose **File**, **Open**.
2	In the **Open Voice File** dialog box, select the file to open.
3	Click **OK**. *You return to the Voice Prompt Editor window. The window contains the list of segments in the selected voice file.*

--End--

Reverting to a previously saved voice file

If you change a voice file and then decide that you do not want to keep the changes, you can restore the previous copy of the voice file.

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 124).
- Open a voice file and make changes to it. See Opening a voice file (page 126).

Procedure steps

Step	Action
1	From the **Voice Prompt Editor** window, choose **File**, **Revert**.

--End--

Copying a voice file

Copy a voice file.

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 124).
- Ensure that the voice file is closed.

Procedure steps

Step	Action
1	From the **Voice Prompt Editor** window, choose **File**, **Copy**.

--End--

Renaming a voice file

Rename a voice file.

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 124).
- Ensure that the voice file is closed.

Procedure steps

Step	Action
1	From the **Voice Prompt Editor** window, choose **File**, **Rename**.

--End--

Deleting a voice file

You can delete a voice file.

The voice file is not deleted until you log off the Voice Prompt Editor. Until then, you can restore any voice file that you mark for deletion.

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 124).
- Ensure that the voice file is closed.

Procedure steps

Step	Action
1	From the **Voice Prompt Editor** window, choose **File**, **Delete**.

--End--

Restoring a voice file

If you delete a voice file, you can restore it, provided that you did not log off the Voice Prompt Editor since you marked the file for deletion.

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 124).

- Ensure that the voice file is closed.

Procedure steps

Step	Action
1	From the **Voice Prompt Editor** window, choose **File**, **Undelete**.

--End--

Creating a voice segment

Create voice segments to add to voice files.

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 124).
- Open a voice file. See Opening a voice file (page 126).

Procedure steps

Step	Action
1	In the **Voice Prompt Editor** window, in the **Voice Segment** box, click **New**.
2	In the **New Voice Segment** dialog box, in the **Name** box, type the name of the new voice segment.
3	In the **Title** box, type a description for the new voice segment.
4	In the **Script** box, type the text that the new segment is to contain. (This is for reference only.)
5	Click **OK**. *The New Voice Segment dialog box closes and the new segment is created.*

--End--

Recording a voice segment

After you create voice segment file, you can record a voice segment.

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 124).
- Create a voice segment. See Creating a voice segment (page 129).

Procedure steps

Step	Action
1	In the **Voice Prompt Editor** window, select the voice segment to record.
2	Click the **Record** icon. *The phone that you specified during log on rings.*
3	Answer the phone.
4	After the tone, say the words that you want to record in the voice segment.
5	Click the **Stop** icon.
6	Hang up.
7	To record another segment, repeat step 2 to step 6.
8	Select **File**, **Save** to save the new voice segments.

Attention: You must save all new voice segments to the server before you close the Voice Prompt Editor.

--End--

Playing a voice segment

Play back a voice segment to hear what the customer hears when the voice segment is played.

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 124).
- Create a voice segment. See Creating a voice segment (page 129).

- Record a voice segment. See Recording a voice segment (page 130).

Procedure steps

Step	Action
1	In the **Voice Prompt Editor** window, select the voice segment to play.
2	Click the **Play** icon. *If the phone that you specified during log on is on-hook, it rings. If the phone is off-hook, the segment starts to play.*
3	If the phoneset is on-hook, answer the phone. *The segment starts to play.*
4	To move backward increments of 5 seconds, click the **Skip Backward** icon. **OR** To move forward by increments of 5 seconds, click the **Skip Forward** icon.
5	To play the next voice segment in the Voice Segment list, click the **Play Next** icon.
6	To stop, click the **Stop** icon.
7	Hang up.

--End--

Playing a group of voice segments

Play a group of voice segments after you record them to see how they fit together and to determine if you need to adjust the silence in any segment.

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 124).
- Create a voice segment. See Creating a voice segment (page 129).
- Record a voice segment. See Recording a voice segment (page 130).

Procedure steps

Step	Action
1	In the **Voice Prompt Editor** window, click **Group**.
2	In the **Edit Play Group** dialog box, from the **Voice Segments** list, select a voice segment to add to the play group.
3	Click **Add**. *The voice segment is added to the Play Group list.*
4	Repeat step 2 to step 3 until the voice segments that you need appear in the play group.
5	To remove a voice segment from the group, in the **Play Group** list, click the voice segment and then click **Remove**.
6	Click **Play**.
7	To move a voice segment up or down, in the **Play Group** list, click the voice segment and then click **Up** or **Down**.
8	When you finish playing the group, click **Stop**.
9	Click **Close** to return to the **Voice Prompt Editor** window.

--End--

Searching for a voice segment

Search for a voice segment by its segment ID or by one or more of the following elements:

- the name of the voice segment
- the title of the voice segment
- the words used in the voice segment (as specified in the Script box)
- the duration of the voice segment

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 124).
- Create a voice segment. See Creating a voice segment (page 129).

- Record a voice segment. See Recording a voice segment (page 130).

Procedure steps

Step	Action
1	In the **Voice Prompt Editor** window, click **Search**.
2	In the **Search for Segment** dialog box, click **Segment ID**.
3	In the **Segment ID** box, type the ID number of the voice segment.
4	To search on name, title, script, or duration, click **Text Fields**.
5	In the **Name**, **Title**, **Script**, or **Duration** boxes, type the text to find.
6	Click **Find Next**.
7	Click **Find Next** again to find the next segment that satisfies the search conditions.
8	When you finish, click **Cancel** to close the **Search for Segment** dialog box.

--End--

Lengthening or shortening a voice segment

After you record a voice segment, you can lengthen or shorten the silence in the voice segment.

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 124).
- Create a voice segment. See Creating a voice segment (page 129).
- Record a voice segment. See Recording a voice segment (page 130).

Procedure steps

Step	Action
1	In the **Voice Prompt Editor** window, select the voice segment.
2	Click **Length**.
3	In the **Edit Length for Current Segment** dialog box appears, select the **Edit Length at** option.

4 Select the **Beginning with** check box.

5 To remove voice, noise, or silence from the beginning of the voice segment, from the **Beginning with** list, select a negative number of milliseconds.

OR

To add voice, noise, or silence to the beginning of the voice segment, from the **Beginning with** list, select a positive number of milliseconds.

6 Select the **End with** check box.

7 To remove voice, noise, or silence from the end of the voice segment, from the **End with** list, select a negative number of milliseconds.

OR

To add voice, noise, or silence to the end of the voice segment, from the **End with** list, select a positive number of milliseconds.

8 Click **Apply**.

The Edit Length for Current Segment dialog box closes, and the voice segment is shortened or lengthened.

--End--

Removing all silence from a voice segment

You can remove all silence from a specified voice segment.

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 124).
- Create a voice segment. See Creating a voice segment (page 129).
- Record a voice segment. See Recording a voice segment (page 130).

Procedure steps

Step	Action
1	In the **Voice Prompt Editor** window, select the voice segment.
2	Click **Length**.
3	In the **Edit Length for Current Segment** dialog box, select the **Normalize** check box.

4 To remove all voice, noise, or silence from the beginning of the voice segment, select the **Beginning of Segment** check box.

5 To remove all voice, noise, or silence from the end of the voice segment, select the **End of Segment** check box.

6 Click **Apply**.

The Edit Length for Current Segment dialog box closes, and all silence is removed from the beginning or end of the voice segment, or from both.

--End--

Removing or adding a specified length to all voice segments

You can remove or add voice, silence, or noise to all voice segments.

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 124).
- Create a voice segment. See Creating a voice segment (page 129).
- Record a voice segment. See Recording a voice segment (page 130).

Procedure steps

Step **Action**

1 From the **Voice Prompt Editor** window, choose **File**, **Length**.

2 In the **Edit Segment Lengths in Voice File** dialog box, select **Edit Length at**.

3 Select the **Beginning with** check box.

4 To remove voice, noise, or silence from the beginning of the voice segments, from the **Beginning with** list, select a negative number of milliseconds.

OR

To add voice, noise, or silence to the beginning of the voice segments, from the **Beginning with** list, select a positive number of milliseconds.

5 Select the **End with** check box.

6 To remove voice, noise, or silence from the end of the voice segments, from the **End with** list, select a negative number of milliseconds.

OR

To add voice, noise, or silence to the end of the voice segments, from the **End with** list, select a positive number of milliseconds.

7 Click **Apply**.

The Edit Segment Lengths in Voice File dialog box closes, and all voice segments are lengthened or shortened.

--End--

Removing all silence from all voice segments

Remove all silence from all voice segments at one time.

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 124).
- Create a voice segment. See Creating a voice segment (page 129).
- Record a voice segment. See Recording a voice segment (page 130).

Procedure steps

Step	Action
1	From the **Voice Prompt Editor** window, choose **File**, **Length**.
2	In the **Edit Segment Lengths in Voice File** dialog box, select the **Normalize** option.
3	To remove voice, noise, or silence from the beginning of the voice segment, select the **Beginning of Segment** check box.
4	To remove voice, noise, or silence from the end of the voice segment, select the **End of Segment** check box.
5	Click **Apply**. *The Edit Segment Lengths in Voice File dialog box closes, and all silence is removed from the beginning or end of all voice segments.*

--End--

Deleting a voice segment

You can delete voice segments. The voice segment is not deleted until you close the voice file or log off the Voice Prompt Editor. Until then, you can restore any voice segments that you mark for deletion.

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 124).
- Create a voice segment. See Creating a voice segment (page 129).
- Record a voice segment. See Recording a voice segment (page 130).

Procedure steps

Step	Action
1	In the **Voice Prompt Editor** window, from the **Voice Segment** list, click the voice segment.
2	Click **Delete**. *The deletion mark (**d**) appears beside the selected voice segment.*

--End--

Restoring a deleted voice segment

If you delete a voice segment and then decide you do not want to delete it, you can cancel the deletion, provided that you did not close the voice file since deleting the segment.

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 124).
- Create a voice segment. See Creating a voice segment (page 129).
- Record a voice segment. See Recording a voice segment (page 130).

Procedure steps

Step	Action
1	In the **Voice Prompt Editor** window, click the voice segment marked for deletion.
2	Click **Undo**. *The deletion mark (**d**) disappears from beside the selected voice segment.*

--End--

Contact Center Manager Administration

Contact Center Manager Administration configuration

The Contact Center Manager Administration server is the location of the configuration of the main controls for your Contact Center. Use the Contact Center Manager Administration application to configure servers, agents, supervisors, skillsets, route points, and many other tools for routing contacts to agents.

For procedures to add, change, and delete items from the Contact Center Manager Administration database, see the Contact Center Manager Administration online Help and *Nortel Contact Center Manager Administration – Client Administration* (NN44400-611).

The procedures in this chapter refer to any configuration items that you must perform on the server, outside of the Contact Center Manager Administration Client application.

Prerequisites to Contact Center Manager Administration configuration

- Install Contact Center Manager Administration server. See *Nortel Contact Center Installation* (NN44400-311).
- Commission Contact Center Manager Administration server. See *Nortel Contact Center Commissioning* (NN44400-312).

Navigation

- Configuring the License Manager Service (page 141)
- Configuring your logon warning message title and text (page 142)
- Enabling the logon warning message (page 143)
- Configuring Real-Time Reporting (page 144)
- Configuring Emergency Help (page 146)
- Configuring e-mail notifications for Historical reporting (page 147)
- Creating a shared folder to export historical reports (page 149)

- Installing the Service Creation Environment (page 151)
- Configuring Agent Desktop Display parameters on the server (page 152)
- Changing the password for the iceAdmin user account (page 155)
- Configuring the LPR port for printers (page 156)
- Configuring a network printer on the CCMA server (page 157)
- Configuring a network printer to use the CCMA server as the print server (page 158)
- Configuring a network printer to use a print server other than the CCMA server (page 160)
- Installing the XML Automated Assignments feature (page 161)
- Configuring Call Recording and Quality Monitoring (page 162)
- Configuring CDN Landing Pads for Universal Networking or Integrated Reporting (page 163)
- Configuring a DNIS Landing Pad for Universal Networking (page 165)

Configuring the License Manager Service

Configure the License Manager Service for the Report Creation Wizard component to function if your Contact Center Manager Administration server is not co-resident with another Contact Center application.

If you installed the Contact Center Manager Administration server software co-resident with Contact Center Manager Server, the IP address and port number are set up by the Contact Center Manager Server installation procedure.

Prerequisites

- Ensure that the Contact Center Manager Administration server software is installed on a stand-alone server.
- Ensure that you have administrator privileges on the Contact Center Manager Administration server.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server as an administrator.

2 Click **Start, All Programs, Nortel, Contact Center, Manager Administration, Configuration**.

3 In the left pane, navigate to **Nortel, Applications, LM Service Configuration**.

4 In the right pane, click the **LM Service Configuration** icon.

5 In the **LM Service – Configuration Setup** dialog box, in the **Primary Server's IP Address** boxes, type the IP address for the primary License Manager server.

6 In the **Primary Server's Port** box, type port number for the primary License Manager server.

7 If you have a standby License Manager server, in the **Standby Server's IP Address** boxes, type the IP address for the standby License Manager server.

8 If you have a standby License Manager server, in the **Standby Server's Port** box, type the port number for the standby License Manager server.

9 Click **OK** to submit the information.

10 In the **LM Service - Configuration Setup** dialog box, click **OK**.

11 In the dialog box that prompts you to restart the License Manager Service, click **Yes**.

12 Click **OK**.

13 Close all windows.

--End--

Configuring your logon warning message title and text

You can customize a warning message that appears when users attempt to log on to the Contact Center Manager Administration server. By default, this feature is enabled in the Contact Center Manager Administration software; however, a message is not visible unless you configure your message title and text in the Local Security Policy tool of Windows Server 2003.

If you have a domain security policy in place with a logon warning message configured, you cannot change the logon warning message using this procedure. In this case, you must contact your administrator to change the logon warning message.

If you enable the Security Framework, the logon message is overridden.

Prerequisites

- Ensure that you have administrator privileges on the Contact Center Manager Administration server.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Click **Start, Control Panel, Administrative Tools, Local Security Policy**.
3	In the **Local Security Settings** window, in the left pane, navigate to **Local Policies, Security Options**.
4	In the right pane, in the list of **Security Options**, right-click **Interactive logon: Message title for users attempting to log on** and select **Properties**.
5	In the **Interactive Logon** dialog box, in the **Interactive logon** box, type your message title.
6	Click **Apply**.
7	Click **OK**.
8	In the list of **Security Options**, right-click **Interactive logon: Message text for users attempting to log on** and select **Properties**.
9	In the **Interactive Logon** dialog box, in the **Interactive logon** box, type your warning message.
10	Click **Apply**.
11	Click **OK**.
12	Close all windows to complete the procedure.
13	If the Contact Center Manager Server is part of a networked contact center, configure this setting on each Contact Center Manager Administration server.

--End--

Enabling the logon warning message

If you configured a logon warning message, enable the message. Users receive the message when they log on to Contact Center Manager Administration.

If you did not configure a logon warning message, proceed to Configuring Real-Time Reporting (page 144).

Prerequisites

- Ensure that you have administrator privileges on the Contact Center Manager Administration server.
- Configure your logon warning message title and text. See Configuring your logon warning message title and text (page 142).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Click **Start, All Programs, Nortel, Contact Center, Manager Administration, Configuration**.
3	In the **Nortel Applications Configuration** window, in the right pane, click the **Change Login Warning Settings** icon.
4	In the **LoginWarning Properties** dialog box, select the **Use Login Warning Message** check box.
5	Click **OK**.
6	Close all windows.
7	If the Contact Center Manager Server is part of a networked contact center, configure this setting on each Contact Center Manager Administration server.

--End--

Configuring Real-Time Reporting

Configure Real-Time Reporting if you plan to use multicast-based data transmission. You must configure the IP multicast addresses for the Contact Center Manager Server to receive Multicast data and the Contact Center Manager Administration server sending IP multicast data.

If you configure a replicating server, you must select the multicast transmission options under the Real-time Reporting Configuration.

If you plan to use unicast-based transmission, skip this procedure.

Prerequisites

- Ensure that the IP multicast addresses that you select for Real-time Statistics Multicast (RSM) sending and receiving are in the 224.0.1.0 to 239.255.255.255 range. Check with your network administrator for acceptable IP multicast addresses for your specific network.
- Ensure that the Contact Center Manager Administration server sending and receiving IP multicast addresses differ.
- If the Contact Center Manager Server is part of a networked contact center, ensure that all Contact Center Manager Servers within the network have the same multicast IP address.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Click **Start, All Programs, Nortel, Contact Center, Manager Administration, Configuration**.
3	In the **Nortel Applications Configuration** window, in the left pane, navigate to **Nortel, Applications, Real-Time Reporting**.
4	In the right pane, click the **RTR Registry Settings** icon.
5	In the **RTR Properties** dialog box, in the **IP Receive Address** box, type the Contact Center Manager Administration server receiving IP multicast address.
6	In the **IP Send Address** box, type the Contact Center Manager Administration server sending IP multicast address.
7	For the **Output Rate** box and the **Transform Rate** box, accept the default values (5000 and 1000).

Attention: You can adjust the default values; however, reducing the Output Rate value and the Transform Rate value increases the workload on the Contact Center Manager Administration server.

8 For the **OAM Timeout** box, accept the default value (10 000).

9 Select the **Compress Realtime Data Packets** check box.

Attention: If you clear this check box, you disable real-time data packet compression.

10 In the **Transmission Options** area, select one of the following options:

- If your network supports multicast traffic, select Multicast. Nortel recommends this option.

- If you want no multicast traffic on your network, select Unicast.
- To support both transmission types, select Multicast and Unicast.

11 If you selected the **Multicast** option, proceed to step 14.

12 In the **Maximum Unicast Sessions** box, type the maximum number of simultaneous unicast sessions that you want the server to allow.

13 Select the **Restart Real Time Reporting Service** check box.

14 Click **OK**.

The Restart ICERtdService status window appears while the service is restarts and closes after the service successfully restarts.

15 Close all windows to complete the procedure.

--End--

Procedure job aid

You may need to increase the OAM Timeout value if the following situations occur:

- You can see no partition elements in the right pane when you create or view a partition in Access and Partition Management. This can occur when a large amount of information is stored on Contact Center Manager Server and the network is slow.
- Your contact center has a large numbers of agents or skillsets. In this case, it may not be possible to return a large list of agents or skillsets when viewing a report using the Historical Reporting component or running Agent or Skillset real time displays in the Real-Time Reporting component.

Increase the OAM Timeout value to provide more time to collect the partition elements on each server. Nortel recommends that you increase this value in increments of 3000 milliseconds (5 minutes).

Configuring Emergency Help

Configure Emergency Help for an agent. If the Emergency Help feature is configured and an agent requests assistance, the supervisor is notified through the Emergency Help component of Contact Center Manager Administration. For example, if a caller is abusive to an agent, the agent can press Emergency on the phone and the supervisor is notified.

Prerequisites

- Ensure that you have administrator privileges on the Contact Center Manager Administration server.
- Ensure that the Emergency Help Configuration settings on the replicating server match the Emergency Help Configuration settings on the primary server. This applies only if you configure a replicating server.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Click **Start, All Programs, Nortel, Contact Center, Manager Administration, Configuration**.
3	In the **Nortel Applications Configuration** window, in the left pane, navigate to **Nortel, Applications, Emergency Help**.
4	In the right pane, click the **Emergency Help Registry Settings** icon.
5	In the **EH Properties** dialog box, in the **IP Send Address** box, type the IP address to which the Contact Center Manager Administration server sends Emergency Help information.
6	Select the **Restart Emergency Help Service** check box.
7	Click **OK** to restart Emergency Help.
8	Close all windows to complete the procedure.

--End--

Configuring e-mail notifications for Historical reporting

Configure Simple Mail Transfer Protocol (SMTP) to send an e-mail notification to report recipients when the Historical Reporting component of Contact Center Manager Administration generates a scheduled report.

You must install and configure the SMTP server on the Contact Center Manager Administration server.

Prerequisites

- Install Internet Information Services (IIS) on the Contact Center Manager Administration Server. See *Nortel Contact Center Installation* (NN44400-311).

- Install Microsoft Active Directory Application Mode on the Contact Center Manager Administration Server. See *Nortel Contact Center Commissioning* (NN44400-312).
- Install an SMTP Server. See *Nortel Contact Center Installation* (NN44400-311).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Click **Start**, **Administrative Tools**, **Internet Information Services (IIS) Manager**.
3	In the left pane of the **Internet Information Services (IIS) Manager** window, expand **<Computer Name> (local computer)**.
4	Right-click the **Default SMTP Virtual Server**, and click **Properties**.
5	In the **Default SMTP Virtual Server Properties** dialog box, click the **Delivery** tab.
6	Click **Advanced**.
7	In the **Fully qualified domain name** box, type the domain name of the Contact Center Manager Administration server.
8	Click **Check DNS** to validate the name of the Domain Name Service (DNS).
9	On the confirmation box, click **OK**.
10	In the **Smart host** box, type the host name of the Microsoft Exchange server.
11	Select the **Attempt direct delivery before sending to smart host** check box.
12	Select the **Perform reverse DNS** lookup on incoming messages check box.
13	Click **OK** to close the Advanced Delivery dialog box.
14	Click the **Access** tab.
15	Click **Authentication**.
16	Clear the **Basic authentication** check box.
17	Select the **Anonymous Access** check box.
18	Click **OK** to close the Authentication dialog box.
19	Click **Connection**.
20	Click **All except the list below**.
21	Click **OK**.
22	Click the **Messages** tab.

23 Select all check boxes.

24 In the **Send copy of Non-Delivery Report** to box, type the e-mail address of the person who monitors the Non-Delivery report.

25 Click **OK** to close the Default SMTP Virtual Server Properties window.

--End--

Variable definitions

Variable	Value
<Computer Name> (local computer)	The name of your local computer.
Fully qualified domain name (FQDN)	The format of the FQDN is <computername>.<domain name>.com Example: pcbox123.softwarehouse.com Domain names can include alphanumeric characters only, including hyphens (-) and periods (.) but not underscores (_).
Smart host	The smart host name must be the name of a valid mail server. Check the properties of your Microsoft exchange server to find the Smart Host name, or contact your System Administrator.

Creating a shared folder to export historical reports

Create a shared folder to export historical reports if you want multiple users to access scheduled historical reports from the same folder.

Prerequisites

- Grant change and read permissions to the users who can access the scheduled report account; for example, the iceAdmin account or the domain account.

Procedure steps

Step **Action**

1 Log on to the Contact Center Manager Administration server.

2 Create a folder.

3 Right-click the new folder and select **Sharing and Security**.

4 In the **<folder name> Properties** dialog box, on the **Sharing** page, select the **Share this folder** option.

5 Click **Permissions**.

6 In the **Permissions for <folder name>** dialog box, in the **Groups or user names** list, select **Everyone**.

7 To grant change and read permissions to the Everyone account, proceed to step 16.

8 To grant change and read permissions to the iceAdmin or domain account, click **Remove** to remove the **Everyone** account.

9 Click **Add**.

10 In the **Select Users, Computers, or Groups** dialog box, click **Advanced**.

11 Click **Find Now**.

12 In the expanded portion of the **Select Users or Groups** dialog box, locate and select the **iceAdmin** account

OR

Select the domain account used for IIS directory security.

13 Click **OK**.

14 In the **Select Users, Computers, or Groups** dialog box, click **OK**.

15 In the **Permissions** dialog box, select the account that you selected in step 12.

16 Select the **Allow** check box for the following:

- Change
- Read

17 Click **Apply**.

18 Click **OK** to close the **Permissions for <folder name>** dialog box.

19 Click **Apply**.

20 Click **OK** to close the **<folder name> Properties** dialog box.

--End--

Installing the Service Creation Environment

Install the Service Creation Environment to manage Contact Center applications. You can use applications to route contacts based on certain criteria from the contact such as skillset or customer name.

Procedure steps

Step **Action**

1 Log on to the Contact Center Manager Administration browser.

2 On the **Launchpad**, click **Scripting**.

3 In the Scripting window, on the menu, click **Service Creation**, and then click **Launch Service Creation**.

4 In the message box requesting you to download a .msi file, click **OK**.

5 In the dialog box, click **Run**.

6 In the **Service Creation Environment - InstallShield Wizard**, click Next.

7 In the **User Name,** type a name.

8 In the **Organization**, type your company name.

9 Select one of the following options:

- Anyone who uses this computer (all users)
- Only for me (User Name)

10 Click **Next**.

11 Accept the default Destination Folder.

OR

Click **Browse** to select a different location.

This folder is where the offline application is installed.

12 Click **Next**.

13 Click **Install**.

14 Click **Finish**.

--End--

Procedure job aid

Information about the Service Creation Environment is found in *Nortel Contact Center Configuration – Service Creation Environment Application Development* (NN44400-510).

Configuring Agent Desktop Display parameters on the server

The Agent Desktop Display component functions only if you use the multicast communication method from the Contact Center Manager Administration server to the client.

To use Agent Desktop Display on a client, you must configure the parameters on the Contact Center Manager Administration server. You must also have the Real-Time Reporting component installed and configured on the Contact Center Manager Administration server for Agent Desktop Display to function properly.

- Configure the Contact Center Manager Administration IP send address in the Real-Time Reporting Configuration tool.

Step	Action
1	Click **Start**, **All Programs**, **Nortel, Contact Center, Manager Administration, Agent Desktop Displays**, **Server Configuration Parameters**.
2	On the **Configuration Parameters** window, confirm that the address in the **IP multicast address** box is the Contact Center Manager Administration server IP send address in the Real-Time Reporting Configuration Tool.
3	In the **Refresh rate (seconds)** box, type the rate in seconds at which you want to refresh the display of real-time data.
4	In the **Max agents** box, type the maximum number of agents who can simultaneously log on to the Agent Desktop Display component and view the real-time statistics.
5	In the **View** mode list, select the moving window or Interval-to-date mode.
6	To require agents to log on to their phones before they can start Agent Desktop Display, select the **Agents phoneset login required for ADD** check box.
7	To disable automatic notifications for Agent Desktop Display client upgrades, select the **Disable Automatic ADD Client Upgrade** check box.
8	In the **Statistics Configuration** table, choose the statistics to appear in the Agent Desktop Display.
9	To add the statistics column to the displays, select the **Show** check box for each statistic you want to add.
10	To arrange the order in which the statistics columns appear, use the column order buttons, select the statistic to move, and then click the up or down button to change the position.

11 To configure the threshold display color, highlight a statistic, and then from the following lists, select the threshold color for that statistic.

12 If you want the selected statistic to blink in the Agent Desktop Display when the value reaches the threshold, select the **Blink** check box.

13 If you want the Agent Desktop Display to beep when the value reaches the threshold, select the **Beep** check box. If you do not select the Beep check box, proceed to step 15.

14 To indicate that a beep should occur only once, select the **Once** option.

OR

To indicate that a beep should occur continuously until the statistic reaches an acceptable value, select **Continuously**.

15 Click **Save**.

--End--

Variable definitions

Variable	Value
Agents phoneset login required for Agent Desktop Display	Require agents to log on to their phones before they start ADD. If this check box is clear, when an agent logs on to Agent Desktop Display, the agent sees data only if other agents log on to skillsets to which that agent is assigned.
IP multicast address	The IP multicast addresses that you select for RSM sending and receiving must be within the 224.0.1.0 and 239.255.255.255 range. Check with your network administrator for acceptable IP multicast addresses for your specific network.
Max agents	The maximum number of agents who can simultaneously log on to the Agent Desktop Display component and view the real-time statistics. When the number of agents who log on to the application reaches this number, additional agents who try to log on receive a message informing them to try again later. If you leave this box empty, the system uses the default value of 1 000 agents. The maximum value that you can type in this box is 3 000 agents.
Refresh rate (seconds)	The rate in seconds at which you want to refresh the display of real-time data. The minimum value is 2 seconds. If you leave this box empty, the system uses the default value of 5 seconds.
View mode	The method in which you want to view the collected data: • Moving window: In moving window mode, statistics shown represent the last 10 minutes of system activity. • Interval-to-date: In interval-to-date mode, statistics are collected only for the current interval. When the interval ends, data fields reset to 0 and collection begins for the next interval. The interval can correspond to a work shift or to another system-defined period.

Changing the password for the iceAdmin user account

After you install Contact Center Manager Administration and specify a custom password for the iceAdmin user account, change the account password.

If you forget or misplace the iceAdmin password, you must reset it. For information, see Resetting the iceAdmin password (page 544).

Prerequisites

- Ensure that you have administrative privileges on the Contact Center Manager Administration server.
- Obtain the domain account name and password from your administrator to export reports to a domain account.

Procedure steps

Step	Action
1	Click **Start, All Programs, Nortel, Contact Center, Manager Administration, Configuration**.
2	In the **Nortel Applications Configuration** window, in the left pane, expand **Nortel, Applications, IceAdmin Password Change**.
3	In the right pane, click the **IceAdmin Password Change** icon.
4	In the **IceAdmin Password Change** dialog box, In the **Old Password** box, type the old password for this account.
5	In the **New Password** box, type the new password for the iceAdmin user account.
6	In the **Confirm Password** box, type the password again.
7	If you do not want to export scheduled reports to a domain account, or if the **Domain Account** button is unavailable, proceed to step 14.
8	To export scheduled reports to a domain account, click **Domain Account**.
9	In the **Optional Domain Account Setup** dialog box, from the **Select Domain Name** list, select the name of the domain to add.
10	In the **Enter Domain Account** box, type the domain account.
11	In the **Enter Domain Account Password** box, type the domain account password.

Attention: You must enter the correct domain account password. If the password is incorrect, the process cannot continue.

12	In the **Confirm Domain Account Password** box, retype the domain account password.

13 Click **OK**.

The iceAdmin Password Change dialog box reappears and activates all scheduled reports using the domain account instead of the local iceAdmin account.

14 Click **OK**.

--End--

Configuring the LPR port for printers

Configure the Line Printer Remote (LPR) port on your server to connect a printer.

Prerequisites

- Ensure that you have the Windows Server 2003 installation disk.

Procedure steps

Step	Action
1	Log on to the server.
2	Click **Start**, **Control Panel**.
3	Select **Add/Remove Programs**.
4	In the left column, select **Add/Remove Windows components**.
5	Select the **Other Network File and Print services** check box.
6	Click **Details**.
7	Select the **Print Services for Unix** check box.
8	Click **OK**.
9	Click **Next**.
10	Click **Finish**.

--End--

Configuring a network printer on the CCMA server

Print on-demand and scheduled historical reports and scripts to a network printer. Configure a Line Print Terminal (LPT) port on the Contact Center Manager Administration server to use the network printer, and then add a local printer on this same LPT port on the Contact Center Manager Administration server.

Prerequisites

- Ensure that you have administrator privileges on the Contact Center Manager Administration server.
- Configure a network printer.
- Know the computer name of the server to which the printer is attached.
- Know the share name of the printer.

Procedure steps

Step **Action**

1 Log on to the Contact Center Manager Administration server.

2 Click **Start, Run**.

3 In the **Open** box, type **cmd** to open an MS-DOS prompt.

4 Click **OK**.

5 At the prompt, enter

```
net use <port> [\\<print server name>\<printer share
name>] / USER:<print server name>\Administrator /
PERSISTENT:YES
```

A message appears indicating that the password for the printer is invalid and asking you to type the password.

6 At the prompt, type the administrator password for the server to which the printer is attached.

7 Press **Enter**.

8 On the server, click **Start, Printers and Faxes**.

9 In the **Printers and Faxes** window, double-click **Add a printer**.

10 In the **Add Printer Wizard**, click **Next**.

11 In the **Local or Network Printer** dialog box, select the **Local printer attached to this computer** option.

12 Clear the **Automatically detect and install my Plug and Play printer** check box.

13 Click **Next**.

14 In the **Select the Printer Port** dialog box, select the **Use the following port** option.

15 From the list, select the port you typed in step 5.

16 Click **Next**.

17 In the **Install Printer Software** dialog box, in the **Manufacturer** and **Printers** lists, select the appropriate information for your printer.

18 Click **Next**.

19 In the **Name your printer** dialog box, for the question **Do you want to use this printer as the default printer**, select **Yes**.

20 Click **Next**.

21 In the **Printer Sharing** dialog box, select **Do not share this printer**.

22 Click **Next**.

23 In the **Print Test Page** dialog box, for the question **Do you want to print a test page**, select **No**.

24 Click **Next**.

25 In the **Completing the Add Printer Wizard** dialog box, click **Finish**.

--End--

Variable definitions

Variable	Value
<port>	The port name.
<print server name>	The name of the printer server.
<printer share name>	The printer share name.

Configuring a network printer to use the CCMA server as the print server

Configure a network printer that uses the Contact Center Manager Administration server as the print server.

Prerequisites

- Ensure that you have administrator privileges on the Contact Center Manager Administration server.

- Ensure that your network printer has standard TCP/IP protocol or uses a Hewlett-Packard Jet Direct card.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Click **Start, Printers and Faxes**.
3	In the **Printers and Faxes** window, double-click **Add a printer**.
4	In the **Add Printer Wizard**, click **Next**.
5	In the **Local or Network Printer** dialog box, select the **Local printer attached to this computer** option.
6	Clear the **Automatically detect and install my Plug and Play printer** check box.
7	Click **Next**.
8	Select the **Create a new port** option.
9	From the **Type of port** list, select **Standard TCP/IP Port**.
10	Click **Next**.
11	In the **Welcome to the Add Standard TCP/IP Printer Port Wizard** dialog box, click **Next**.
12	In the **Add Port window** dialog box, in the **Printer Name or IP address** box, type the printer IP address.
13	Click **Next**.
14	In the **Completing the Add Standard TCP/IP Printer Port Wizard** dialog box, click **Finish**.
15	In the **Install Printer Software** dialog box, in the **Manufacturer** and **Printer** boxes, select the appropriate information for your printer.
16	Click **Next**.
17	In the **Name Your Printer** dialog box, type the printer name (or accept the default name).
18	Click **Next**.
19	In the **Printer Sharing** dialog box, accept the default with **Share name** selected.
20	Click **Next**.
21	(Optional) In the **Location and Comment** dialog box, in the **Location and Comment** boxes, type location and comment information.
22	Click **Next**.
23	In the **Print Test Page** dialog box, click **Yes** to print a test page.

24	In the **Completing the Add Printer Wizard** dialog box, click **Finish**.

--End--

Configuring a network printer to use a print server other than the CCMA server

Configure a default network printer that is connected to a print server other than the Contact Center Manager Administration server (for example, a UNIX server).

Prerequisites

- Ensure that you have administrator privileges on the Contact Center Manager Administration server.
- If the print server is a UNIX computer, install Print Services for UNIX on the Contact Center Manager Administration server. To install this utility, use the Windows Server 2003 CD.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Click **Start, Printers and Faxes**.
3	In the **Printers and Faxes** window, double-click **Add a printer**.
4	In the **Add Printer Wizard**, click **Next**.
5	In the **Local or Network Printer** dialog box, select **Local printer attached to this computer**.
6	Clear the **Automatically detect and install my Plug and Play printer** check box.
7	Click **Next**.
8	Select **Create a new port**.
9	From the **Type of port** list, select **LPR port**.
10	Click **Next**.
11	In the **Add LPR Compatible Printer** dialog box, in the **Name or address of server providing lpd** box, type the Domain Name Service (DNS) name or IP address of the print server.

12 In the **Name of printer or print queue on that server** box, type the name of the printer as it is identified by the host, which is either the direct-connect printer or the UNIX computer.

13 Click **OK** to close the window and return to the wizard.

14 Follow the remaining prompts in the wizard to finish installing the printer.

--End--

Installing the XML Automated Assignments feature

Use the XML Automated Assignments feature to simultaneously update multiple supervisor and skillset assignments by creating a specially formatted Extensible Markup Language (XML) file.

This is an optional feature that you use with the Contact Center Management component.

For information about obtaining the XML Automated Assignment toolkit, contact a member of the Developer Program at www.nortel.com/developer. General information about the Developer Program, including an online membership application, is also available on this site.

Prerequisites

- Ensure that you have administrator privileges on the Contact Center Manager Administration server.

Procedure steps

Step **Action**

1 Log on to the Contact Center Manager Administration server.

2 Insert the Contact Center Installation DVD into the drive.

3 On the DVD, browse to **CCMA, XML Automated Assignments Service**.

4 Expand the **XML Automated Assignments Service** folder.

5 In this folder, double-click **Symposium Web Client Automated Assignments Service.msi**.

6 In the **Welcome to the InstallShield Wizard for Contact Center Manager Administration Automated Assignments** dialog box, click **Next**.

7 In the **Customer Information** dialog box, in the **User Name** box, type your user name.

8 In the **Organization** box, type the name of your organization.

9 Click **Next**.

10 In the **Destination Folder** dialog box, click **Change** to select the folder in which to store the XML files to be parsed, and the folder in which the system stores XML files that it cannot parse due to error. You can also accept the default folders.

11 Click **Next**.

12 In the **Ready to Install the Program** dialog box, click **Install**.

13 In the **Completed** dialog box, click **Finish**.

--End--

Configuring Call Recording and Quality Monitoring

You can use Call Recording and Quality Monitoring (CRQM) to navigate to the management applications for the CRQM system.

To define server names and URLs, use the Configuration component in the Contact Center Manager Administration client. Contact Center Manager Administration users can then use the server names and URLs to start the CRQM applications.

Procedure steps

Step **Action**

1 Log on to the Contact Center Manager Administration browser.

2 On the launchpad, click **Configuration**.

3 In the left pane, select the Contact Center Manager Server on which to configure **CRQM**.

4 Expand the list and select **Call Recording and Quality Monitoring**.

5 In the **Primary Serve Name** box, type the name of the primary call recording server.

6 In the **Primary Server URL** box, type the URL for the Call Recording manager software which runs on the Call Recording server.

7 In the **Standby Server Name** box, type the name of the standby call recording server.

8 In the **Standby Server URL** box, type the URL for the standby Call Recording manager software which runs on the standby Call Recording server.

9 In the **Slave Servers** section, enter the name and URL of each slave Call Recording server.

10 Click the **Quality Monitoring** heading.

11 In the **Quality Monitoring Server Name** box, type the name of the Quality Monitoring server.

12 In the **Quality Monitoring Server URL**, type the URL for the Quality Monitoring manager software which runs on the Quality Monitoring server.

13 Click the **Quality Viewer** heading.

14 In the **Quality Viewer Server Name** box, type the name of the Quality Viewer server.

15 In the **Quality Viewer Server URL** box, type the URL for the Quality Viewer manager software which runs on the Quality Viewer server.

16 Click the **Quality Archiver** heading.

17 In the **Quality Archiver Server Name** box, type the name of the Quality Archiver server.

18 In the **Quality Archiver Server URL** box, type the URL for the Quality Archiver software which runs on the Quality Archiver server.

19 Click **Submit** to save the changes.

--End--

Configuring CDN Landing Pads for Universal Networking or Integrated Reporting

A Landing Pad associates data with a call that is sent to a target site. For Universal Networking the target site reserves a Landing Pad for the call ID at the source site. The source site then requests the call server to send the call to the Landing Pad. For Integrated Reporting, only one site is involved. When the call arrives on the Landing Pad at the target site, the Contact Center Manager Server maps the call to the original call ID, along with other data specified in the Landing Pad, to determine how to route the call. For Universal Networking, the call will be routed to an agent. For Integrated Reporting, the call will be routed to a CDN specified in the Landing Pad data by the application that originated the call. Landing Pads can be configured to use either CDNs or DNISs.

For each site configured to use Universal Networking or Integrated Reporting, you must define the Landing Pads. If the site can use CDN Landing Pads, you must configure CDN Landing Pads; if the site can use DNIS Landing Pads, you must configure DNIS Landing Pads and the DNIS Network CDN. Integrated Reporting is only supported when CDN Landing Pads are used.

CDN Landing Pads may also be used to assign a call ID to an incoming call for the purpose of Integrated Reporting, and to attach data to the call without requiring CTI.

Prerequisites

Configure the CDNs on the telephony switch. For information about configuring a CDN on the telephony switch, see *Nortel Contact Center Configuration – CS1000 Integration (NN44400-512)*.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration.
2	Click **Configuration**.
3	On the system tree, in the Configuration component, double-click the server in Contact Center Manager Server to which you want to add the Landing Pad CDN (Route Point).
4	Click the **CDNs (Route Points)** heading.
5	Select the **Landing Pads** tab.
6	In the empty **Name** box at the bottom of the table, type the name of the new Landing Pad CDN (Route Point).
7	Press **Tab**.
8	In the **Number** box, type the Landing Pad CDN (Route Point) number. This number must match the number configured on the telephony switch.
9	For SIP contact centers, you must configure the Landing Pad URI. This field is only present for SIP contact centers. In the **URI** box, type the value for the Universal Resource Indicator (URI) of the CDN (Route Point) on the SIP server.
10	Select the **Acquired?** check box to acquire the CDN.
11	Press **Tab** to submit your changes.

--End--

Configuring a DNIS Landing Pad for Universal Networking

A Landing Pad associates data with a call that is sent to a target site. For Universal Networking the target site reserves a Landing Pad for the call ID at the source site. The source site then requests the call server to send the call to the Landing Pad. When the call arrives on the Landing Pad at the target site, the Contact Center Manager Server maps the call to the original call ID, along with other data specified in the Landing Pad, to determine how to route the call. For Universal Networking, the call will be routed to an agent.

For each site configured to use Universal Networking, you must define the Landing Pads. If the site can use DNIS Landing Pads, you must configure DNIS Landing Pads and the DNIS Network CDN.

Integrated Reporting is not supported when DNIS Landing Pads are used.

Prerequisites

Configure the DNISs on the telephony switch. For information about configuring the telephony switch, see *Nortel Contact Center Configuration – CS1000 Integration (NN44400-512)*.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration.
2	On the launch pad, click **Configuration**.
3	In the left pane, expand the server under which to add the DNIS LandingPad.
4	Click the **DNISs** heading.
5	Select the **Landing Pads** tab.
6	In **Name** box, type the name of the new DNIS.
7	In the **Number** box, type the DNIS number. This number must match the number configured on the telephony switch.
8	Optionally, in the **Description** box, type a description for the DNIS Landing Pad.

9 Press **Tab** to save your changes.

--End--

CS 1000 Data Extraction Tool operation

The Communication Server 1000 Data Extraction Tool is an application that extracts information about resources such as Terminal Numbers (TNs), voice ports, Controlled Directory Numbers (CDNs), Interactive Voice Response Automatic Call Distribution DNs (IVR ACD-DNs), and routes from a Communication Server 1000/Meridian 1 switch. The tool saves this information in Excel spreadsheets.

To save data entry time, you can use Excel spreadsheets with the Contact Center Manager Administration Configuration upload utility by copying the Communication Server 1000/Meridian 1 switch data and pasting it into the Configuration Tool spreadsheet templates that you download from the Contact Center Manager Administration application.

You cannot upload data from the CS 1000 Data Extraction Tool spreadsheets directly to Contact Center Manager Administration. You must copy the data from the CS 1000 Data Extraction Tool spreadsheet into the Contact Center Manager Administration Configuration Tool spreadsheet and then upload the data. Contact Center Manager Administration does not support uploading directly from the CS 1000 Data Extraction Tool spreadsheets.

For more information about Contact Center Manager Administration Configuration Tool spreadsheets, see the Contact Center Manager Administration online Help.

Prerequisites to CS 1000 Data Extraction Tool

- Connect to Communication Server 1000/Meridian 1.

Navigation

- Extracting data from a serial connection (page 168)
- Extracting data using a modem (page 169)
- Extracting data from a file (page 171)
- Capturing Terminal Number data (page 172)
- Capturing voice port data (page 174)

Extracting data from a serial connection

Extract data from the CS 1000/Meridian 1 through a serial connection using an available serial port on your computer.

When you install and use the CS1000 Data Extraction Tool on the client PC, the tool connects directly to the CS 1000/Meridian 1 through the serial port; it does not connect to the telephony switch through a server.

Prerequisites

- Ensure your serial connection parameters match the parameters of the CS 1000/Meridian 1. Contact your telephony switch administrator if you do not know which parameters to select.

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Nortel Contact Center**, **CS100 Data Extraction Tool**, **CS1000 Data Extraction Tool**.
2	In the **Select Options** dialog box, select **Serial Port**, and then click **Next**.
3	In the **CS1000 Data Extraction Tool - Step 1 of 4** dialog box, from the **Connect Using** list, select your available COM port to configure your serial connection parameters
4	In the **Connection Preferences** area, select your connection preferences.
5	In the **Flow Control** area, select a flow control option.
6	To test your COM port, click **Test**. *A message appears in the Status box informing you if your COM port is working.*
7	Click **Next**.
8	In the **CS1000 Data Extraction Tool - Step 2 of 4** dialog box, in the **Switch Resources** area, select the resources to download from the telephony switch.
9	In the **Login Account** section, enter your user ID and password for the telephony switch.

The default user ID is admin.

Attention: Do not type CS 1000/Meridian 1 overlay commands in the User ID box. Type only your user ID for the CS 1000/Meridian 1 telephony switch.

10 In the **Select option to load TN Data** section, select the overlay to use to download TN data:

- **LD 20 All TNS**
- **LD 81 Agent & Supervisors TNS**

11 In the **Customer Number** box, type your customer number.

12 Click **Browse** to select the location in which to save exported data.

13 In the **Save As** dialog box, click **OK**.

The path you select appears in the File name box.

14 Click **Next**.

The CS1000 Data Extraction Tool - Step 3 of 4 window appears, confirming your selected resources, user ID, and exported file name.

15 If the **Failed to logon** dialog box appears, exit the CS1000 Data Extraction Tool, confirm your settings, restart the CS1000 Data Extraction Tool, and then attempt to log on again.

16 Click **Next** to download the data.

The CS1000 Data Extraction Tool - Step 4 of 4 window appears indicating the progress of connecting to the CS 1000/Meridian 1, retrieving the data, and exporting it to the Excel file.

17 Click **Finish** when the data extraction is complete.

--End--

Extracting data using a modem

Extract data by using a modem to connect to the CS 1000/Meridian 1.

Prerequisites

- Connect the CS 1000/Meridian 1 switch to a modem.

Procedure steps

Step	Action
1	From the **Start** menu, select **Programs**, select **Nortel Contact Center**, select **CS100 Data Extraction Tool**, and then click **CS1000 Data Extraction Tool**.
2	In the **Select Options** dialog box, select **Modem**.
3	Click **Next**.
4	In the **CS1000 Data Extraction Tool - Step 1 of 4** dialog box, from the **Connect using** list, select the modem to use.
5	In the **Phone number** box, type the phone number used for the modem at the CS 1000/Meridian 1 telephony switch.
6	To test your COM port, click **Test**. *A message appears in the Status box informing you if your COM port is working.*
7	Click **Next**.
8	In the **CS1000 Data Extraction Tool - Step 2 of 4** dialog box, in the **Switch Resources** section, select the resources to download from the telephony switch.
9	In the **Login Account** section, type your user ID and password for the telephony switch.
10	In the **Select option to load TN Data** section, select which overlay to use to download TN data: • LD 20 All TNS • LD 81 Agent & Supervisor TNS.
11	In the **Customer Number** box, type your customer number.
12	Click **Browse** to select the location to save exported data. *The Browse for Folder window appears with the default folder selected.*
13	Accept the default selection, or navigate to the folder of your choice.
14	Click **OK**. *The path you select appears in the File name box.*
15	Click **Next**. *The CS1000 Data Extraction Tool - Step 3 of 4 dialog box appears, confirming your selected resources, user ID, and exported file name.*
16	Click **Next** to download the data.

The CS1000 Data Extraction Tool - Step 4 of 4 dialog box appears indicating the progress of connecting to the CS 1000/Meridian 1, retrieving the data, and exporting it to the Excel file.

17 Click **Finish** when the data extraction is complete.

--End--

Extracting data from a file

You can use the Extract from File option to extract data from an output file that you captured from the CS 1000/Meridian 1 and saved on your computer.

Prerequisites

- Ensure that you have at least one file from which to extract data.

Procedure steps

Step	Action
1	From the **Start** menu, point to **Programs**, point to **Nortel Contact Center**, point to **CS100 Data Extraction Tool**, and then click **CS1000 Data Extraction Tool**.
2	In the **Select Options** dialog box, select **File**.
3	Click **Next**.
4	In the **CS1000 Data Extraction Tool - Step 1 of 4** dialog box, in the **Source File name** box, type the name of the file that contains the CS 1000/ Meridian 1 data. **OR** Click **Browse** to navigate to the file.
5	Click **Next**.
6	In the **CS1000 Data Extraction Tool - Step 2 of 4** dialog box, in the **Switch Resources** section, check the telephony switch resources to download from the file.
7	In the **File name** box, type the path and file name. OR Click **Browse** to select the location in which to save exported data. *The Browse for Folder dialog box appears with the default folder selected.*
8	Click **OK**.

9 Click **Next**.

The CS1000 Data Extraction Tool - Step 3 of 4 dialog box appears, confirming your selected resources and the exported file name.

10 Click **Next**.

The CS1000 Data Extraction Tool - Step 4 of 4 dialog box appears indicating the progress of connecting to the output file and exporting the data you selected to the Excel file.

11 Click **Finish** when the data extraction is complete.

--End--

Capturing Terminal Number data

Capture a list of all configured Terminal Numbers (TNs).

Prerequisites

- Connect to Overlay program 20.

Procedure steps

Step **Action**

1 At the **LD** prompt, enter

```
20
```

2 At the **REG** prompt, enter

```
PRT
```

3 At the **TYPE** prompt, enter

```
TNB
```

4 AT the **TN** prompt, enter

```
TN
```

5 At the **CDEN** prompt, enter CDEN.

6 At the **CUST** prompt, enter the customer number.

7 At the **DATE** prompt, enter the date from which to print.

8 At the **PAGE** prompt, enter **Yes** to print data for each page.

9 At the **DES** prompt, enter a designator.

--End--

Example of capturing terminal data

An example of the output follows:

```
DES LAB30
TN 002 0 00 00
TYPE 500
CDEN 4D
CUST 0
WRLS NO
DN 7050 0 MARP
CPND
NAME 500 set-1
XPLN 9
DISPLAY_FMT FIRST,LAST
AST NO
IAPG 0
HUNT
TGAR 0
LDN NO
NCOS 0
SGRP 0 RNPG 0
XLST
SCI 0
CLS UNR DTN FBD XFA WTA THFD FND HTD ONS
LPR XRA CWD SWD MWD RMMD SMWD LPD XHD CCSD LND TVD
CFTD SFD MRD C6D CNID CLBD AUTU
ICDD CDMD LLCN EHTD MCTD
GPUD DPUD CFXD ARHD OVDD AGTA CLTD LDTD ASCD
MBXD CPFA CPTA DDGA NAMA
MCRD
EXR0 SHL ABDD CFHD DNDY DNO3
CWND USMD USRD BNRD OCBD RTDD RBDD RBHD FAXD
 CNUD CNAD
PGND FTTU
PLEV 02
SPID NONE
PRI 01
AACD NO
AACS NO
MLWU_LANG 0
FTR CFW 16 FTR PHD
FTR ACD 3500 3204
AGN
DATE 8 MAR 1999
```

Capturing voice port data

You can capture a list of all voice ports configured as TNs on the telephony switch by using Overlay program 81. To separate voice ports from the other TNs, request only those TNs with the Voice Messaging Allowed (VMA) feature.

Prerequisites

- Log onto Overlay program 81.

Procedure steps

Step	Action
1	At the **LD** prompt, enter `81`
2	At the **REQ** prompt, enter `lst`
3	At the **CUST** prompt, enter the customer number.
4	At the **DATE** prompt, enter the date.
5	At the **DES** prompt, enter the description.
6	At the **FEAT** prompt, enter `vma`

--End--

Output example

VMA	00	TN	010 0 00 01	SL1	MMAIL	NO DATE
VMA	00	TN	010 0 00 08	SL1	MMAIL	15 MAY 1997

Capturing CDN data

You can capture a list of all of the CDNs by using Overlay program 23.

Prerequisites

- Connect to Overlay 23.

Procedure steps

Step	Action
1	At the **LD** prompt, enter `23`
2	At the **REQ** prompt, enter `PRT`
3	At the **TYPE** prompt, enter `CDN`
4	At the **CUST** prompt, enter the customer number.
5	At the **CDN** prompt, enter `CDN`

--End--

Example of Overlay 23 output

```
TYPE CDN
CUST 0
CDN 4911
FRRT
SRRT
....
ACNT
```

Capturing IVR ACD-DN data

Capture a list of all of the IVR ACD-DNs by using Overlay program 23.

Prerequisites

- Connect to Overlay 23.

Procedure steps

Step	Action
1	At the **LD** prompt, enter `23`
2	At the **REQ** prompt, enter `prt`

3 At the **TYPE** prompt, enter

`ACD`

4 At the **CUST** prompt, enter the customer number.

5 At the **ACDN** prompt, enter the ACDN.

--End--

Example of output from option 11C for IVR ACD-DNs

```
TYPE ACD
CUST 0
ACDN 6700
....
CWNT NONE
```

Capturing route data

Capture a list of all of the route numbers from the switch by using Overlay program 21.

Prerequisites

- Connect to Overlay program 21.

Procedure steps

Step **Action**

1 At the **LD** prompt, enter

`21`

2 At the **REQ** prompt, enter

`prt`

3 At the **TYPE** prompt, enter

`rdb`

4 A the **CUST** prompt, enter the customer number.

5 At the **ROUT** prompt, enter the route.

6 At the **ACOD** prompt, enter the ACOD.

--End--

CCMA and Security Framework backup and restore

Nortel recommends that all contact centers perform regular backups of Contact Center Manager Administration data files to a secure location such as a tape drive or network drive. You can help your contact center to recover from events, such as data loss and damage due to disk failures and power outages, by creating a backup of your contact center data. This applies to data on the Contact Center Manager Administration server and on the server in Contact Center Manager Server. This can be the same server if you work on a co-resident installation.

If you install a replicating server, you must perform regular backups of the primary Contact Center Manager Administration server. Unlike ADAM replication, backups provide snapshots of your Contact Center Manager Administration data files at moments in time. Backing up data and not using ADAM replication as the only method of backing up Contact Center Manager Administration data is important for the following two reasons:

- Not all Contact Center Manager Administration data is stored in ADAM and therefore is not replicated.
- You cannot use replication to roll back data to a specific time, which may be required.

You can use the Nortel Backup and Restore utility to back up a preselected series of Contact Center Manager Administration files (including Historical Reporting files, ADAM files, and database files). You can also use the utility to schedule singular or multiple backup tasks on a daily, weekly, or monthly basis. However, you cannot use this utility to back up operating system files or data files that are not related to Contact Center Manager Administration.

In addition to backing up files, you must record your Real-Time Reporting configuration settings and your Emergency Help configuration settings whenever these settings change. During the restoration, you must manually reconfigure these settings.

You must back up Contact Center Administration data for the following reasons:

- To avoid loss of data in the event of a server failure, Nortel recommends that you schedule backups and back up your Contact Center Administration data at least once a day (or more frequently based on your contact center requirements). Schedule backups during periods of low activity.
- If you upgrade Contact Center Manager Administration or if you migrate Contact Center Manager Administration to a new server, you must perform a full backup of your Contact Center Manager Administration before you perform the upgrade or migration.
- To keep data synchronized between Contact Center Manager Administration and Contact Center Server, you must back up and restore Contact Center Manager Administration data and your Contact Center Manager Server data at the same time to ensure proper functionality in your contact center. If the Contact Center Manager Server files change infrequently, you can back up only the Contact Center Manager Administration data. In a co-resident environment, when you perform a full backup of Contact Center Manager Server, you back up the entire server, including Contact Center Manager Administration. This ensures that the data between the two applications is always synchronized. However, whenever you perform a partial backup of Contact Center Manager Server, you must also perform a backup of Contact Center Manager Administration. Furthermore, you must store both backups in the same location. See the *Contact Center Manager Server Installation and Maintenance Guide*.

Having current backup data is essential:

- to revert back to a previous version of the software, if necessary, following an upgrade
- to migrate Contact Center Manager Administration data to a new server
- to roll back erroneous data
- to recover from catastrophic events (such as data loss and damage due to disk failures and power outages)

You also can back up and restore the Security Framework in the same method as you use to back up the Contact Center Manager Administration server.

Prerequisites

- Install Contact Center Manager Administration. See the *Nortel Contact Center Installation Guide*.

- Commission Contact Center Manager Administration. See the *Nortel Contact Center Commissioning Guide*.

Navigation

- Backing up Contact Center Manager Administration (page 179)
- Backing up Security Framework (page 184)
- Viewing scheduled tasks in the Nortel Backup and Restore utility (page 187)
- Recording Real-Time Reporting and Emergency Help configurations (page 188)
- Restoring Contact Center Manager Administration data (page 189)
- Restoring Security Framework data (page 191)
- Switching to the standby server in Agent Desktop Display (page 192)

Backing up Contact Center Manager Administration

Back up the Contact Center Manager Administration data files to save a single file that is a snapshot of selected Contact Center Manager Administration files. Save the backup file to a predefined location on the same server or on another server in the same domain.

The Backup and Restore utility is automatically installed on the Contact Center Manager Administration server when you install the Contact Center Manager Administration software.

You can use this utility to back up the files located in the following folders (C is the drive on which you installed Contact Center Manager Administration):

- ADAM-specific data stored in the following folders:
  C:\Program Files\Microsoft ADAM\
  C:\Windows\ADAM
- Historical reporting template files (both imported and custom) and Audit Trail event logs stored in the following folders:
  C:\Nortel\Contact Center\Manager Administration\Apps\Reporting\
  C:\Nortel\Contact Center\Manager Administration\Apps\Common\
- The Report Creation Wizard database files stored in the following folder:
  C:\Nortel\Contact Center\Manager Administration\Server\RCW\Data
- A record of displays for real-time reporting exported to the following folder:
  C:\Nortel\Contact Center\Manager Administration\Apps\Reporting\

- An index file for Custom Report Groups stored in the following folder: C:\Nortel\Contact Center\Manager Administration\Apps\AccessMgt\
- A record of displays for Emergency Help exported to the following folder: C:\Nortel\Contact Center\Manager Administration\Apps\EmergencyHelp\

The file Backup.bks lists all the individual files that you need to back up. This file is created when you run the utility and is in the following location:

C:\Nortel\Contact Center\Manager Administration\Apps\SupportUtil\

When you back up the files with this utility, the system creates a single file that you can then use to restore the individual files. By default, this file is called Restore.bkf and is in the same folder.

Prerequisites

- Map a drive to the server in the domain where you want to back up ADAM.
- Ensure that you have write privileges on the server where you want to back up ADAM.
- Ensure that you have a user name and password configured with administrative privileges on the server where you want to back up ADAM.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, click **Start, All Programs, Nortel, Contact Center, Manager Administration, Configuration**.
2	In the left pane of the Configuration window, expand **Nortel**, **Applications**.
3	In the **Nortel Applications Configuration** window, select **Backup & Restore**.
4	In the right-hand pane, click **Backup & Restore**.
5	In the **Contact Center Manager Administration - Backup and Restore** utility, select the **Backup** tab.
6	In the **Backup** window, select **File**.
7	Accept or change the location of the backup file, Restore.bkf.
8	From the **Archive Backup Files Every** list, select the number of backup files to keep in the backup location.
9	To save the backup file to a tape drive, select **Tape**, indicate the Media Pool name of the tape drive, and click **Start, Control Panel, Administrative Tools, Computer Management, Storage, Removable Storage, Media Pool, Backup**. The Media Pool name is listed in Backup folder. In the **Media**

Pool box, type the Media Pool name of the tape drive. The Media Pool name must match the Media Pool name in the backup folder.

10 Click **Next**.

11 On the **Schedule** page, select an option to schedule the backups.

12 Define the backup schedule, and then click **Next**.

13 In the **Username** box on the **User Account with Administrative Privileges** page, type a valid administrator user name.

14 In the **Password** box, type a valid administrator password.

15 If you selected a backup location on another server in a domain, from the **Domain** list, select the domain. The default option is **this computer** (for example, the Contact Center Manager Administration server on which you are logged).

16 Click **Finish**.

17 Click **Close**.

--End--

Variable definitions

Variable	Value
Archive Backup Files Every	You can keep 2 to 10 backups, or all backups. This provides the flexibility to retain only the most recent backups, to save space in your backup location.
Backup file name	This is the file that the utility creates when you back up the Contact Center Manager Administration files. The file contains a snapshot of all Contact Center Manager Administration files that you back up. To change the default name or location of this file, click Browse, navigate to the location in which you want to store the file, and type a new file name. Nortel recommends that you change the name of the backup file from Restore.bkf to CCMA_7_[SUxx]_Restore.bkf where [SUxx] is replaced with the last SU or SUS installed. You can save the file to another server in the same domain as the Contact Center Manager Administration server. To select a file location on another server in the domain, you must map a drive to that server and you must have read/write privileges on that server.
Schedule definition	You can schedule a task only on the last day of the month that contains the least number of days. For example, if you want the backup to run every month, then you can schedule it to occur on day 28 only. However, if you clear February from the schedule, then the last day of a monthly schedule is 30. If you clear April, June, September, and November from the schedule, then the last day of a monthly schedule is 31.

Variable	Value
Schedule options	The time interval for scheduled backups. This can be • Daily (to schedule recurring backups once a day) • Weekly (to schedule recurring backups once a week) • Monthly (to schedule recurring backups once a month) • One Time Only (to schedule a one-time-only backup at a time in the future) • Run Now (to back up files immediately after you enter a valid username and password)
Username and Password	You must configure a user name and password with administrative privileges on the server to which you back up.

Procedure job aid

Data files stored on Contact Center servers

Contact Center server	Data files stored on server	Business consequence of CCMA server failure
Contact Center Manager Administration server	Schedule information for historical reports Partitions, access classes, report groups, and the Contact Center Manager Administration users Real-time display configuration data and real-time display filters Private historical reports Contact Center Management scheduled assignment information	If the Contact Center Manager Administration server fails, your supervisors and administrators cannot access the Contact Center Manager Administration application. Therefore, access to real-time displays, agent desktop display, schedule information for historical reports, and all data stored on in the application is interrupted.
Contact Center Manager Server	Agents, supervisors, skillsets and all their related assignments (accessed through Contact Center Management) CDNs, DNISs and all other data items (accessed through the Configuration component)	If your stand-alone Contact Center Manager Administration server fails, calls continue to be routed according to your defined scripts and your contact center can still receive calls because all user and agent assignments, CDNs, and DNISs are stored on the Contact Center Manager Server.

Backing up Security Framework

Back up the Security Framework data files to save a single file that is a snapshot of the Security Framework files. Save the backup file to a predefined location on the same server or on another server in the same domain.

The Backup and Restore utility for the Security Framework is automatically installed on the server when you install the Security Framework software.

When you back up the files with this utility, the system creates a single file that you can then use to restore the individual files. By default, this file is called Restore.bkf and is in the same folder.

Prerequisites

- Map a drive to the server in the domain where you want to back up Security Framework.
- Ensure that the Nortel JBoss and Nortel Common Network Directory services are running.
- Ensure that you have a user name and password configured with administrative privileges on the server where you want to back up Security Framework.

Procedure steps

Step	Action
1	On the Security Framework server, click **Start, All Programs, Nortel, Contact Center, Security Framework, Backup and Restore**.
2	In the **Security Framework - Backup and Restore** utility, select the **Backup** tab.
3	In the **Backup** window, select **File**.
4	Accept or change the location of the backup file, Restore.bkf.
5	From the **Archive Backup Files Every** list, select the number of backup files to keep in the backup location.
6	To save the backup file to a tape drive, select **Tape**, indicate the Media Pool name of the tape drive, and click **Start, Control Panel, Administrative Tools, Computer Management, Storage, Removable Storage, Media Pool, Backup**. The Media Pool name is listed in Backup folder. In the **Media Pool** box, type the Media Pool name of the tape drive. The Media Pool name must match the Media Pool name in the backup folder.
7	Click **Next**.
8	On the **Schedule** page, select an option to schedule the backups.
9	Define the backup schedule, and then click **Next**.
10	In the **Username** box on the **User Account with Administrative Privileges** page, type a valid administrator user name.
11	In the **Password** box, type a valid administrator password.
12	If you selected a backup location on another server in a domain, from the **Domain** list, select the domain.
13	Click **Finish**.
14	Click **Close**.

--End--

Variable definitions

Variable	Value
Archive Backup Files Every	You can keep 2 to 10 backups, or all backups. This provides the flexibility to retain only the most recent backups, to save space in your backup location.
Backup file name	This is the file that the utility creates when you back up the files. The file contains a snapshot of all Security Framework files that you back up. To change the default name or location of this file, click Browse, navigate to the location in which you want to store the file, and type a new file name. Nortel recommends that you change the name of the backup file from Restore.bkf to SF_7_[SUxx]_Restore.bkf where [SUxx] is replaced with the last SU or SUS installed. To select a file location on another server in the domain, you must map a drive to that server and you must have read/write privileges on that server.
Schedule definition	You can schedule a task only on the last day of the month that contains the least number of days. For example, if you want the backup to run every month, then you can schedule it to occur on day 28 only. However, if you clear February from the schedule, then the last day of a monthly schedule is 30. If you clear April, June, September, and November from the schedule, then the last day of a monthly schedule is 31.

Variable	Value
Schedule options	The time interval for scheduled backups. This can be • Daily (to schedule recurring backups once a day) • Weekly (to schedule recurring backups once a week) • Monthly (to schedule recurring backups once a month) • One Time Only (to schedule a one-time-only backup at a time in the future) • Run Now (to back up files immediately after you enter a valid username and password)
Username and Password	You must configure a user name and password with administrative privileges on the server to which you back up.

Viewing scheduled tasks in the Nortel Backup and Restore utility

Use the Nortel Backup and Restore utility to view scheduled tasks, including the task status or scheduled run time, to review or delete scheduled tasks.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, click **Start, All Programs, Nortel, Contact Center, Manager Administration, Configuration**.
2	In the left pane of the **Nortel Configuration** window, expand **Nortel** and **Administration**.
3	In the **Nortel Applications Configuration** window, click **Backup & Restore**.
4	In the right-hand pane, click **Backup & Restore**.
5	On the **Nortel Backup and Restore** utility, select the **View Scheduled Tasks** tab to display a list of scheduled tasks including the status and the next scheduled run time of each task.
6	To view the details of a task, highlight a task, and click **View Details** to display a detailed log file of your task.

7	To delete a task, highlight a task and click **Delete Task**.
8	On the confirmation box, click **Yes** to delete the task.
9	Click **Close**.

--End--

Recording Real-Time Reporting and Emergency Help configurations

Record the Real-Time Reporting configuration settings (IP Send and IP Receive Addresses) and the Emergency Help configuration settings whenever these settings change (for example, after you install or upgrade Contact Center Manager Administration).

Because these settings change infrequently and you cannot back them up using backup procedures, you must manually reconfigure the settings during a restoration.

Procedure steps

Step	Action
1	Click **Start, All Programs, Nortel, Contact Center, Manager Administration, Configuration**.
2	In the left pane of the Configuration window, select the **Real-Time Reporting** folder.
3	In the right pane, select the **RTR Registry Settings** icon.
4	Record all settings in the **RTR Registry Settings** dialog box.
5	Close the **RTR Registry Settings** dialog box.
6	In the left pane of the **Configuration** window, select the **Emergency Help** folder.
7	In the right pane, select the **Emergency Help Registry Settings** icon.
8	Record all settings in the **Emergency Help Properties** dialog box.
9	Close all windows to complete the procedure.

--End--

Restoring Contact Center Manager Administration data

Restore Contact Center Manager Administration data in the following situations:

- if you recover from a Contact Center Manager Administration server hardware failure when Contact Center Manager Server data is being restored.
- if you move to a replicating server as a result of a failure on your primary Contact Center Manager Administration server.
- if you revert the Contact Center Manager Administration software to a previous version. You must restore data to the same version of Contact Center Manager Administration as you backed up.
- if you lose data or make an error while entering Contact Center Manager Administration data and you need a previous version of the data (Contact Center Manager Administration data is all data excluding configuration data, scripts, and agents and supervisors).
- if you migrate Contact Center Manager Administration data to a new server.

When you back up Contact Center Manager Administration data with the Nortel Backup and Restore utility, it creates a single file with the default name of Restore.bkf. If you need to restore the Contact Center Manager Administration data to the original state when you backed up the files, you can start the utility and navigate to this file.

Use the Nortel Backup and Restore utility to restore the series of specified Contact Center Manager Administration files that you backed up with this utility.

Prerequisites

- Restore data that was backed up from the same release and version of the software as is currently installed on the Contact Center Manager Administration server. For example, if your Contact Center Manager Administration server currently contains Contact Center Manager Administration Release 7.0, then you can only restore a backup of Release 7.0 data to this server.
- Do not attempt to restore data from previous Service Updates. If you restore data backed up on previous versions, you corrupt your server.
- Restore no ADAM-specific data if you restore data on a server on which ADAM replication is enabled or you overwrite the replicated data. Ensure that you clear the following two files—C:\Program Files\Microsoft ADAM\SymposiumWC\ and C:\WINDOWS\ADAM—either before you backed up your data or before you restore your data.

- Retain the permission properties of the ADAM data directory and ADAM files if you restore these files (for example, you must retain permissions such as NETWORK SERVICE). If you do not maintain permission properties, the SymposiumWC service does not start.
- Restore the Contact Center Manager Administration data whenever you restore the Contact Center Manager Server data to prevent synchronization issues.
- The restore automatically reactivates scheduled events on the server.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, click **Start, All Programs, Nortel, Contact Center, Manager Administration, Configuration**.
2	In the left pane of the **Nortel Configuration** window, expand **Nortel** and **Administration**.
3	In the **Nortel Applications Configuration** window, click **Backup & Restore**.
4	On the **Contact Center Manager Administration - Backup and Restore** utility, click the **Restore** tab.
5	Click **Restore Files**.
6	Use the **Backup and Restore Wizard**, click **Next**. **OR** On the **Windows Backup** utility, click the **Restore and Manage Media** tab.
7	Click the **Restore and Manage Media** tab.
8	In the left pane, select the most recent backup file (or the file containing the data to restore).
9	Expand the file.
10	Select the check box for each file to restore. To select all the files, select the check box beside the parent file name.
11	Ensure you select the option to always replace the files on the computer.
12	Ensure that Original location appears in the **Restore files to** list.
13	Click **Start Restore**.
14	Update the URL that refers to the Contact Center Manager Administration server on all client PCs.
15	If your registry settings are unchanged, skip to step step 25. **OR**

If you restore to a new server, or if your registry settings are corrupted or overwritten, continue to step step 16 to manually reconfigure your Real-Time Reporting and Emergency Help configuration settings and to ensure these settings are the same as they were before the restore.

16 Click **Start, All Programs, Nortel, Contact Center, Manager Administration, Configuration**.

17 In the left pane of the Configuration window, click on the **Real-Time Reporting** folder.

18 In the right pane, click the **RTR Registry Settings** icon.

19 In the **RTR Registry Settings** dialog box, reenter all settings that you recorded for the Real-Time Reporting and Emergency Help configurations.

20 Click **OK**.

21 In the left pane of the Configuration window, click on the **Emergency Help** folder.

22 In the right pane, click on the **Emergency Help Registry Settings** icon.

23 In the **Emergency Help Properties** dialog box, reenter all settings that you noted when you backed up the Real-Time Reporting and Emergency Help configurations.

24 Click **OK**.

25 Restore the Security Framework if it is installed co-resident with Contact Center Manager Administration.

--End--

Restoring Security Framework data

Restore Security Framework data in the following situations:

- if you recover from a server hardware failure.
- if you lose data or need a previous version of the data.
- if you migrate data to a new server.

Prerequisites

- Restore data that was backed up from the same release and version of the software as is currently installed on the server.
- Do not attempt to restore data from previous Service Updates. If you restore data backed up on previous versions, you corrupt your server.

Procedure steps

Step	Action
1	On the Security Framework server, click **Start, All Programs, Nortel, Contact Center, Security Framework, Backup and Restore**.
2	In the **Security Framework - Backup and Restore** utility, select the **Restore** tab.
3	Click **Restore Files**.
4	Use the **Backup and Restore Wizard**, click **Next**.
	OR
	On the **Windows Backup** utility, click the **Restore and Manage Media** tab.
5	Click the **Restore and Manage Media** tab.
6	In the left pane, select the most recent backup file (or the file containing the data to restore).
7	Expand the file.
8	Select the check box for each file to restore. To select all the files, select the check box beside the parent file name.
9	Ensure you select the option to always replace the files on the computer.
10	Ensure that Original location appears in the **Restore files to** list.
11	Click **Start Restore**.
12	Choose **Start**, **All Programs**, **Nortel**, **Contact Center**, **Security Framework**, **Security Settings**.
13	Select **Restart Security Framework**.
14	Click **Close**.

--End--

Switching to the standby server in Agent Desktop Display

Switch to the standby server in Agent Desktop Display if the primary server fails, if you have a replicating server installed, and if you configured your Agent Desktop Display with IP addresses for standby servers.

The IP addresses of the standby server are configured when you installed and configured Agent Desktop Display on the client.

Procedure steps

Step	Action
1	On each agent workstation, click **Start, All Programs, Agent Desktop Displays, Server IP Addresses Configuration**.
2	In the **Server Configuration** dialog box, select the standby server.

--End--

Active Directory Application Mode replication

Active Directory Application Mode (ADAM) is a Microsoft information storage framework that runs as a non operating system service.

Replication means that you share the data stored in one ADAM instance with another ADAM instance, to ensure that the replicated data is the same across both servers. If the active Contact Center Manager Administration server fails, a replicating server provides immediate access to all data files stored in ADAM from the primary server. Contact Center Manager Administration users can use replication to immediately point their browser to the standby Contact Center Manager Administration server to maintain a level of productivity with minimal interruption of access to the Contact Center Manager Administration application.

While you may have access to multiple ADAM instances and multiple Contact Center Manager Administration-specific ADAM instances, each Contact Center Manager Administration server can have only one Contact Center Manager Administration-specific ADAM instance. To maintain the integrity of your Contact Center Manager Administration data, you can replicate a Contact Center Manager Administration-specific ADAM instance only with one or more other Contact Center Manager Administration-specific instances of ADAM.

ADAM replication is not a replacement for scheduling regular backups of your Contact Center Manager Administration data. For the following reasons, you must still schedule backups on your primary server even if you have a standby server installed with replication enabled:

- Not all Contact Center Manager Administration data files are replicated.
- You cannot use replication to roll back data to a specific point in time, which may be required.

For more information about ADAM, see the Microsoft Web site at www.microsoft.com.

After you install ADAM on the Contact Center Manager Administration server, to consult the ADAM online Help, click Start, All Programs, ADAM, ADAM Help.

To monitor Active Directory replication issues, you can use the Active Directory Replication Monitor (ReplMon.exe). The Active Directory Replication Monitor is a graphical user interface tool that is included with Windows Server 2003 Support Tools. You can use the Active Directory Replication Monitor to view the status of Active Directory replication, verify replication topology, force synchronization between domain controllers, and monitor the status and performance of domain controller replication.

Navigation

Setting up ADAM replication

You can set up ADAM replication so that if the active Contact Center Manager Administration server fails, a replicating server can provide immediate access to all data files stored in ADAM from the primary server.

Prerequisites

- Ensure that you enable replication during the install. You cannot enable replication after you install ADAM.
- Ensure that you install only one instance of ADAM on a Contact Center Manager Administration server.
- Ensure that you install both instances of Contact Center Manager Administration before you point a Contact Center Manager Administration server ADAM instance to another Contact Center Manager Administration server ADAM instance.
- Ensure that you point the secondary server ADAM instance to the primary server ADAM instance during the install of the secondary server; you cannot do this after you install the secondary server.
- Ensure that you do not install ADAM on a server that is a domain controller.

- Before you install the first instance of ADAM with replication, ensure that you note the environment into which you install it.
- Before you replicate an existing instance of ADAM, ensure that you note both the environment into which you install the replica instance and the type of service account chosen for the original instance. Your choices for the replica instance depend on the Windows domain into which the original ADAM was installed, and on the service account chosen for the original ADAM instance.

Procedure steps

Step	Action
1	Install the Contact Center Manager Administration server software on the primary server without replication.
2	On the secondary server, log on to the domain as the administrator or as a user with administrative privileges.
3	On the secondary server, install the Contact Center Manager Administration server software with replication.
4	While you install the Contact Center Manager Administration server software with replication on the secondary server, point the secondary server ADAM instance to the primary server ADAM instance.

--End--

Procedure job aid

If you replicate ADAM during your Contact Center Manager Administration installation, only certain Contact Center Manager Administration data files are copied between replicated servers.

The following list of information is exchanged between servers, so that if it changes on one server, it is replicated to the other servers within the same domain:

- access classes
- partitions
- private and graphical real-time reports
- real-time report filters

However, not all Contact Center Manager Administration data is stored in ADAM, and therefore cannot be replicated. If a server fails, you must use backup files to restore the following files to the standby server, because the data is not replicated using ADAM:

- scheduling data for Contact Center Management assignments
- scheduling data for historical reports
- historical report output files
- user-created historical reports that are imported into Contact Center Manager Administration
- real-time report exported files
- Emergency Help exported files
- Report Creation Wizard user-created formulas (stored in the file RCW.mdb)
- Report Creation Wizard user-created reports and report definitions

Choosing ADAM service accounts

Choose a service account after you install ADAM on the Contact Center Manager Administration server, because ADAM runs as a service. The type of ADAM service account that you can choose during the ADAM installation depends on the Windows workgroup or domain environment into which you install ADAM, and whether this is the first instance that you install on your network or if you replicate an existing instance.

By default, ADAM is always installed as a network service account, unless you manually change the service account settings to domain user or workstation user.

Prerequisites

- Know the Windows workgroup or domain environment into which you installed ADAM.
- Know the service account chosen for the original instance of ADAM, if you are replicating an existing instance of ADAM.

Procedure steps

Step	Action
1	After you install ADAM, and based on the environment into which you installed ADAM, choose the appropriate ADAM service account.

--End--

Procedure job aid

ADAM service account options

Domain context	Service account (primary server)	Service account (secondary server)	Default replication authentication method
Windows Server 2000 domain OR Windows Server 2003 domain or forest	Network service	Network service or Domain user	Negotiated
	Workstation user	Workstation user	Negotiated pass-through
	Domain user	Network service or Domain user	Negotiated
Windows NT 4.0 domain	Workstation user	Workstation user	Negotiated pass-through
	Domain user	Domain user	Negotiated

Stopping replication on replicating servers

Stop ADAM replication on all replicating servers.

Procedure steps

Step	Action
1	Click **Start, Run**.
2	In the text box, type **cmd**.
3	Click **OK**.

4 Navigate to the ADAM directory, for example, C:\Windows\ADAM.

5 To disable outbound replication, type **repadmin /options +DISABLE_OUTBOUND_REPL**.

6 Press **Enter**.

7 Close all windows.

--End--

Starting replication on replicating servers

Start ADAM replication on all replicating servers.

Procedure steps

Step **Action**

1 Click **Start, Run**.

2 In the text box, type **cmd**.

3 Click **OK**.

4 Navigate to the ADAM directory, for example, C:\Windows\ADAM.

5 To enable outbound replication, type **repadmin /options -DISABLE_OUTBOUND_REPL**.

6 Press **Enter**.

7 Close all windows.

--End--

Contact Center Manager Administration failure recovery

If the Contact Center Manager Administration server hardware fails, you must restore your backup data quickly.

You can only configure Unified Communication Management (UCM) users on the primary security server. If your system security is managed by the backup Security Framework server, then you cannot make any changes to a user account.

When the primary server fails, a secondary server can take over managing the data. Contact Center allows a replication server that maintains duplicate data for the primary server. Your secondary server can use backup of the Contact Center Manager Administration data, or if you are using a replication server, the data on the replication server.

After the failure is resolved, you can go back to use the primary server or use another server to manage the data and revert to the original primary-secondary server configuration.

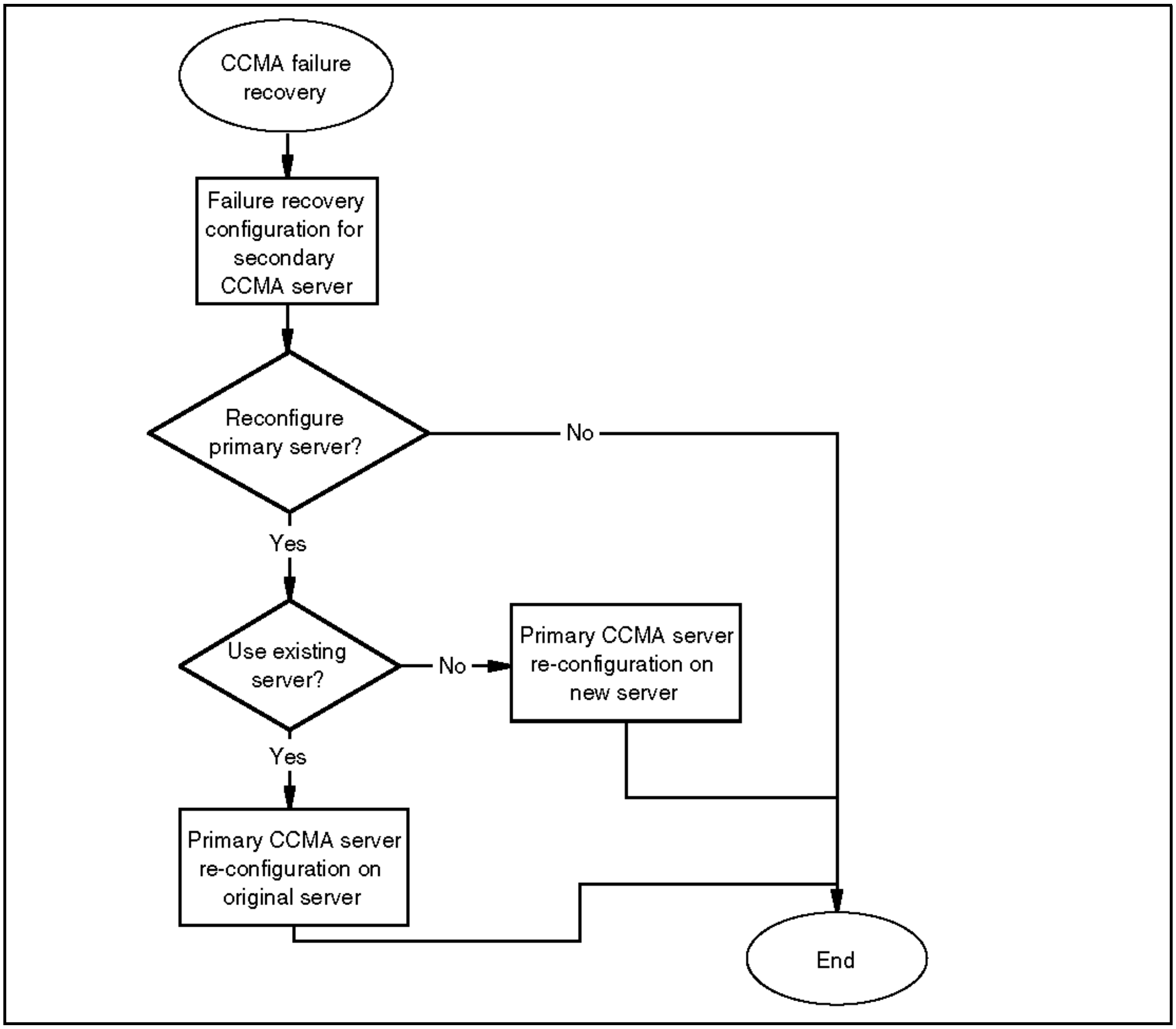
Prerequisites for Contact Center Manager Administration failure recovery

- If you do not have a replicating server in your network, ensure that you backup data using your current release of Contact Center Manager Administration software frequently.
- If you update the Contact Center Manager Administration software using service updates or service packs, backup the data after you update the CCMA software.

Contact Center Manager Administration server failure recovery tasks

This work flow shows you the sequence of procedures you perform to recover the operation of your contact center after a Contact Center Manager Administration server failure. It also includes the optional steps to restore your servers to the initial configuration.

Contact Center Manager Administration failure recovery tasks


CCMA failure recovery
Failure recovery configuration for secondary CCMA server
Reconfigure primary server?
No
Yes
Use existing server?
No
Primary CCMA server re-configuration on new server
Yes
Primary CCMA server re-configuration on original server
End

Contact Center Manager Administration failure recovery navigation

- Failure recovery configuration for secondary CCMA server (page 201)
- Primary CCMA server re-configuration on original server (page 205)
- Primary CCMA server re-configuration on new server (page 209)

Failure recovery configuration for secondary CCMA server

When the primary server fails (for example, a hardware failure), a secondary Contact Center Manager Administration server performs the data management to run your contact center.

Generally, the secondary server is engaged one of three ways:

- If you have a replicating server in your network, the replicating server automatically restores the latest data files on your secondary server Your contact center may be down for a short time.
- If you do not have a replicating server in your network, but can use the existing server, restore the data from your latest backups and continue the contact center activities. Your contact center may be down for a short time.
- If you do not have a replicating server in your network, and cannot reuse the existing hardware, install software and restore the data from your latest backups. Your contact center may be down for a considerable length of time.

For each failure recovery, you must perform some manual steps as described in this section to configure the applications that connect to your Contact Center Manager Administration server.

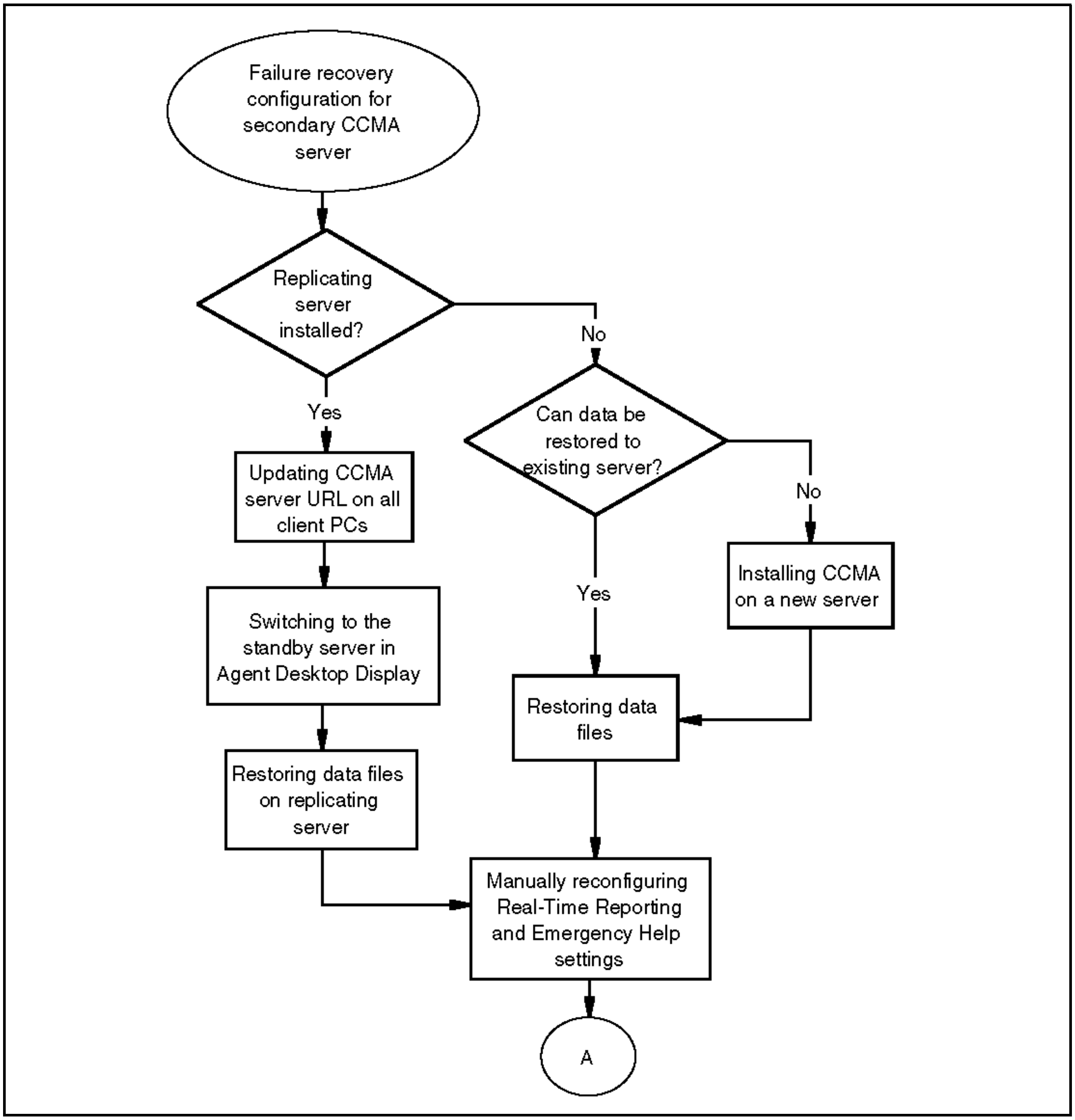
Prerequisites for failure recovery configuration for secondary Contact Center Manager Administration server

- Back up your Contact Center Manager Administration server data.
- Ensure that the data you want to restore was backed up using the same release and version of the software you are using on the secondary server. For example, if your Contact Center Manager Administration server currently contains Contact Center Manager Administration Release 7.0 patch SU03, then you can restore only a backup of Release 7.0 SU03 data onto the secondary server.
- If you are using a replication server, do not restore ADAM-specific data. if you restore data on a server on which ADAM replication is enabled, you overwrite the replicated data.
  Clear the following two files—C:\Program Files\Microsoft ADAM\SymposiumWC\ and C:\WINDOWS\ADAM—before you restore your data.
- Retain the permission properties of the ADAM data directory and ADAM files if you restore these files (for example, you must retain permissions such as NETWORK SERVICE). If you do not maintain permission properties, the SymposiumWC service does not start.

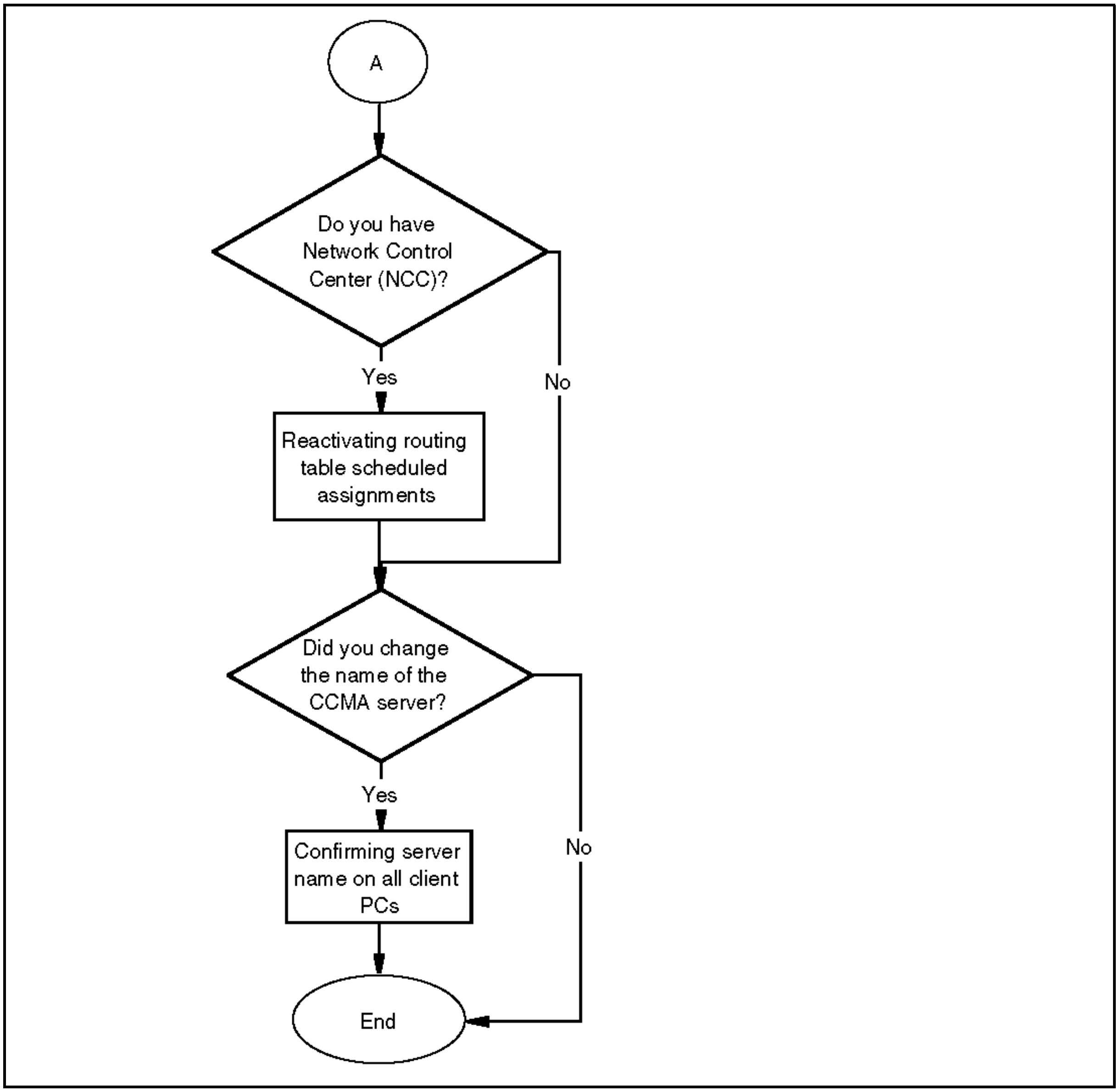
Failure recovery configuration for secondary CCMA server procedures

This task flow shows you the sequence of procedures you perform to configure the secondary server after a Contact Center Manager Administration server failure, with and without a replicating server in your system.

Failure recovery configuration for secondary CCMA server procedures


Failure recovery configuration for secondary CCMA server
Replicating server installed?
No
Yes
Can data be restored to existing server?
No
Yes
Updating CCMA server URL on all client PCs
Switching to the standby server in Agent Desktop Display
Restoring data files on replicating server
Installing CCMA on a new server
Restoring data files
Manually reconfiguring Real-Time Reporting and Emergency Help settings
A

Failure recovery configuration for secondary CCMA server procedures (continued)


A
Do you have Network Control Center (NCC)?
Yes
No
Reactivating routing table scheduled assignments
Did you change the name of the CCMA server?
Yes
No
Confirming server name on all client PCs
End

Failure recovery configuration for secondary CCMA server navigation

- Updating CCMA server URL on all client PCs
- Switching to the standby server in Agent Desktop Display
- Restoring data files on replicating server (*Nortel Contact Center Upgrade and Patches* (NN44400-410))
- Installing CCMA on a new server (*Nortel Contact Center Installation* (NN44400-311))

- Restoring data files (*Nortel Contact Center Upgrade and Patches* (NN44400-410))
- Recording Real-Time Reporting and Emergency Help configurations (page 188)
- Reactivating routing table scheduled assignments
- Confirming server name on all client PCs

Job aid: Functionality after CCMA server failure recovery

After a Contact Center Manager Administration server failure, with replication enabled, all information in ADAM is replicated to the secondary server. This enables operation of the contact center to continue.

Many functions are maintained and are immediately available from the replicating server. However, some Contact Center Manager Administration information is held in flat files or databases outside ADAM. To enable all features in Contact Center Manager Administration, you must manually restore the files from Nortel\Contact Center\Manager Administration on the primary server to the replicating server.

Primary CCMA server re-configuration on original server

When the secondary server is engaged in managing data, you can resolve the failure of the primary server and restore the Contact Center Manager Administration data management to the original primary server.

If you cannot reuse the original primary server, you can install the Contact Center Manager Administration server software on a new server and restore your data. For more information, see Primary CCMA server re-configuration on new server (page 209).

For each configuration, you must perform some manual steps as described in this section to configure the applications that connect to your Contact Center Manager Administration server.

Prerequisites for primary CCMA server re-configuration on original server

- Back up your Contact Center Manager Administration server data.
- Ensure that the data you want to restore was backed up using the same release and version of the software you are using on the secondary server. For example, if your Contact Center Manager Administration server currently contains Contact Center Manager Administration Release 7.0 patch SU03, then you can restore only a backup of Release 7.0 SU03 data onto the secondary server.
- If you are using a replication server, do not restore ADAM-specific data. if you restore data on a server on which ADAM replication is enabled, you overwrite the replicated data.

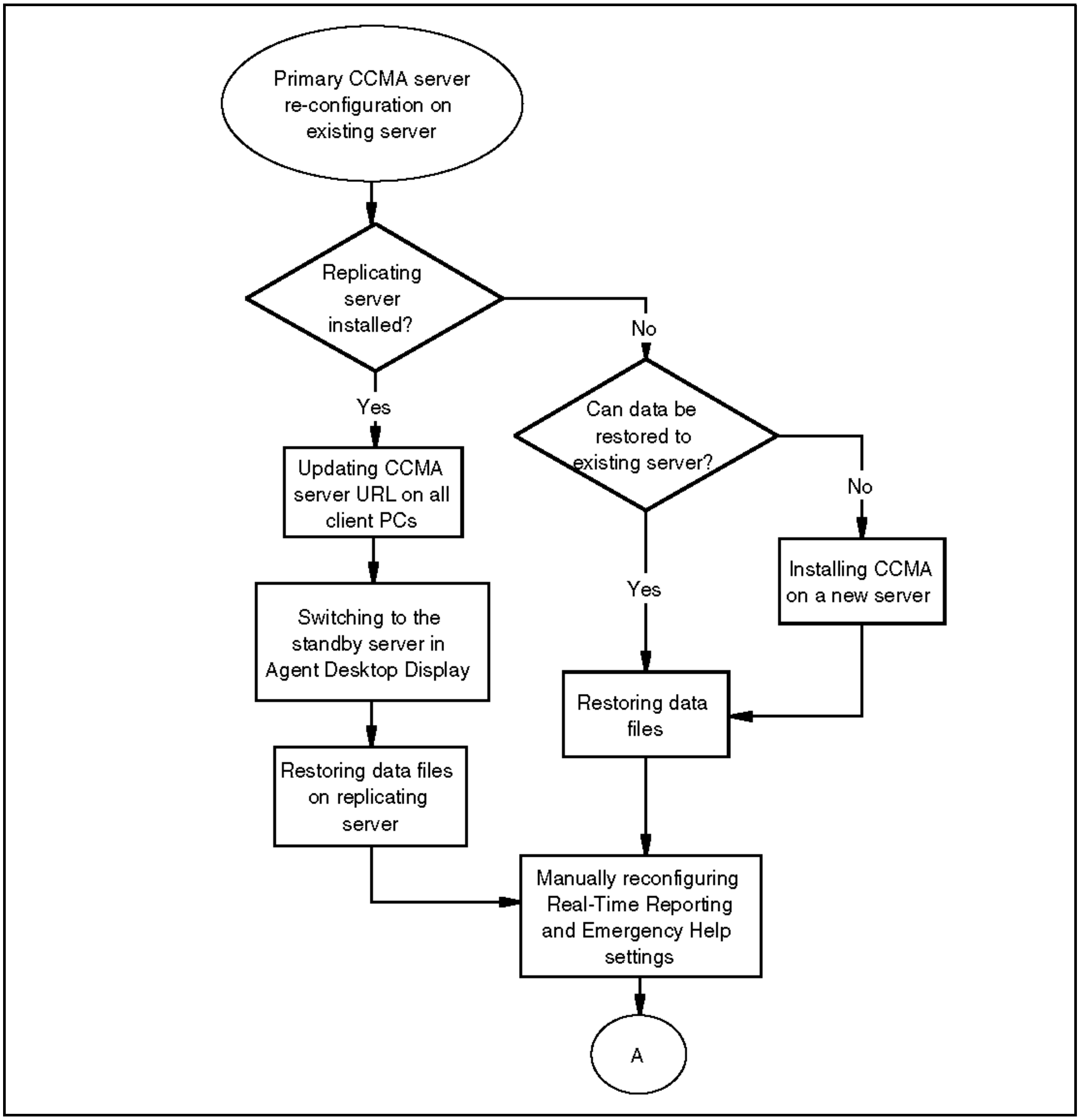
Clear the following two files—C:\Program Files\Microsoft ADAM\SymposiumWC\ and C:\WINDOWS\ADAM—before you restore your data.

- Retain the permission properties of the ADAM data directory and ADAM files if you restore these files (for example, you must retain permissions such as NETWORK SERVICE). If you do not maintain permission properties, the SymposiumWC service does not start.

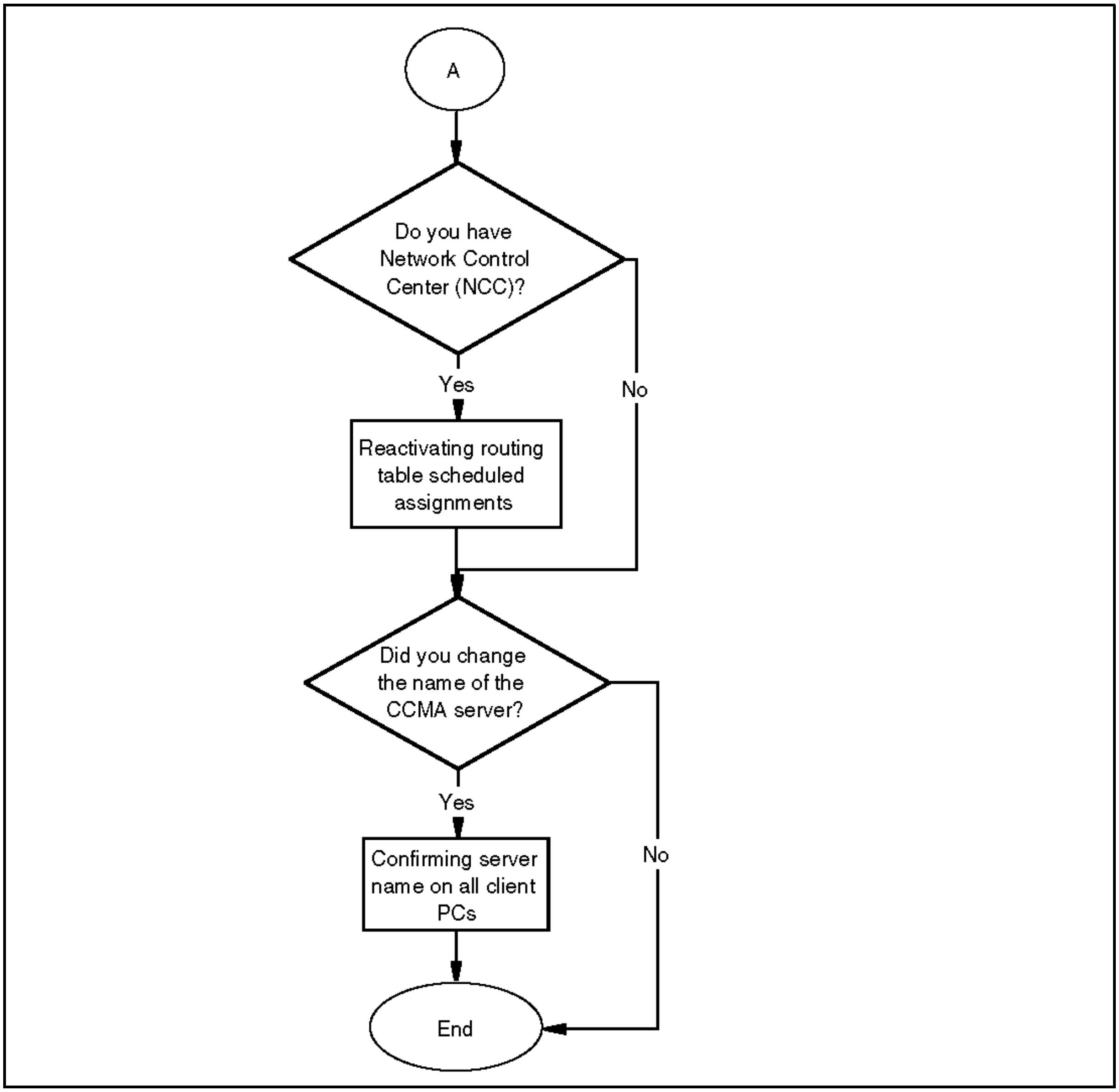
Primary CCMA server re-configuration on original server procedures

This task flow shows you the sequence of procedures you perform to reconfigure the original primary server after a Contact Center Manager Administration server failure, with and without a replicating server in your system.

Primary CCMA server re-configuration on original server procedures


Primary CCMA server re-configuration on existing server
Replicating server installed?
No
Yes
Can data be restored to existing server?
No
Updating CCMA server URL on all client PCs
Yes
Installing CCMA on a new server
Switching to the standby server in Agent Desktop Display
Restoring data files
Restoring data files on replicating server
Manually reconfiguring Real-Time Reporting and Emergency Help settings
A

Primary CCMA server re-configuration on original server procedures (continued)


A
Do you have Network Control Center (NCC)?
Yes
No
Reactivating routing table scheduled assignments
Did you change the name of the CCMA server?
Yes
No
Confirming server name on all client PCs
End

Primary CCMA server re-configuration on original server navigation

- Updating CCMA server URL on all client PCs
- Switching to the standby server in Agent Desktop Display
- Restoring data files on replicating server (*Nortel Contact Center Upgrade and Patches* (NN44400-410))
- Installing CCMA on a new server (*Nortel Contact Center Installation* (NN44400-311))

- Restoring data files (*Nortel Contact Center Upgrade and Patches* (NN44400-410))
- Recording Real-Time Reporting and Emergency Help configurations (page 188)
- Reactivating routing table scheduled assignments
- Confirming server name on all client PCs

Job aid: Primary CCMA server re-configuration on original server

After a Contact Center Manager Administration server failure, with replication enabled, all information in ADAM is replicated to the secondary server. This enables operation of the contact center to continue.

Many functions are maintained and are immediately available from the replicating server. However, some Contact Center Manager Administration information is held in flat files or databases outside ADAM. To enable all features in Contact Center Manager Administration, you must manually restore the files from Nortel\Contact Center\Manager Administration on the primary server to the replicating server.

Primary CCMA server re-configuration on new server

When the secondary server is engaged in managing data, you can resolve the failure of the primary server and restore the Contact Center Manager Administration data management to the original primary server. If you cannot reuse the original primary server, you can install the Contact Center Manager Administration server software on a new server and restore your data.

For each configuration, you must perform some manual steps as described in this section to configure the applications that connect to your Contact Center Manager Administration server.

Prerequisites for primary CCMA server re-configuration on new server

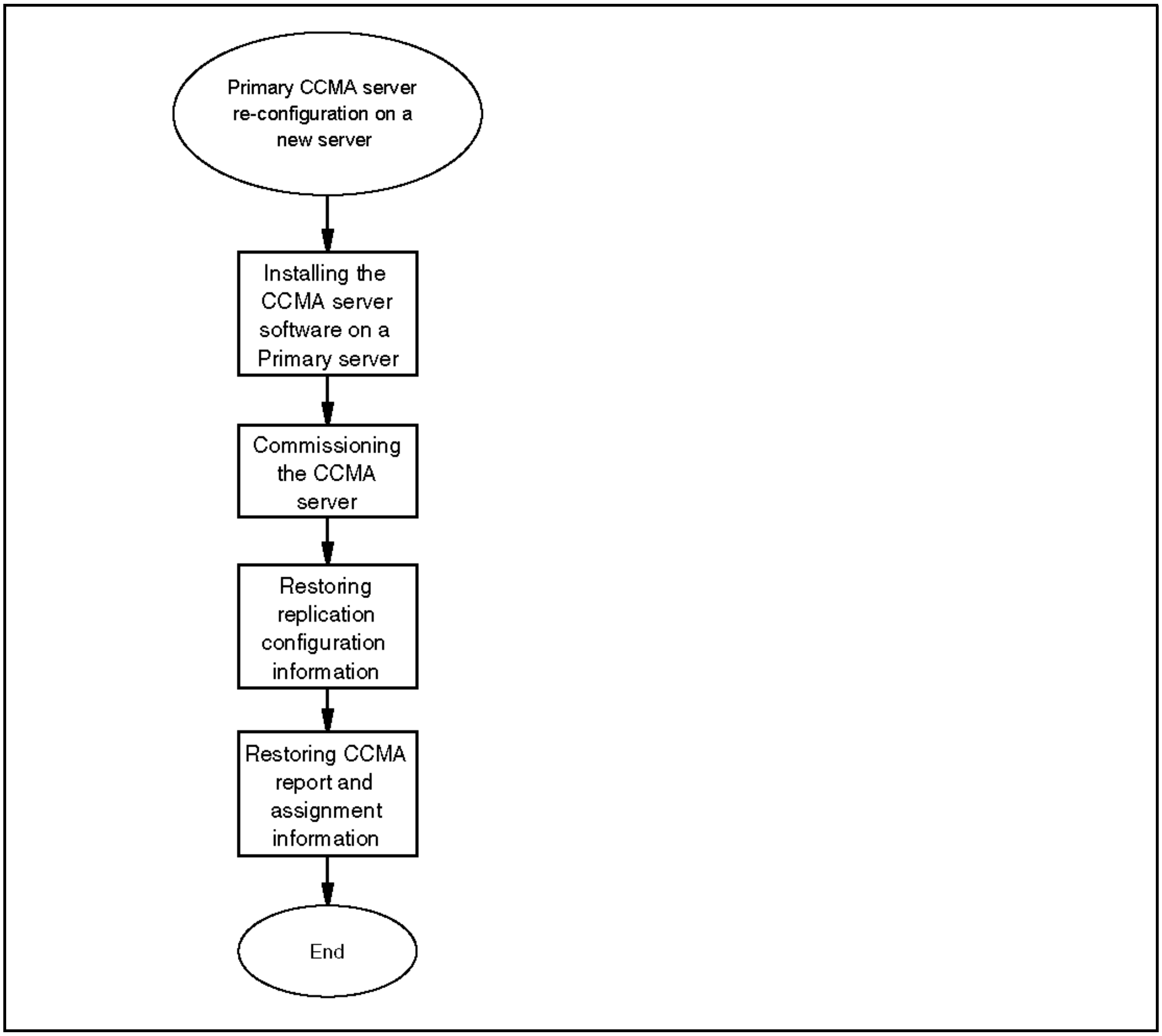
- Back up your Contact Center Manager Administration server data on the secondary server.
- Ensure that you have a CCMA backup of the primary server available for restoring the replication configuration details.
- Know the IP address or host name and domain configuration for the original primary CCMA server to replace it with the new server.
- Ensure that the data you want to restore was backed up using the same release and version of the software you are using on the secondary server. For example, if your Contact Center Manager Administration server currently contains Contact Center Manager Administration Release 7.0 patch SU03, then you can restore only a backup of Release 7.0 SU03 data onto the secondary server.

- If you are using a replication server, do not restore ADAM-specific data. if you restore data on a server on which ADAM replication is enabled, you overwrite the replicated data.
  Clear the following two files—C:\Program Files\Microsoft ADAM\SymposiumWC\ and C:\WINDOWS\ADAM—before you restore your data.
- Retain the permission properties of the ADAM data directory and ADAM files if you restore these files (for example, you must retain permissions such as NETWORK SERVICE).

Primary CCMA server re-configuration on new server procedures

This task flow shows you the sequence of procedures you perform to reconfigure a new primary server after a Contact Center Manager Administration server failure.

Primary CCMA server re-configuration on new server procedures



Primary CCMA server re-configuration on a new server
Installing the CCMA server software on a Primary server
Commissioning the CCMA server
Restoring replication configuration information
Restoring CCMA report and assignment information
End

Primary CCMA server re-configuration on new server navigation

- Installing CCMA on a new server (*Nortel Contact Center Installation* (NN44400-311))
- Commissioning the CCMA server (*Nortel Contact Center Commissioning* (NN44400-312))
- Restoring replication configuration information (page 212)
- Restoring CCMA report and assignment information (page 213)

Job aid: Primary CCMA server re-configuration on new server

After a Contact Center Manager Administration server failure, with replication enabled, all information in ADAM is replicated to the secondary server. This enables operation of the contact center to continue.

Many functions are maintained and are immediately available from the replicating server. However, some Contact Center Manager Administration information is held in flat files or databases outside ADAM. To enable all features in Contact Center Manager Administration, you must manually restore the files from Nortel\Contact Center\Manager Administration on the primary server to the replicating server.

Restoring replication configuration information

Restore the replication configuration information from a backup of the old primary Contact Center Manager Administration server to allow the replication server to synchronize the data between the new primary and secondary servers.

Prerequisites

- Ensure that you have a back up of data from the CCMA Primary server.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Manager Administration**, **Configuration**.
2	In the left pane of the Nortel Configuration window, expand **Nortel**, **Applications**, **Backup & Restore**.
3	In the right pane, click **Backup & Restore**.
4	In the **Contact Center Manager Administration - Backup And Restore** dialog box, click the **Restore** tab.
5	Click **Restore Files**.
6	In the **Welcome to the Backup or Restore Wizard** dialog box, click **Next**.
7	In the **Backup or Restore** dialog box, select **Restore files and settings**.
8	Click **Next**.
9	In the **What to Restore** dialog box, in the left pane, select **Program Files**, **Microsoft ADAM**, **instance1**, **data**. Expand each folder fully by clicking the plus sign (+) beside it.
10	In the right pane, select **Microsoft ADAM**.
11	Click **Next**.
12	In the **Completing the Backup or Restore Wizard** dialog box, click **Advanced**.

13 In the **Where to Restore** dialog box, from the **Restore files to** list, select **Original location**.

14 Click **Next**.

15 In the **How to Restore** dialog box, select **Replace existing files**.

16 Click **Next**.

17 Click **Finish**.

--End--

Restoring CCMA report and assignment information

Restore the CCMA report and assignment information to ensure the settings are the same as they were previously, both on the original primary server, and on the recent secondary server.

Prerequisites

- Ensure that you have a back up of data from the Secondary CCMA server.

Procedure steps

Step **Action**

1 On the Contact Center Manager Administration server, click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Manager Administration**, **Configuration**.

2 In the left pane of the Nortel Configuration window, expand **Nortel**, **Applications**, **Backup & Restore**.

3 In the right pane, click **Backup & Restore**.

4 In the **Contact Center Manager Administration - Backup And Restore** dialog box, click the **Restore** tab.

5 Click **Restore Files**.

6 In the **Welcome to the Backup or Restore Wizard** dialog box, click **Next**.

7 In the **Backup or Restore** dialog box, select **Restore files and settings**.

8 Click **Next**.

9 In the **What to Restore** dialog box, in the left pane, select **Nortel**, **Contact Center**. Expand each folder fully by clicking the plus sign (+) beside it.

10 In the right pane, select **Nortel**.

11 Click **Next**.

12 In the **Completing the Backup or Restore Wizard** dialog box, click **Advanced**.

13 In the **Where to Restore** dialog box, from the **Restore files to** list, select **Original location**.

14 Click **Next**.

15 In the **How to Restore** dialog box, select **Replace existing files**.

16 Click **Next**.

17 Click **Finish**.

--End--

Language support fundamentals

This chapter provides background information for Language support. If you want to use English across all platforms, you can ignore this chapter.

Contact Center Manager Administration supports the following languages:

- English
- French
- German
- Japanese
- Traditional Chinese
- Simplified Chinese
- Russian

Attention: To install and configure the software for the Contact Center Manager Administration server in languages other than English, you must ensure that the server is free of all English operating system components. Otherwise, you encounter functionality problems in this server.

You can install a language pack to access translated Historical Reporting templates, Online Help, and various other files that are required to work in the language you choose.

Navigation

- Language levels (page 215)
- Language family compatibility (page 216)
- Co-resident servers compatibility (page 217)

Language levels

Contact Center Manager Administration supports two levels of language environment:

- international environment

- international and local environment

International environment

In the international environment, the graphic user interface, the online Help, and all reports are in English. However, you can enter user information that contains non-ASCII characters (such as agent and supervisor names). Also, you can manage date and time formats from a different regional time zone.

International and local environment

In the combined international and local environment, the graphic user interface, the online Help, and all reports are translated into one of the eight supported languages: French, Simplified Chinese, German, Spanish, Japanese, Traditional Chinese, Russian, and Brazilian Portuguese. Also, you can enter user information that contains non-ASCII characters and you can use date and time formats from a different regional time zone.

In this environment, you must install the language pack on the Contact Center Manager Administration server. If you use Contact Center Manager Administration server as a client PC, you must change the language preferences in Internet Explorer.

Language family compatibility

For Contact Center Manager Administration to function properly, the language family of the operating systems must be compatible across all platforms in the network. If the language versions of the operating systems on the Contact Center Manager server, Contact Center Manager Administration server, and the client PC belong to the same language family, the platforms can coexist on the same network. This compatibility is useful if your contact center supports multiple languages.

The character sets for English are included in all language families. Contact Center Manager Administration recognizes the following language families:

- Latin I
- Japanese
- Traditional Chinese
- Simplified Chinese
- Russian

Latin I includes all Western European languages that use the Latin 1 character set. French and German belong to the Latin I language family. Agents in the contact center can view Contact Center Manager Administration in English, French, German, Spanish and Brazilian Portuguese. For Latin 1 language family and co-resident servers compatibility, see Co-resident servers compatibility (page 217).

If you use the Japanese language family, users in the same contact center can view Contact Center Manager Administration in English or Japanese. If you use the Traditional Chinese language family, users in the same contact center can view Contact Center Manager Administration in English or Traditional Chinese.

Co-resident servers compatibility

If your Contact Center Manager Administration co-resides with other Contact Center 7.0 applications, Contact Center supports the eight languages specified above.

Language support configuration

For Contact Center Manager Administration to support languages other than English, you must configure language support. You must ensure that the language versions of the operating systems for all platforms are compatible. See Language support fundamentals (page 215).

Navigation

- Editing the locales.dat file (page 218)
- Configuring the Windows regional settings (page 219)
- Configuring the language preferences in Internet Explorer (page 220)

Editing the locales.dat file

You can configure the language family character set by editing the locales.dat file. This file controls the character set used for communication between the Contact Center Manager Administration and the Contact Center Manager Server. To edit the locales.dat file, use the utility that comes with Contact Center Manager Administration, stored on the Contact Center Manager Administration server.

If your Contact Center Manager Administration server software is installed on a co-resident system, you do not have to edit the locales.dat file. The locales.dat file is updated at installation time.

Prerequisites

- Ensure the client PC and agent workstations are installed.
- Ensure that you know the location of Sybase Open Client Version12.5.
- Log on to Contact Center Administration server.

Procedure steps

Step	Action
1	Click **Start**, **All programs**, **Internet Explorer**.
2	In the **Address** box, enter http://<localhost>/locales.asp.
3	Next to the **File Path** box, click **Browse** to navigate to the **<SYBASE>\locales\locales.dat** file.
4	In the **Language Option** list, select **Latin 1**, **Japanese**, **Simplified Chinese, Traditional Chinese** or **Russian**.
5	Click **Set Locale** to save your changes.

--End--

Variable definitions

Variable	Value
<localhost>	Name or IP address of the Contact Center Manager Administration server
<SYBASE>	Directory location of the Sybase Open Client 12.5, installed on the Contact Center Manager Administration server

Configuring the Windows regional settings

On an English operating system, configure the Windows regional settings to use the Latin 1, Japanese, Simplified Chinese, Traditional Chinese or Russian versions of Contact Center Manager Administration. You must change the Regional Settings on the Contact Center Manager Administration server.

Prerequisites

- Log on to Contact Center Manager Administration server.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, click **Start**, **Control Panel**, **Regional and Language Options**.

2	Double-click **Regional and Language Options**.
3	On the **Regional and Language Options** dialog box, click the **Languages** tab.
4	In the **Languages** dialog box, select the **Install files for East Asian languages** check box.
5	On the **Regional and Language Options** dialog box, click the **Regional Options** tab.
6	On the **Regional Options** dialog box, from the list in the **Standards and formats** section, select **Chinese (Taiwan)** or **Japanese 6**.
7	Click **OK**.

--End--

Configuring the language preferences in Internet Explorer

The language preference settings on the client PC browse determines the language in which an application appears. You must perform this procedure on each client PC that connects to Contact Center Manager Administration server.

Prerequisites

- Connect to Contact Center Manager Administration server as a client.
- Configure the client.

Procedure steps

Step	Action
1	Click **Start**, **Control Panel**.
2	Double-click **Internet Options**.
3	In the **Internet Options** dialog box, click **Languages**.
4	In the **Language Preference** dialog box, click **Add**.
5	In the **Language** list, select the required language
6	In the **Add Language** dialog box, click **OK**.
7	In the **Language Preference** dialog box, click the required language.
8	Click **Move Up** until the language appears at the top of the list.
9	In the **Language Preference** dialog box, click **OK**.

10 In the **Internet Options** dialog box, click **OK**.

--End--

Security Framework configuration

The Security Framework provides an identify management security framework that enables integration with the customer directory services infrastructure (for example Active Directory) for authentication and authorization of a user. The Security Framework helps reduce the administrative costs and eliminates the redundant user information associated with each application.

The procedures in this chapter are optional configuration steps to enable security certificates or to disable the Security Framework in Contact Center. Key procedures to configure the Security Framework are in *Nortel Contact Center Commissioning* (NN44400-312).

If you plan to use the Security Framework for your Contact Center, Nortel recommends that you do not use the Contact Center Manager Administration security.

For information about supported languages, see *Nortel Contact Center Planning and Engineering* (NN44400-210), Language support fundamentals (page 215), and Language support configuration (page 218).

Prerequisites to Security Framework configuration

- Install the Security Framework. For more information, see *Nortel Contact Center Installation* (NN44400-311).
- Commission the Security Framework. For more information, see *Nortel Contact Center Commissioning* (NN44400-312).

Navigation

- Obtaining a server certificate from the Security Framework (page 223)
- Obtaining a server certificate from a third-party authority (page 224)
- Installing a server certificate (page 225)
- Configuring the Contact Center Manager Administration security details (page 226)
- Disabling the Security Framework (page 227)

- Saving the root certificate authority to a file (page 228)
- Importing the root certificate authority to Internet Explorer (page 228)
- Configuring security prompts in Internet Explorer (page 229)
- Viewing the security server settings (page 231)

Obtaining a server certificate from the Security Framework

Obtain a server certificate from the Security Framework. The Security Framework installs its own certification authority to use to sign a certificate request to secure the Contact Center Manager Administration Web site using an X.509 interface. You need this certificate to run Contact Center Manager Administration over a secure channel, such as HTTPS.

Once you create the certificate request using the Web Server Certificate Wizard this certificate must be signed before it is installed. This certificate can be signed using SFW Certificate Authority by using the Agent Certificate Configuration utility provided with the CCMA server.

If the request is successful, you receive a server certificate that you must install using the Web Server Certificate Wizard. For more information, see Installing a server certificate (page 225).

Prerequisites

- Install Internet Information Services Manager on the Contact Center Manager Administration server.
- Install and configure the Security Framework.

Procedure steps

Step	Action
1	Click **Start**, **Administrative Tools**, **Internet Information Services (IIS) Manager**.
2	Double-click the local computer, and then double-click the **Web Sites** folder.
3	Right-click the Web site or file for which you want to request a certificate, and then click **Properties**.
4	Click on the **Directory Security** tab if you selected a Web site **OR** Click on the **File Security** tab if you selected a file.

5 In the **Secure communications** group, click **Server Certificate**.

6 In the Web Server Certificate Wizard, follow the prompts to renew or create a new certificate.

7 Click **Prepare the request now, but send it later**.

8 Complete the remaining steps in the Web Server Certificate Wizard, and then click **Finish**.

9 On the CCMA server where you generated the certificate request, click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Manager Administration** to run the Client Certificate Management utility.

10 Type the fully qualified domain name of the SFW server to sign the certificate request.

11 Type a valid User ID and Password for this server.

12 Select the certificate request file created by the Web Server Certificate Wizard.

13 Click **Process Request**.

Two files are created in the folder from where you select the certificate request file. The ClientCertificate.cer file is the certificate file that you install on your Web server. The RootCACertificate.cer file is the root CA certificate file that you add to your Trusted Root Certification Authorities on each of your clients.

--End--

Obtaining a server certificate from a third-party authority

Obtain a server certificate from a third-party certification authority to secure the Contact Center Manager Administration Web site using an X.509 certificate. You need this certificate to run Contact Center Manager Administration over a secure channel, such as HTTPS.

After you request a server certificate from a third-party certification authority, the request is processed. If the request is successful, you receive a server certificate that you must install using the Web Server Certificate Wizard. For more information, see Installing a server certificate (page 225).

Prerequisites

- Install IIS Manager on the Contact Center Manager Administration server.

Procedure steps

Step	Action
1	Click **Start**, **Administrative Tools**, **Internet Information Services (IIS) Manager**.
2	Double-click the local computer, and then double-click the **Web Sites** folder.
3	Right-click the Web site or file for which you want to request a certificate, and then click **Properties**.
4	Click on the **Directory Security** tab if you selected a Web site **OR** Click on the **File Security** tab if you selected a file.
5	In the **Secure communications** group, click **Server Certificate**.
6	In the Web Server Certificate Wizard, follow the prompts to renew or create a new certificate.
7	Click **Prepare the request now, but send it later**.
8	Complete the remaining steps in the Web Server Certificate Wizard, and then click **Finish**.

--End--

Installing a server certificate

Install a server certificate after you request and receive a server certificate from a third-party certification authority. You need this certificate to run Contact Center Manager Administration over a secure channel, such as HTTPS.

Prerequisites

- Ensure that you received a server certificate. For more information, see Obtaining a server certificate from a third-party authority (page 224).

Procedure steps

Step	Action
1	Click **Start**, **Administrative Tools**, **Internet Information Services (IIS) Manager**.

2 Double-click the local computer, and then double-click the **Web Sites** folder.

3 Right-click the Web site or file for which you requested and received a certificate, and then click **Properties**.

4 Click on the **Directory Security** tab if you selected a Web site.

OR

Click on the **File Security** tab if you selected a file.

5 In the **Secure communications** group, click **Server Certificate**.

6 In the Web Server Certificate Wizard, click **Process Pending Request**.

7 Perform the remaining steps in the Web Server Certificate Wizard, and then click **Finish**.

--End--

Configuring the Contact Center Manager Administration security details

Configure the Contact Center Manager Administration security details to record the location and settings of your security server.

Prerequisites

- Install and configure your Contact Center Manager Administration security server.

Procedure steps

Step **Action**

1 From the **Start** menu, select **All Programs, Nortel, Contact Center, Manager Administration, Configuration, Security Settings**.

2 In the **Security Details** window, under **Configuration Setup**, select the option to indicate where your security server is installed.

3 In the **Contact Center Manager Administration (CCMA) Details** group, select the **Web Site Identifier** of the Contact Center Manager Administration Web site from the list.

4 Select your **CCMA Server Protcol**.

5 Select the **IIS Port Number** for the Contact Center Manager Administration server.

6 In the **Security Server Details** group, type the details of the Contact Center Manager Administration security server, including the FDQN, Protocol, and Port Number.

7 Click **Enable**.

A confirmation message appears indicating that the CCMA Security Details configuration of the security server was successful.

--End--

Variable definitions

Variable	Definition
Configuration Setup	The location of the installed security server: On this server (Co-resident with CCMA) or Other Server.
Web Site Identifier	A list of available Web site location identifiers.
CCMA Server Protocol	The security protocol of the CCMA server: http or https.
IIS Port Number	A list of available IIS port locations. The default is the location of the Contact Center Manager Administration server.
Security Server FQDN	The Fully Qualified Domain Name (FQDN) of the Contact Center Manager Administration security server, for example, server1.nortel.com.
Security Server Protocol	The security protocol of the Contact Center Manager Administration security server: http or https.
Security Server Port Number	The port number of the Contact Center Manager Administration security server, for example, 8443.

Disabling the Security Framework

Disable the Security Framework if you need to access the Contact Center Manager Administration server without the restriction of the security policies or to revert to the old Contact Center Manager log on method without the Security Framework.

Procedure steps

Step	Action
1	On the **Start** menu, click **All Programs, Nortel, Contact Center, Manager Administration, Configuration, Security Settings**.
2	In the Security Details window, click **Disable**.

--End--

Saving the root certificate authority to a file

Save the root certificate authority to a file that is accessible to the client so that you can import the security certificate to the browser.

Prerequisites

- Ensure that you have a server certificate. For more information, see Obtaining a server certificate from a third-party authority (page 224).

Procedure steps

Step	Action
1	Log on to the Unified Communication Management (UCM) utility using the Administrator account, with the **User ID** admin.
2	Under **Security**, click **Certificates**.
3	Click the **Private Certificate Authority** tab.
4	Click **Download** and then name and save the security certificate to a file.

--End--

Importing the root certificate authority to Internet Explorer

Import the root certificate authority to the browser to prevent Internet Explorer from displaying a Security Alert when you connect to the security server. You must add the Root CA certificate to Trusted Root Certification Authorities.

Prerequisites

- Install and configure your Contact Center Manager Administration security server.
- Save the security certificate to a file. For more information, see Saving the root certificate authority to a file (page 228).

Procedure steps

Step	Action
1	Open Internet Explorer.
2	Select **Tools, Internet Options**.
3	Click the **Content** tab.
4	Click **Certificates**.
5	In the **Certificates** window, click the **Trusted Root Certification Authorities** tab.
6	Click **Import**.
7	In the Certificate Import Wizard, perform the steps to import the security certificate for the Contact Center Manager Administration security server. Locate and select the certificate from the location where you saved the file and accept all other defaults in the Wizard.
8	Click **Finish**.
9	Restart your browser to apply the changes.

--End--

Configuring security prompts in Internet Explorer

Configure security prompts in the Internet Explorer browser to suppress warning messages that can appear when you access the security server URL.

Procedure steps

Step	Action
1	Open Internet Explorer.
2	Select **Tools, Internet Options**.

3 Click the **Security** tab.

4 Click **Trusted Sites**.

5 Click **Custom Level**.

6 In the Security Settings window, scroll through the list until you find the option **Don’t prompt for client certificate selection when no certificates or only one certificate exists**, and then click **Enable** for this setting.

7 Click **OK**.

8 Click **Yes** to confirm the change.

9 Click **OK**

10 Restart your browser to apply the changes.

--End--

Viewing the security server settings

Use the application to view the security framework (SFW) port settings, to enable or disable the enforcement of SSL between the Contact Center Manager Administration server and the security framework, or to restart the SFW service.

Do not change the port numbers for the SFW service.

Prerequisites

- If you want to enforce SSL between the CCMA and SFW server, ensure that you have a certificate installed on the CCMA Web server.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration security server.
2	From the **Start** menu, select **All Programs**, **Nortel**, **Contact Center**, **Security Framework**, **Security Server Settings**.
3	In the **Security Settings** dialog box, select the **Enforce secure channel (SSL) communications** check box if you want to enforce SSL between the CCMA and SFW server.
4	Select the **Restart Security Service** check box.
5	Click **Update**.
6	Confirm changes by accepting any warning messages that appear.
7	Click **Close**.

--End--

Security Commissioning

User identity provisioning

Provision user identities to supply accounts that allow you to access the Contact Center server.

Navigation

Adding a local user identity and password

Add a local user identity and password to set up an administrator who is authenticated locally in Unified Communications Management (UCM).

Procedure steps

Step	Action
1	Log on to UCM as a security administrator.
2	In the navigation pane, click **User Services**, **Administrative Users**.
3	On the **Administrative Users** page, click **Add**.
4	On the **Add New Administrative User Step 1** page, in the **User ID** field, type a user ID.
5	In the **Authentication Type** section, click **Local**.
6	In the **Full Name** field, type the full name of the user.
7	In the **Temporary password** field, type a password for the user.
8	In the **Re-enter password** field, retype the password.
9	Click **Save** and **Continue**.
10	On the **Add New Administrative User Step 2** page, select one or more **Role Name** check boxes to assign roles to the new local user.

Step	Action
11	Click **Finish**.

--End--

Variable definitions

Variable	Value
Local	Specifies a user who is authenticated locally in Unified Communications Management (UCM).
Full Name	The user’s full name, including first and last name.
Re-enter password	Retype the temporary password.
Temporary Password	The temporary password required to connect to UCM.
User ID	A unique identifier used by an administrative user to log on to UCM. Valid values are 1 to 31 characters. Valid characters are a to z, A to Z, 0 to 9, - and _ .

Adding an external account (optional)

Add an external account to Unified Communications Management (UCM) to set up an administrator who is authenticated with external authentication. Contact Center performs external authentication through Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial In User Service (RADIUS), or Kerberos.

Prerequisites

- Provision an external server. For more information, see External identity repository configuration (page 247).

Procedure steps

Step	Action
1	Log on to UCM as a security administrator.
2	In the navigation pane, click **User Services**, **Administrative Users**.
3	On the **Administrative Users** page, click **Add**.
4	On the **Add New Administrative User Step 1** page, in the **User ID** field, type a user ID.

5 In the **Authentication Type** section, click **External**.

6 In the **Full Name** field, type the full name of the user.

7 Click **Save** and **Continue**.

8 On the **Add New Administrative User Step 2** page, select one or more **Role Name** check boxes to assign roles to the new external user.

9 Click **Finish**.

--End--

Variable definitions

Variable	Value
External	Specifies a user who is authenticated externally. Contact Center performs external authentication through Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial In User Service (RADIUS), or Kerberos.
Full Name	The user’s full name, including first and last name.
User ID	A unique identifier used by an administrative user to log on to UCM. Valid values are 1 to 31 characters. Valid characters are a to z, A to Z, 0 to 9, - and _ .

Role creation and management

Create and manage roles to control user access to elements.

Navigation

- Creating a custom role (page 236)
- Deleting a custom role (optional) (page 237)

Creating a custom role

Create a role to control user access to elements.

You can assign roles to users. Each role defines the management functions a user can perform on an element.

Procedure steps

Step	Action
1	Log on to Unified Communications Management as a security administrator.
2	In the navigation pane, click **Security**, **Roles**.
3	On the **Roles** page, click **Add**.
4	On the **Add New Role Step 1** page, in the **Role Name** field, type a unique name for the role.
5	In the **Role Description** field, type a description for the role.
6	Click **Save** and **Continue**.
7	On the **Role Details** page, click **Save**.

--End--

Variable definitions

Variable	Value
Role Description	A description of the role. The description may be up to 500 characters long. Allowed characters are a-z, A-Z, 0-9, - and _.
Role Name	A unique name for the role. The name must be at least one character long. Allowed characters are a-z, A-Z, 0-9, - and _.

Deleting a custom role (optional)

Delete a role to remove custom roles from Unified Communications Management (UCM). You cannot delete built-in roles.

Prerequisites

- You must create a custom role.

Procedure steps

Step	Action
1	Log on to UCM as a security administrator.
2	In the navigation pane, click **Security**, **Roles**.
3	On the **Roles** page, select the check box next to the role you want to delete.
4	Click **Delete**.
5	On the **Delete Roles** page, click **Delete**.

--End--

Element and permission mapping

Map element permissions to a role to control which management functions a user with that role can perform on an element.

Navigation

- Mapping elements and permissions to a role (page 238)
- Mapping elements and permissions by copying from another role (page 239)
- Removing elements from a role (optional) (page 240)

Mapping elements and permissions to a role

Map elements and permissions to a role to control which management functions a user with that role can perform on an element.

Procedure steps

Step	Action
1	Log on to UCM as a security administrator.
2	In the navigation pane, click **Security**, **Roles**.
3	On the **Roles** page, in the **Role Name** column, click the name of the role to which you want to map elements.
4	On the **Role Details** page, on the **Element/Service Permission** tab, select the check boxes next to the elements for which you want to map permissions.
5	Click **Add Mapping**.
6	On the **Select Elements To Map to Role** page, in the **Element Name** list, select the element you want to map to the role.
7	Click **Next**.

8 On the **Permission Mapping** page, in the list next to each management function, select a permission setting (Deny, View, or Modify).

9 Optionally, select the **Allow use of Element Manager** check box.

10 Click **Save**.

--End--

Variable definitions

Variable	Value
Allow use of Element Manager	Select this check box to allow users with this role to use Element Manager.
Deny	Prevents users with the role from using the specified management function.
View	Allows users with the role to view but not modify the specified management function.
Modify	Allows users with the role to view and modify the specified management function.

Mapping elements and permissions by copying from another role

Copy element and permissions mapping from another role to assign the same access as an existing role.

Procedure steps

Step **Action**

1 Log on to UCM as a security administrator.

2 In the navigation pane, click **Security**, **Roles**.

3 On the **Roles** page, in the **Role Name** column, click the name of the role to which you want to map elements.

4 On the **Role Details** page, on the **Element/Service Permission** tab, select the check boxes next to the elements for which you want to map permissions.

5 Click **Copy All From**.

6 On the **Permission Mapping** page, in the **Copy from Role** list, select the role from which you want to copy permissions.

7	Click **Copy**.

--End--

Removing elements from a role (optional)

Remove elements from a role to remove access to that element for users with that role.

Procedure steps

Step	Action
1	Log on to UCM as a security administrator.
2	In the navigation pane, click **Security**, **Roles**.
3	On the **Roles** page, in the **Role Name** column, click the name of the role to which you want to map elements.
4	On the **Role Details** page, on the **Element/Service Permission** tab, select the check boxes next to the elements for which you want to map permissions.
5	Click **Delete Mapping**.
6	On the **Delete Mapping** page, click **Delete**.

--End--

Role mapping

Map roles and users to grant users the element permissions associated with a selected role.

Navigation

- Assigning roles to a user (page 241)
- Assigning users to a role (page 242)

Assigning roles to a user

Assign roles to a user to grant the user the element permissions associated with selected roles.

You can also assign roles to a user by copying them from another role. For information, see Mapping elements and permissions by copying from another role (page 239).

Procedure steps

Step	Action
1	Log on to UCM as a security administrator.
2	In the navigation pane, click User **Services**, **Administrative Users**.
3	On the **Administrative Users** page, click the User ID of the user for whom you want to assign a role.
4	On the **User Details** page, in the **Roles** pane, click **Select Roles**.
5	On the **User Roles** page, select the check boxes next to the roles that you want to assign to the user.
6	Click **Save**.

--End--

Assigning users to a role

Assign users to a role to grant users the element permissions associated with a selected role.

Procedure steps

Step	Action
1	Log on to UCM as a security administrator.
2	In the navigation pane, click **Security**, **Roles**.
3	On the **Roles** page, in the **Role Name** column, click the name of the role to which you want to assign users.
4	On the **Role Details** page, select the **Assigned Users** tab. The Role Details page refreshes with a list of users who are granted the permissions associated with the selected role.
5	Click **Select Users**.
6	On the **Assigned Users** page, select the check boxes next to the users for whom you want to add the permissions associated with the selected role.
7	Click **Save**.

--End--

Policy creation and management

Create and manage policies to enforce rules that help ensure security. In Unified Communications Management (UCM), security policies apply to passwords.

Navigation

- Creating a security policy for passwords (page 243)

Creating a security policy for passwords

Create a security policy for passwords to configure aging, history, strength, and lockout parameters for passwords used for locally authenticated users in UCM. Set your password policies according to your business requirements.

Procedure steps

Step	Action
1	Log on to Unified Communications Management as an administrator.
2	In the navigation pane, click **Security**, **Policies**.
3	On the **Policies** page, in the **Password Policy (for locally authenticated users)** pane, click **Edit**.
4	On the **Password Policy** page, select the **Aging** check box.
5	In the **Expiration period** field, type the number of maximum allowable days before the password expires.
6	In the **Expiration warning** field, type the number of days before a password expires to send a warning to a user.
7	In the **Minimum age** field, type the minimum allowable days for a password age.
8	Select the **History** check box.

9 In the **Previous passwords blocked** field, type the number of passwords to remember in history.

10 In the **Strength** section, in the **Minimum Total Length** field, type the minimum number of characters required for a password.

11 In the **Minimum by character Type** section, in the **Lower case** field, type the minimum number of lower case characters required for a password.

12 In the **Upper case** field, type the minimum number of upper case characters required for a password.

13 In the **Numeric case** field, type the minimum number of numeric characters required for a password.

14 In the **Special case** field, type the minimum number of special characters required for a password.

15 Select the **Lockout** check box.

16 In the **Consecutive Invalid Login Attempts** field, type the maximum number of failed logon attempts before the system locks out a user.

17 In the **Interval for Consecutive Invalid Login Attempts** field, type the number of seconds allowed for consecutive invalid logon attempts before the system locks out the user.

18 In the **Lockout Time** field, type the number of minutes an account can remain unused before the system locks it.

19 Click **Save**.

--End--

Variable definitions

Variable	Value
Consecutive Invalid Login Attempts	The maximum number of failed logon attempts before the system locks out a user. The maximum number of failed login attempts must be at least one.
Expiration period	The number of maximum allowable days before the password expires. Valid values are 1 to 365 days. The user is forced to change the password after the threshold for the password expires and before the threshold to disable the account. The password is locked until it is reset by the security administrator.

Variable	Value
Expiration warning	The number of days before a password expires to send a warning to a user. Valid values are 1 to 15 days. The user receives a password expiration warning when the password is about to expire and before the password expires.
Interval for Consecutive Invalid Login Attempts	The number of minutes allowed for consecutive invalid logon attempts before the system locks out the user. Valid values are 0 or more minutes.
Lockout Time	The number of minutes an account can remain unused before the system locks it. Valid values are 0 or more minutes.
Lower case	The minimum number of lower case characters required for a password. The minimum number of lower case characters cannot exceed the minimum total length. Enter a value of 0 to indicate that passwords do not require a minimum number of lower case characters.
Minimum age	The minimum allowable days for a password age. A minimum age prevents password recycling that could otherwise defeat the history policy. Valid values are 0 to 7 days. The user's new password is rejected when the current password has not reached the minimum password duration.
Minimum Total Length	The minimum number of characters required for a password. The minimum total length must be at least 6 characters.
Numeric case	The minimum number of numeric case characters required for a password. The minimum number of numeric case characters cannot exceed the minimum total length. Enter a value of 0 to indicate that passwords do not require a minimum number of numeric case characters.
Previous passwords blocked	The number of passwords to remember in history. Valid values are 1 to 99 previous passwords.

Variable	Value
Special case	The minimum number of special case characters required for a password. An example of a special character is an exclamation mark (!). The minimum number of special case characters cannot exceed the minimum total length. Enter a value of 0 to indicate that passwords do not require a minimum number of special case characters.
Upper case	The minimum number of upper case characters required for a password. The minimum number of upper case characters cannot exceed the minimum total length. Enter a value of 0 to indicate that passwords do not require a minimum number of upper case characters.

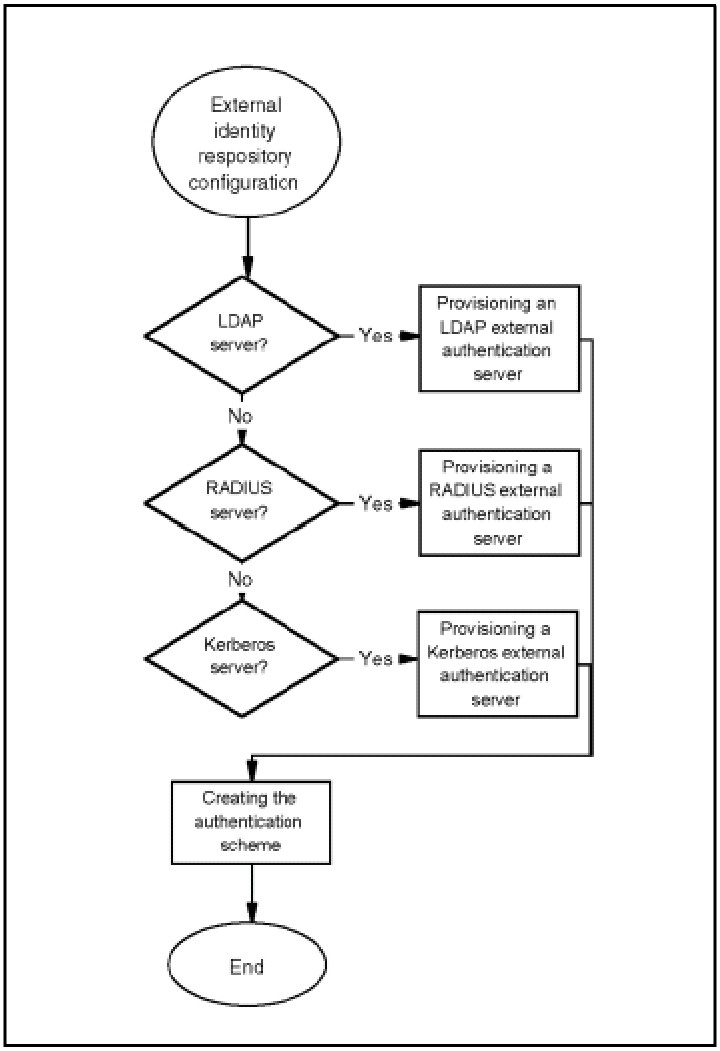
External identity repository configuration

Configure external identity repositories to enable external authentication for Contact Center.

External identity repository configuration procedures

The following task flow shows the order of procedures you perform to configure external identity repositories on Unified Communications Management (UCM). To link to any procedure, go to External identity repository configuration navigation (page 248).

External identity repository configuration procedures


External identity respository configuration
LDAP server?
Yes
Provisioning an LDAP external authentication server
No
RADIUS server?
Yes
Provisioning a RADIUS external authentication server
No
Kerberos server?
Yes
Provisioning a Kerberos external authentication server
Creating the authentication scheme
End

External identity repository configuration navigation

- Provisioning an LDAP authentication server (page 249)
- Installing the LDAP server certificate onto Quantum (page 250) (if required)
- Provisioning a RADIUS authentication server (page 251)
- Provisioning a Kerberos authentication server (page 252)
- Creating an authentication scheme (page 253)

Attention: Support for Security Framework fail-over is not available for Kerberos and RADIUS authentication.

Provisioning an LDAP authentication server

Provision a Lightweight Directory Access Protocol (LDAP) authentication server to enable external authentication for Contact Center LDAP.

Procedure steps

Step	Action
1	Log on to Unified Communications Management as a security administrator.
2	In the navigation pane, click **User Services, External Authentication**
3	On the **External Identity Repositories** page, in the **Authentication Servers** pane, click **Configure**.
4	On the **Authentication Servers** page, select the **Provision LDAP Server** check box.
5	In the **Provision LDAP Server** pane, in the **IP (or DNS)** field, type the IP or DNS for the server.
6	In the **TCP Port** field, type the TCP port.
7	In the **Base Distinguished Name** field, type the base distinguished name.
8	Optionally, select the **SSL/TLS Mode** check box.
9	Optionally, select the **Is Active Directory** check box.
10	In the **Distinguished Name for Root Binding** field, type a distinguished name for root binding.
11	In the **Password for Root Binding** field, type a password.
12	Click **Save**.

Attention: After you provision an LDAP authentication server, an external user account is automatically added to Element Manager. This new user account is based on the information you typed in the Distinguished Name for Root Binding field, which refers to a pre-existing Windows log on account.

--End--

Variable definitions

Variable	Value
Base Distinguished Name	Path of the root node in the directory server from which the system can start searching for users.
Distinguished Name for Root Binding	Path of the node in the directory server pointing to a user with administrator rights; this node binds to the LDAP server during the authentication process.
IP (or DNS)	IP address or DNS of the LDAP server.
Is Active Directory	Select this check box if the LDAP server is a Windows server with Active Directory installed on it.
Password for Root Binding	The password of the administrative user who is identified through the distinguished name for root binding field.
SSL/TLS Mode	Select this check box if the communication is carried out through a secure protocol like SSL.
TCP Port	Port for network communication with the LDAP server; the standard port is 389, but 3268 may also be used in the context of the global catalog.

Installing the LDAP server certificate onto Quantum

If the LDAP server is using secure sockets layer (SSL) security, install the certificate for the LDAP server as a trusted item in the Quantum list.

Procedure steps

Step	Action
1	In the Unified Communications Management application, open the Certificate Management page.
2	Under Certificate Authorities, click **Add**.
3	In the **Friendly Name** box, type a name for the certificate.
4	Ensure that your certificate meets the criteria for the Certificate Authority (CA).
5	Click **Submit**.

--End--

Provisioning a RADIUS authentication server

Provision a Remote Authentication Dial In User Service (RADIUS) authentication server to enable external authentication for Contact Center using RADIUS.

Procedure steps

Step	Action
1	Log on to Unified Communications Management as a security administrator.
2	In the navigation pane, click **User Service, External Authentication**.
3	On the **External Identity Repositories** page, in the **Authentication Servers** pane, click Configure.
4	On the **Authentication Servers** page, select the Provision Radius Server check box.
5	In the **Provision Radius Server** pane, in the **IP (or DNS)** field, type the IP or DNS for the server.
6	In the **UDP Port** field, type the UDP port number.
7	In the **Shared Secret** field, type a shared secret.
8	Click **Save**.

--End--

Variable definitions

Variable	Value
IP (or DNS)	IP address or DNS of the RADIUS server.
Shared Secret	A password that is shared between the RADIUS server and clients. The administrator configures the shared secret the first time the RADIUS server is configured.
UDP Port	The port for network communication with the RADIUS server. The standard port is 1812.

Provisioning a Kerberos authentication server

Provision a Kerberos authentication server to enable external authentication for Contact Center using the Kerberos computer network authentication protocol.

When Kerberos is configured, only SSO is enabled with the browser. Kerberos also allows you to remain authenticated if the session management values (max session or max idle time) expire. These features do not apply to SCE. In SCE, if the session values expire, you must re-authenticate through Contact Center Manager Administration (CCMA), and then log on to SCE.

Procedure steps

Step	Action
1	Log on to Unified Communications Management as a security administrator.
2	In the navigation pane, click **User Services, External Authentication**.
3	On the **External Identity Repositories** page, in the **Authentication Servers** pane, click **Configure**.
4	On the **Authentication Servers** page, select the **Provision Kerberos Server** check box.
5	In the **Provision Kerberos Server** pane, in the **DC Host Name (FQDN)** field, type the fully qualified domain name (FQDN) for the Kerberos server.
6	In the **DC Computer Domain** field, type the domain name of the Kerberos server.
7	In the **Keytab File** field, type the absolute path of the keytab file on the UCM server. **OR**

Click **Browse** to browse to the keytab file on the UCM server.

8 Click **Save**.

--End--

Variable definitions

Variable	Value
DC Computer Domain	The domain name of the Kerberos server. For example, tommy1.tommy.net. A Kerberos server is a Domain Controller machine implementing the Kerberos authentication protocol. A Domain Controller machine (DC) is a Windows 2003 server with an Active Directory (AD) installed on it, that is some form of repository containing information about miscellaneous entities on the network, such as user accounts or printers.
DC Host Name (FQDN)	The fully qualified domain name for the Kerberos server. For example, CCMATMDEV2tommy1.tommy.net.
Keytab File	An encrypted copy of the Kerberos server's key. This file is generated on the Kerberos server and then copied to the UCM server.

Creating an authentication scheme

Create an authentication scheme to define the order of the authentication servers that Contact Center should use to authenticate users.

Prerequisites

- Configure at least one external authentication server.

Procedure steps

Step	Action
1	Log on to Unified Communications Management as a security administrator.
2	In the navigation pane, click **User Services, External Authentication**.
3	On the **External Identity Repositories** page, in the **Authentication Scheme** pane, click **Edit**.

4 On the **Authentication Scheme** page, select the option that represents the order of the authentication servers that Contact Center should use to authenticate users.

Attention: The number of options on the Authentication Scheme page depends on the number of external authentication servers in your system.

5 Click **Save**.

--End--

Element Management

If you are authenticated locally in Unified Communications Management (UCM), you must follow the following procedures to manage elements in the UCM application.

The following procedures are optional if you are authenticated through the Security Framework.

Navigation

Adding a new Contact Center application (Optional)

Add a new application to allow UCM to control which users can access an application.

Prerequisites

- Ensure you obtain the Uniform Resource Locator (URL) of the server.

Procedure steps

Step	Action
1	Log on to Unified Communications Management as a security administrator.
2	In the navigation pane, choose **Network, Elements**.
3	On the **Elements** page, click **Add**.
4	On the **Add New Element Step 1** page, in the **Name** field, type a name for the element.
5	Optionally, in the **Description** field, type a description for the element.
6	In the **Type** list, select **Contact Center**.

Attention: The Type list is dynamic, based on the type of elements in your system. Depending on your system configuration, you may see options in addition to the Contact Center option.

Step	Action
7	Click **Next**.
8	On the **Add New Element Step 2** page, in the **Server Address** field, type the URL of the server.
9	Click **Save**.

--End--

Variable definitions

Variable	Value
Description	A description for the element.
Name	A unique identifier for the element. The name can include 1 to 32 characters in length.
Release	The software release of the new element.
Server Address	The IP address and port of the new element. Use the following format: https://<FQDN of MAS>:8443

Editing a secured element (optional)

Edit an element to change the properties and role-permission mapping.

Prerequisites

- Add an element. For more information, see Adding a new Contact Center application (Optional) (page 256).

Procedure steps

Step	Action
1	Log on to Unified Communications Management as a security administrator.
2	In the navigation pane, click **Network, Elements**.
3	On the **Elements** page, select the check box next to the element that you want to edit.
4	Click **Edit**.
5	On the **Element Details** page, make the required changes. For more information about a field, click the **Help** link in the top right of the Element Manager page to access the online Help.
6	Click **Save**.

--End--

Deleting a secured element (Optional)

Remove an element from UCM if you no longer require the element.

Prerequisites

- Add an application. For more information, see Adding a new Contact Center application (Optional) (page 256).

Attention: If you cannot add new elements or delete selected elements after you restart the security service, click the Refresh icon on the Elements page.

Procedure steps

Step	Action
1	Log on to UCM as a security administrator.
2	In the navigation pane, click **Network, Elements**.
3	On the **Elements** page, select the check boxes next to the elements that you want to delete.
4	Click **Delete**.
5	On the **Delete Elements** page, click **Delete**.

Attention: UCM maintains an in-memory cache for all elements accessed from the current Web server. After you delete an element, the in-memory cache still contains the information for the element. However, UCM denies all permissions on an element after you delete it.

--End--

Security log management

Manage security logs to track security information for your elements. Log files can be opened directly, or downloaded for offline analysis.

Navigation

Inspecting security logs

Inspect security logs to open and view management activity information for all servers in your Unified Communications Management framework.

Procedure steps

Step	Action
1	Log on to Unified Communications Management as a security administrator.
2	In the navigation pane, click **Tools**, **Logs**.
3	On the **Logs** page, in the **Filename** column, click the name of the log you want to view.

--End--

Downloading and inspecting security logs

Download and inspect security logs to download and view management activity information for all servers in your UCM framework on your local system.

Procedure steps

Step	Action
1	Log on to Unified Communications Management as a security administrator.
2	In the navigation pane, click **Tools**, **Logs**.
3	On the **Logs** page, in the **Filename** column, right-click the name of the log you want to download, and select **Save Target As** in the shortcut menu.
4	In the **Save As** window, browse to where you want to save your .txt file and click **Save**.
5	In the **Download Complete** window, click **Close**.
6	Click the **Windows Start** button.
7	Click **My Computer**.
8	Browse to where you saved your .txt file, and double-click the file to open the file and view the contents.

--End--

Account and password management

Manage user accounts and passwords to control who can access your Contact Center server.

Navigation

Changing your password

Change your password to ensure the security of an admin account.

You can only configure Unified Communication Management (UCM) users on the primary security server. If your system security is managed by the backup Security Framework server, then you cannot make any changes to a user account.

Attention: You must wait 24 hours after setting a password before the system allows you to change it again.

Procedure steps

Step	Action
1	Log on to Unified Communications Management (UCM) as a security administrator, using the account for which you want to change the password.

2. In the navigation pane, click **User Services**, **Password**.
3. Click **Change Password**.
4. On the **Change Password** page, in the **Current password** field, type your current password.
5. In the **New password** field, type your new password.
6. In the **Confirm new password** field, retype your new password.
7. Click **Save**.

--End--

Variable definitions

Variable	Value
New password	The new password for the admin account. Allowed characters in the password are: a-z A-Z 0-9 { } | ( ) , / . = [ ] ^ ~ _ @ ! ‘ ; The new password must conform to any password policies defined by the security administrator. Applicable password policies are listed at the bottom of the Change Password page.

Resetting a user password

Reset user passwords when users cannot remember their password.

You can only configure Unified Communication Management (UCM) users on the primary security server. If your system security is managed by the backup Security Framework server, then you cannot make any changes to a user account.

Prerequisites

- Ensure that the user for whom you want to reset the password is locally authenticated. You cannot reset the password for an externally authenticated user.

Procedure steps

Step **Action**

1 Log on to Unified Communications Management (UCM) as a security administrator.

2 In the navigation pane, click **User Services**, **Administrative Users**.

3 On the **Administrative Users** page, in the **User ID** column, click the link of the user whose password you want to reset.

4 On the **User Details** page, in the **Password** field, type a new password for the user.

5 In the **Re-enter password** field, retype the new password.

6 Click **Save**.

The next time the user logs on, UCM prompts the user to change the password.

--End--

Variable definitions

Variable	Value
Password	The password used to log on to ECM. Allowed characters in the password are: a-z A-Z 0-9 { } | ( ) , / . = [ ] ^ ~ _ @ ! ‘ ; The password is a minimum of 8 characters long.

Disabling a user account (optional)

Disable a user account if the user no longer requires access.

You can only configure Unified Communication Management (UCM) users on the primary security server. If your system security is managed by the backup Security Framework server, then you cannot make any changes to a user account.

Procedure steps

Step	Action
1	Log on to Unified Communications Management as a security administrator.
2	In the navigation pane, click **User Services**, **Administrative Users**.
3	On the **Administrative Users** page, select the check box next to the user you want to disable.
4	Click **Disable**.

--End--

Reenabling a user account (optional)

Reenable a user account to grant access again to a user whose account is disabled.

You can only configure Unified Communication Management (UCM) users on the primary security server. If your system security is managed by the backup Security Framework server, then you cannot make any changes to a user account.

Procedure steps

Step	Action
1	Log on to Unified Communications Management as a security administrator.
2	In the navigation pane, click **User Services**, **Administrative Users**.
3	On the **Administrative Users** page, in the **User ID** column, click the link for the disabled account. If the user is disabled, **Disabled** appears in the Status column.
4	On the **User Details** page, select **Enabled**.
5	Click **Save**.

--End--

Deleting a user account (optional)

Delete a user account to remove a user from the system.

You can only configure Unified Communication Management (UCM) users on the primary security server. If your system security is managed by the backup Security Framework server, then you cannot make any changes to a user account.

Procedure steps

Step	Action
1	Log on to Unified Communications Management as a security administrator.
2	In the navigation pane, click **User Services**, **Administrative Users**.
3	On the **Administrative Users** page, select the check box next to the user account you want to delete. You can select multiple users to delete more than one account at a time.
4	Click **Delete**.
5	On the **Delete Users** page, click **Delete**.

--End--

Session management

Manage active sessions to ensure that only authorized administrators are logged on to Unified Communications Management (UCM).

Navigation

- Viewing active sessions (page 266)
- Ending sessions manually (page 266)

Viewing active sessions

View active sessions to determine who is logged on to UCM as an administrator.

Procedure steps

Step	Action
1	Log on to Unified Communications Management as a security administrator.
2	In the navigation pane, click **Security**, **Active Sessions**.

--End--

Ending sessions manually

End sessions manually to stop sessions that are initiated by unauthorized users.

Procedure steps

Step	Action
1	On the **Active Sessions** page, in the **User ID** column, select the check box next to the user for whom you want to end a session.
2	Click **Terminate**.

--End--

Network Control Center Server

Networking Service Monitor configuration

Configure Contact Center Manager Service Monitor to monitor the services status on various servers.

Prerequisites to Networking Service Monitor configuration

- Install all Contact Center Manager Server nodes. See *Nortel Contact Center Installation* (NN44400-311).
- Install all Contact Center Manager Administration servers. See *Nortel Contact Center Installation* (NN44400-311).
- Commission all Contact Center Manager Servers. See *Nortel Contact Center Commissioning* (NN44400-312).
- Commission all Contact Center Manager Server Administration servers. See *Nortel Contact Center Commissioning* (NN44400-312).
- Install the Network Control Center server software. See *Nortel Contact Center Installation* (NN44400-311).
- Install the Contact Center License Manager software. See*Nortel Contact Center Installation* (NN44400-311).

Navigation

- Changing the site to monitor (page 270)
- Closing the Networking Service Monitor (page 270)
- Refreshing the service status (page 271)
- Setting the default site information (client machine) (page 271)
- Adding a site (page 271)

Changing the site to monitor

Change the site to monitor one or more sites in the Contact Center Manager server network.

Procedure steps

Step	Action
1	Log on to the NCC server.
2	Click **Start**, **All Programs**, **Nortel, Contact Center**, **Manager Server**, **System Monitor**.
3	On the left panel, double-click **Other Sites** to display the sites on the network.
4	To monitor a site in the list, double-click the site name.

--End--

Closing the Networking Service Monitor

Close the Network Service Monitor when you no longer need the application to monitor network services.

Procedure steps

Step	Action
1	Right-click the Contact Center Manager Service Monitor icon in the system tray.
2	From the resulting menu, click **Exit Contact Center Manager Service Monitor**. You can not exit the application by clicking an exit button. Running the application again restores the existing instance of the Contact Center Manager Service Monitor.

--End--

Refreshing the service status

Contact Center Manager Service Monitor has an internal timer to refresh the status of the service from time to time. Manually refresh the service status to display the current status.

Procedure steps

Step	Action
1	Click **Refresh All** to refresh the status of all services.
2	Double-click a service in the list to refresh the status.

--End--

Setting the default site information (client machine)

A client user can change the default site information at any time. Changes take effect at the next startup of the Contact Center Manager Service Monitor.

Procedure steps

Step	Action
1	Click **Set Site**.
2	Enter the new IP address.

--End--

Adding a site

Add a site using the Contact Center Manager Server Configuration utility on the Network Control Center with administration access.

Prerequisites

- Log on to the Network Control Center as NGenSys.

- Start the Contact Center Manager Server Configuration utility in administrator mode.

Procedure steps

Step	Action
1	In the Nbconfig utility dialog box, click the **Site Table** tab.
2	Click **Add**.
3	Enter the Nortel server subnet IP address of the site to add.
4	Click **OK**.

--End--

Network Control Center server administration

Configure the Network Control Center server to enable skillset routing in your Contact Center.

Prerequisites

- Install all Contact Center Manager Server nodes. See *Nortel Contact Center Installation* (NN44400-311).
- Install all Contact Center Manager Administration servers. See *Nortel Contact Center Installation* (NN44400-311).
- Install the Network Control Center server software. See *Nortel Contact Center Installation* (NN44400-311).
- Install the Contact Center License Manager software. See*Nortel Contact Center Installation* (NN44400-311).
- Commission each Contact Center Manager server in your contact center. See *Nortel Contact Center Commissioning* (NN44400-312).

Navigation

- Adding a site to the NCC (page 274)
- Configuring network communication parameters (page 275)
- Adding access classes (page 277)
- Adding a site in Contact Center Manager Administration (page 278)
- Synchronizing site information (page 280)
- Adding a network skillset (page 281)
- Configuring network skillset properties (page 282)
- Configuring Agent Order Preference (page 283)
- Configuring the routing tables (page 284)
- Configuring routing table assignments (page 284)
- Configuring the historical statistics collection (page 286)

- Configuring MCDN network CDNs (page 287)
- Configuring DNIS Network CDNs (page 289)

Adding a site to the NCC

Add a site using the Contact Center Manager Server Network Configuration utility.

You can also use the Network Configuration utility to verify the configuration of the communications database at each server and ensure that each site has valid IP addresses.

Prerequisites

- Log on to the Network Control Center server as NGenSys.
- Know the CLAN IP address for each server to add.

Attention: Each server must have a unique CLAN IP address.

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Manager Server**, **Network Configuration**.
2	In the **Nbconfig** dialog box, click the **Site Table** tab.
3	Click **Add**.
4	In the **Add Site** dialog box, in the **CLAN IP Address** box, type the CLAN IP address of the server.
5	Click **OK**. *The server is added to the list in the site table.*
6	Repeat step 3 to step 5 for each server in your network.
7	Click **Verify**. *This verifies the connection to the nodal servers.*
8	If all the site names are correct, click **Apply** to update the database and synchronize the site table. *The Flags column shows the progress of synchronization.*
9	Click **Refresh** to update the status of the flags.

Synchronization is complete when an N appears in the Flags column beside the NCC, and an S appears beside each server.

10 Click the **Address Table** tab.

The communication addresses of the new servers appear on the Address Table page.

--End--

Procedure job aid

The Flags column in the site table can contain the following values

Flag	Description
N	Network Control Center (NCC)
S	Server
T	NCC is transferring information to the server
G	NCC is getting information from the server
D	Deleting site
C	Changing site information

Configuring network communication parameters

Configure the following network communication parameters on each server in the network:

- the number that your telephony switch dials to route a call to that site
- the number of times your server tries to queue calls to the site after a route attempt fails, and the number of seconds between retries
- the amount of time an agent at the site is reserved to answer a call routed from your server
- the amount of time your server waits for a reply from the remote sites, if routing is based on longest idle agent or average speed of answer
- the Landing Pad type, if the server has Universal Networking enabled

Procedure steps

Step **Action**

1 Log on to the Contact Center Manager Administration client.

2 On the launchpad, click **Configuration**.

3 In the left pane, expand **Global Settings**.

4 In the right pane, click the row containing the site for which you want to edit communication parameters.

5 Click **Site Parameters**.

6 From the **Landing Pad Type** list, select the Landing Pad type. Available Landing Pad types depend on the site configuration on the NCC.

This column is present only if Universal Networking is enabled on the server.

If you change Landing Pad type, review all timer settings as they can require modifications depending on the selected Landing Pad type.

7 In the **Dialable DN/Prefix** box, type the number that the telephony switch dials to reach the network CDN at the remote site. The number must include prefixes required by the dialing plan configured on the telephony switch. The Dialable/DN prefix value can be up to 32 characters in length.

If you use MCDN networking, enter the number in the format used in your NACD routing table.

You configure the Dialable DN/Prefix field differently if you select MCDN as the Landing Pad type than if you select CDN (Route Point) or DNIS as the Landing Pad type. If you select MCDN as the Landing Pad type, you must configure the Dialable DN/Prefix field with the full dialable number to the network CDN at the target. This is the number that the telephony switch dials to route a call.

8 In the **Number of Retries** box, type the number of times that your server attempts to route a call to a reserved agent at this site before filtering the site from the routing table.

9 In the **RetryTimer (Sec.)** box, type the time that elapses before the server attempts to queue a call to this site after a route attempt fails (for example, if all trunks are busy).

10 In the **Agent Reserve Timer (Sec.)** box, type the number of seconds an agent at this site is reserved when your site attempts to send a call. If the source site cannot cancel the agent reservation, then it expires after this period.

Make sure that the Agent Reserve Timer allows enough time for calls to be networked at the destination. Make several test calls to a network skillset that has only one agent logged on at the destination site, and then run a report to ensure that the number of times the agent is reserved is equal to the number of network calls answered. If the number of times the agent is reserved is greater than the number of network calls answered, then the reservation timer is probably too low. Increase the agent reservation timer and make the test calls again.

The Agent Reserve Timer also applies to the source site if it uses either the Longest Idle Agent or Average Speed of Answer feature and network skillsets are configured with include local node enabled.

11 For the source node only, in the **Nodal Request Wait Timer (Sec.)** box, specify the length of time to wait for responses from destination servers, if the skillset is configured for longest idle agent or average speed of answer. Normally, all nodes respond before the timer expires; after receiving responses from all destination sites, the local server routes the calls and cancels all agent reservations. If one site is slow to respond, agents remain reserved while the local server waits for the response. This timer determines the length of time the server waits for a response before it routes the call and cancels agent reservations.

The timer should provide sufficient time to allow most destination sites to respond under normal conditions. However, if the timer is too high, agents at the responding sites are reserved (and thus unavailable to answer calls) for long periods of time.

You can configure this timer differently for each source site. However, the timer applies to all destination sites to which the source site queues calls.

The Nodal Request Wait Timer cannot equal or exceed the Agent Reserve Timer for the destination sites. (This ensures that agent reservations do not time out before the call can be routed.) Nortel recommends that the Agent Reserve Timer be at least 2 seconds more than the Nodal Request Wait Timer.

12 Click **Submit** to save your changes.

--End--

Adding access classes

When you log on to the Contact Center Manager Administration client, you can use the Access and Partition Management component to configure access classes for the Contact Center Manager Servers, and for the Network Control Center (NCC) server.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration client.

2	On the launch pad, click **Access and Partition Management**.
3	From the **Add** menu, select **New Access Class**.
4	In the **New Access Class Name** box, type a name for the access class. Use a descriptive name for the type of user to have this access level or, the type of privileges available at this access level. You can use alphanumeric characters only for the access class name.
5	Click **Submit**.
6	Select a server on which to configure the access class.
7	For each element in the **Access Class Properties** list, select an access level.
8	Click **Submit**.

--End--

Adding a site in Contact Center Manager Administration

A site is a location in the network with a telephony switch and a server in Contact Center Manager Server. You must configure the NCC with information about each site in the network so that it can communicate with the network servers and enable the servers to communicate with each other.

Prerequisites

- Make sure that each site is correctly configured before you add the next site.
- The sites that you can add in this window are those that you configured using the Nbconfig utility when you configure the communications database on the NCC. To add a site that is not listed, you must first add it to the site table using this utility.
- You can add up to 30 sites.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration.
2	On the launchpad, click **Configuration**.
3	In the left pane, expand the Network Control Center (NCC) server.

4 Select the **Sites** folder.

The CDN Landing Pad and DNIS Landing Pad columns appear only if Universal Networking is enabled on the NCC and for at least one site. If Universal Networking is not enabled for a site, the CDN Landing Pad and DNIS Landing Pad check boxes are dim.

5 Click **Add Site**.

6 Type the name of the site to add exactly as it appears in the Nbconfig utility.

7 Click **OK**.

The site name appears in the Site Name box. Wait (at least 5 minutes) for confirmation that the site is up.

8 Click **Refresh Status**.

The CDN (Route Point) Landing Pad check box, DNIS Landing Pad check box, and Target Node Count box are all read-only when you add the site for the first time.

9 Click **Refresh Status** to modify these boxes.

10 In the **Contact Person** box, type the name of the person to contact if problems with the site occur.

11 In the **Contact Number** box, type the phone number where the contact person at the site can be reached.

12 In the **Comment** box, type additional information about the contact person.

13 In the **Filter Timer** box, type the amount of time to filter the site from the routing tables if it cannot be reached.

14 From the **Relative to GMT** list, select the time difference (in hours) between GMT and the time zone for the site. This information is used for time zone conversion and consolidated reports.

15 To use CDN (Route Point) Landing Pads (for Universal Networking) for this site, select the **CDN (Route Point) Landing Pad** check box.

This check box is available only if Universal Networking is enabled. If Universal Networking is enabled, you must add a CDN (Route Point) Landing Pad or a DNIS Landing Pad. Optionally, you can add both.

16 To use DNIS Landing Pads (for Universal Networking) for this site, select the **DNIS Landing Pad** check box. This check box is available only if Universal Networking is enabled.

17 In the **Target Node Count** box, type the number of target nodes to which the source node sends a Network Agent Request (NAR). You can type digits from 3 to 20.

18 Click another row of the table to submit the site information.

--End--

Synchronizing site information

Synchronize site information that the Network Control Center shares with each Contact Center Manager Server in the network. This information includes

- sites in the network
- network skillsets
- routing tables

The Network Control Center propagates this information to all sites in the network at the following times:

- when it restarts
- after recovering from a network error (for example, if the connection to a specific site was previously unavailable)
- when you manually synchronize sites

Normally, you do not need to synchronize sites manually. However, if the routing tables at the server do not match the routing tables at the NCC, you can force a manual synchronization rather than wait for the NCC to propagate the changes across the network.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration client.
2	On the Launchpad, click **Configuration**.
3	In the **Configuration** window, double-click the Network Control Center (NCC) server.
4	Select the **Sites** folder.
5	In the **Sites** window, in the table, select the row containing the site to synchronize.
6	Below the table, click **Sync Site**.
7	In the confirmation window, click **Yes**. The NCC sends information to the selected site. A message appears in the message pane indicating if the synchronization was successful. The message is also logged in the Audit Trail window.

--End--

Adding a network skillset

Add a network skillset to the process to assign agents to network skillsets is the same as the process to assign agents to local skillsets. The server administrator of each server in the network must perform this task on the server.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration.
2	On the launchpad, click **Configuration**.
3	In Contact Center Manager Administration, on the system tree in the Configuration component, double-click the Network Control Center (NCC) server.
4	Select the **Network Skillsets** folder.
5	In the **Network Skillset Name** box, type the name of the network skillset. Network skillset names must be unique. You cannot change the name of a network skillset. To change a skillset name, you must delete the skillset, and then add it again.
6	In the **Comment** box, type additional information about the network skillset. This field is optional.
7	From the Routing Method list, select the type of routing table to use for this skillset—round-robin or sequential.
8	For Networking Method, select one of the following options: Select **First Back**. The server routes network calls to the first responding site. **OR** Select **Longest Idle Agent**. The server waits the configured time for sites to respond and then routes calls to the site with the highest priority agent and the longest idle time. **OR**

Select **Average Speed of Answer**. The server waits the configured time for sites to respond and then routes calls to the site with the highest priority agent and the lowest average speed of answer for the skillset.

9 Click another row of the table to save the new network skillset.

--End--

Configuring network skillset properties

Configure the following properties for each network skillset:

- the maximum number of calls that can be queued for the skillset at this server
- the number by which queued calls must decrease before filtering stops
- whether to queue calls to the local site

In addition, if you use the Longest Idle Agent feature, you must make sure that you configure the Agent Order Preference in the Global Settings the same way on every network server.

Procedure steps

Step **Action**

1 Log on to Contact Center Manager Administration.

2 On the launchpad, click **Configuration**.

3 In the left pane, click **Skillsets**.

4 In the **Call Request Queue Size** box, type the maximum number of calls that can be queued for this skillset on your server. For example, if this value is 100, then up to 100 calls can be queued for this skillset at your server. When 100 calls are queued, your server is filtered from the routing tables for this skillset at every other site that attempts to queue a call for this skillset to your site. If the Call Request Queue Size is zero (0), then no calls are networked in from other sites.

5 In the **Flow Control Threshold** box, type the number by which queued calls for this skillset must decrease before filtering of your server stops. For example, if Call Request Queue Size is 100, and Flow Control Threshold is 20, then filtering of this network skillset ceases only when the number of queued calls falls to 80.

6 Select the **Include Local Node** check box to queue calls to the local node, as well as to remote nodes, with the Queue to Network Skillset command. This option is available only for Release 5.0 and later.

7 Click another row of the table to save the changes.

--End--

Configuring Agent Order Preference

Configure the Agent Order Preference for networked sites in your contact center to select the preference. For example, if two agents are available, you can choose the agent closest to the original location of the contact.

Procedure steps

Step **Action**

1 Log on to Contact Center Manager Administration.

2 On the launchpad, click **Configuration**.

3 In the left pane, click **Global Settings**.

4 From the **Agent Order Preference** list, select one of the following:

Longest total time in idle state since login—Choose this option if you want calls presented to the agent who accumulated the most idle time since logging on.

OR

Longest time in idle state since last status change—Choose this option if you want calls presented to the agent who accumulated the most idle time since their last status change.

OR

Longest total time since last CDN/ACD call—Choose this option if you want calls presented to the agent with the longest elapsed time since handling a CDN/ACD call.

5 Ensure that Agent Order Preference is configured identically on each server in the network.

--End--

Configuring the routing tables

When you configure a site, you define a routing table for each network skillset at that site. A routing table defines the sites to which scripts using network skillsets route calls.

Prerequisites

- Add network skillsets.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration.
2	On the launchpad, click **Configuration**.
3	In the left pane, expand the **Network Control Center (NCC)** server.
4	Select the **Sites** folder.
5	In the **Network Sites** table, select the check box for each site to which you want to route calls for this skillset. You can add up to 20 sites to a routing table.
6	To arrange the routing order, select a site, and then click the up and down Rank arrows.
7	After you arrange all the sites in the routing table for this skillset, select the next skillset to configure.
8	Follow step 5 to step 7 for each skillset to include in the routing table.
9	Click **Submit** to immediately activate the routing table for this site.
10	To save the routing table as an assignment, click the black triangle beside the Save/Schedule Routing Table Assignments heading.

--End--

Configuring routing table assignments

Create a routing table assignment or a new routing table assignment or use another assignment as a template to create the routing table assignment.

Each assignment applies only to the site for which it is defined.

Prerequisites

Attention: If you create an assignment from the NCC using a client, you must select all network skillsets for the source site and reconfigure the routing tables. If you do not select a network skillset that is supported by the source site, when you run the table routing assignment, the Site properties routing table is overwritten with a blank routing table.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration.
2	On the launchpad, click **Configuration**.
3	In the left pane, expand the Network Control Center (NCC) server.
4	Select the **Sites** folder.
5	From the table in the Sites window, select the site to configure. The CDN Landing Pad and DNIS Landing Pad columns appear only if Universal Networking is enabled on the NCC and for at least one site. If Universal Networking is not enabled on a site, the CDN Landing Pad and DNIS Landing Pad check boxes are disabled.
6	In the **Network Skillsets** table, click the skillset to configure.
7	In the **Network Sites** table, select the check box beside each site to which to route calls for this skillset. You can add up to 20 sites to a routing table.
8	To arrange the routing order, select a site, and then click the up and down Rank arrows.
9	After you arrange all the sites to include in the routing table for this skillset, click the next skillset to configure.
10	Repeat step 6 to step 9 for each skillset to include in the routing table.
11	Click **Submit** to immediately activate the routing table for this site.
12	To create a routing table assignment, click the black triangle beside the Save/Schedule Routing Table Assignments heading.
13	In the **Save Assignment as** box, type the name of the assignment.
14	In the **Comment** box, type additional information about the assignment.
15	Perform one of the following tasks: To save the routing table assignment, go to step 21. **OR**

To schedule the assignment to run at a future time, from the Schedule Task list, select the type of schedule to create. You can choose from Specific date, Daily, Weekly, and Monthly.

16 From the **Start Time** list, select the time for the schedule to begin.

Attention: The time values represent the application server time, not the client time. If your application server is in a time zone different from the client for which you are scheduling the assignment, you must consider the time difference.

17 To view the current application server time, click **Update** beside the **Application Server Time** box. The schedule that you define must be based on this application server time.

18 In the **Start Date** box, click the button to view a calendar.

19 In the calendar, click the date when you want the schedule to begin.

20 Based on the schedule type (that is, daily, weekly, or monthly), select the days and months when you want the assignment to occur.

21 Click **Save Assignment** to save the assignment.

22 Perform one of the following tasks.

Click **Yes** to create the reset assignment.

OR

Click **No** if you do not want to create a reset assignment.

23 Click **Schedule** to make the assignment effective.

--End--

Configuring the historical statistics collection

Configure the historical statistics collection to specify the length of time network call-by-call statistics are stored on the Network Control Center server.

Procedure steps

Step **Action**

1 Log on to Contact Center Manager Administration.

2 On the launchpad, click **Configuration**.

3 In the left pane, expand the Network Control Center (NCC) server.

4 Click the **Network Historical Statistics** folder.

5 In the **Keep Network Call-by-Call data for** box, specify the number of days to store call-by-call statistics on the NCC.

This value must match the value configured in the Historical Statistics Configuration window on each server. For example, if you retain network call-by-call statistics for 3 days, but you retain call-by-call statistics for 2 days at each site. When you generate a network call-by-call report, the report contains information about events occurring at the destination site, but it does not contain information about events occurring at the source site.

6 In the **Network call rate** box, estimate the average number of calls networked out (routed from one site to another) per hour.

7 Click **Submit**.

The system calculates the amount of disk space required for the call-by-call database under your configuration. This amount appears in the Required box. The available disk space appears in the Actual box.

--End--

Configuring MCDN network CDNs

Configure MCDN network CDNs for your server. On each server in the network, you must configure the MCDN network CDN on which incoming network calls are received when using MCDN NSBR.

You can configure multiple MCDN network CDNs for the following reasons:

- To enable agents to identify the source site from the telephone display. For example, if all calls from Boston arrive on the MCDN network CDN 555-7777, then when this number appears in the phoneset display, the agent knows that the call was sent from Boston. This information can help the agent determine how to respond to the caller. For information about configuring phoneset displays, see the Contact Center Manager Administration online help.
- To generate CDN statistics on a per-site basis. You can use network reports to view which source sites are networking calls in to your site.
- To set up treatments for calls from source sites that are returned to the queue before they are presented to an agent. Calls can be returned to the queue if an agent becomes unavailable (by pressing Not Ready, for example) in the moment between arrival of the call at the site and presentation of the call to the agent. For example, you can give RAN

messages to callers from various source sites who are routed to the target node and are waiting for an agent to answer.

To use multiple MCDN network CDNs, you must configure a CDN for each server from which you receive calls and configure each server to route calls to a different MCDN network CDN.

Prerequisites

Attention: Use the MCDN network CDN for incoming network calls only. To check whether local calls are arriving on an MCDN network CDN, use the Network Call intrinsic, and then give the local call a special treatment, such as a RAN route that gives the number to dial for local calls. For more information, see *Nortel Contact Center Configuration – Service Creation Environment Application Development* (NN44400-510).

- Configure the CDNs on the telephony switch. At the telephony switch, each CDN is configured like a local CDN; MCDN network CDNs have no special requirements. For information about configuring a CDN on the telephony switch, see the *Nortel Contact Center Configuration – CS1000 Integration* (NN44400-512).

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration.
2	On the launchpad, click **Configuration**.
3	In the left pane, click the **CDNs** folder.
4	In the **Name** box, type the name of the CDN as it appears in the CDNs window and on reports.
5	In the **Number** box, type the CDN number as configured on the telephony switch. This number is the dialable DN that other sites must use to send network calls to your site. To recognize where incoming network calls arrive from, you can set up a separate MCDN network CDN for each site from which you can receive calls.
6	From the **Call Type** list, select **MCDN Network**.
7	Select the **Acquired?** check box to acquire this CDN.
8	Click another row of the table to save the new CDN.

--End--

Configuring DNIS Network CDNs

Follow the procedure in this section to configure the DNIS network CDNs for each server in the network. You must configure the DNIS network CDN on which incoming network calls are received on a DNIS Landing Pad for each server in your network.

You can configure only one DNIS network CDN on each server.

Prerequisites

- Configure the DNIS Network CDNs on the telephony switch. At the telephony switch, each CDN is configured like a local CDN; DNIS Network CDNs have no special requirements. For information about configuring a CDN on the telephony switch, see *Nortel Contact Center Configuration – CS1000 Integration* (NN44400-512).

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration.
2	On the launchpad, click **Configuration**.
3	In the left pane, click the **CDNs (Route Points)** folder.
4	In the **Name** box, type the name of the CDN as it appears in the CDNs window and on reports.
5	In the **Number** box, type the CDN number as configured on the telephony switch. Ensure that this number matches the CDN number configured on the telephony switch. The DNIS Landing Pads on the telephony switch must map to the DNIS Network CDN. For information about mapping Landing Pads, see *Nortel Contact Center Configuration – CS1000 Integration* (NN44400-512).
6	From the **Call Type** list, select **DNIS Network**.
7	Select the **Acquired?** check box to acquire this CDN.
8	Click another row of the table to save the new CDN.

--End--

Communication Control Toolkit Server

Communication Control Toolkit fundamentals

The Communication Control Toolkit server is a client/server application that helps you implement Computer-Telephony Integration (CTI) for installed and browser-based client integrations. For switches, the Communication Control Toolkit facilitates the integration of contact center, Knowledge Worker, and Self Service solutions with your client applications. This chapter provides some background information for the Communication Control Toolkit server and the applications.

Navigation

Automatic Call Distribution

Automatic Call Distribution (ACD) is a set of feature packages based on software that provides call distribution in a call center environment. Some of the features include the following:

- The ability to setup one main number and distribute the calls to a group of agents
- The ability to set up a supervisor position for an ACD group
- The ability to monitor the quality of the service provided to incoming callers
- The ability to gather information about the calls such as, hold time, time in queue, and the number of agents logged in a queue

Nortel provides a separate application called ACDProxy Service. This application allows the agents to log on, log off, and go ready or not ready. ACDProxy Service also registers the ACD Queue numbers so an application need not start prior to an agent logs on to a queue. Nortel supports the following ACD features:

- Login or Logout
- Ready or Not Ready
- Make set busy
- Make set in service

Communication Control Toolkit Administration tool (NCCT Console)

The NCCT Console, or Nortel Communication Control Toolkit console is a software component on the Communication Control Toolkit server that you use to load the Communication Control Toolkit database with telephony settings and resource information.

Contact Management Framework

The Contact Management Framework (CMF) is a central repository for objects representing communications, including endpoints (terminals and addresses), transactions (contacts), and the relationships between them. The CMF includes the contact, resource, and agent managers. The CMF is also an abstraction or unification layer for various communications switch interfaces. The Communication Control Toolkit API objects have a one-to-one mapping with the objects in the CMF.

The CMF is driven by one or more switch interface service providers (for example, a connector for CS 1000/Meridian 1 communications or a SIP provider for SIP-enabled contact center). The switch interface service provider updates the CMF objects to reflect the status of the switch and to monitor the objects in the CMF for requests that objects pass to the switch.

Logging trace information

You can use the logging utility to track trace information to diagnose problems, to provide information to technical support, and to verify method calls and operations.

Resources

Configure the following resources in Communication Control Toolkit:

- Windows user—Users who are logged on to one or more communication terminals.
- Windows user group—A logical group of Windows users (for example, a sales group or a support group) that have a common property.

- Contact Center user—Users that are configured in the contact center database on Contact Center Manager Server with a designated role in the contact center such as a supervisor or an agent to received queued contacts.
- Contact Center user group—A logical group of Contact Center users (for example, agents or supervisors) that have a common property.
- Terminal—A physical (including software applications) communications endpoint such as an e-mail client or an IVR line. Two terminal types indicate the types of physical communication endpoints:
  - Agent—An agent terminal can log on to an ACD queue and answer calls routed to that queue (if scripted). An Agent terminal can also make calls.
  - Knowledge Worker—A knowledge worker terminal cannot log on to an ACD queue or answer calls routed to a queue. A knowledge worker terminal can make and answer regular calls.
- Terminal group—A logical group of terminals (for example, local office, support office) that have a common property.
- Address—A logical communications endpoint such as an e-mail address or telephone number. An address can be one of three types:
  - Basic—A basic address (SCR key) is an address that has an associated terminal (physical endpoint). The basic address is used by Communication Control Toolkit users to answer and make calls.
  - Route Point—A route point address (CDN) is an address to a terminal that is not associated with a line. The Route Point address is used by the Telephony Service Provider to accept incoming contacts or as a point to which contacts are routed.
  - Agent—A position ID (ACD key) for the CS 1000/Meridian 1 switch.
- Address group—A logical group of address that have a common property.
- Workstation—A computer used by Communication Control Toolkit client operations on the same domain as the Communication Control Toolkit server.
- Network IVR—In a networked environment, the Network IVR driver uses information stored in the remote host address table to request call data for inbound calls overflowed from a remote CS 1000. The first entry on the Network IVR port for local CCT Server. It has a fixed 127.0.01 IP address and this can not be changed. This first entry can not be deleted.
- Provider—A switch interface service provider to connect telephony devices to the Communication Control Toolkit server. Two provider types are available:
  - Passive (for voice contacts)

— CCMM (for multimedia contacts)

Default address and terminal settings

The Communication Control Toolkit administrator uses a default property page on the Communication Control Toolkit console to configure default values for address and terminal resources. The Communication Control Toolkit console uses these defaults when you add new address or terminal resources (for example, if you have the default for addresses to a route point enabled, then, when you add a new address, those values appear as defaults in the address fields). You can accept or change these default values at any time.

Resource mapping

Mappings use the following principles:

- Mappings are bidirectional. This means that if you map one resource to a second, then the second resource is also mapped to the first. For example, if you map a user to a user group, the user group is also mapped to the user.
- Mappings are distributed using groups. If you map one resource to a second resource that is a group, and the second resource to a third, then the first resource also maps to the third. For example, if you map two users to a user group, and then map the user group to an address, then the users are considered mapped to the address. Or, if you map a user to a user group, the user inherits the user group terminals and addresses.
- Mappings are not associative. If you map one resource to a second, and map the first resource to a third, the second and third resources do not map to each other. For example, if you map a terminal to an address, and then map that terminal to a user, the user does not inherit the address. You must also map the address to the user.
- Resources cannot map resources of the same type. For example, you cannot map a user to a user, or a terminal to a terminal. Grouped resources cannot be mapped to resources that are closely related. For example, you cannot map a terminal group to an address group because both resources are types of end points.
- Automatic address mapping occurs in limited circumstances. Automatic address mapping occurs only when you map terminals or terminal groups to a user (or user group). If you map a terminal to a user, and if automatic mapping is enabled, then the addresses automatically map to the user (or user group) as well. If you map a terminal group to a user (or user group) with automatic mapping enabled, then the addresses of the terminals in the terminal group automatically map to the user (or user group). If you map a terminal group to a user (or user group), and if automatic mapping is enabled, if the terminal group has no terminals at the time of the mapping, then no addresses map to the user. If you add a new terminal to

an existing terminal group, users that map to the new terminal do not automatically map to the address of the new terminal. The user maps to the address manually. Automatic mapping of addresses is supported only when you map terminals or terminal groups to a user or user group.

- Only terminals map to workstations.
- When you map a user to a terminal, you must map the terminal to an address that is maps to the user.
- You do not map route point addresses to terminals. route point addresses do not have associated terminals.

Possible resource-to-resource mappings

	User	**User group**	**Contact Center user**	**Contact Center user group**	**Terminal**	**Terminal group**	**Address**	**Address group**
User		X	X	X	X	X	X	X
User group	X		X	X	X	X	X	X
Contact Center User	X	X		X				
Contact Center User group	X	X	X					
Terminal	X	X				X	X	
Terminal group	X	X			X			
Address	X	X			X			X
Address group	X	X					X	
Workstation					X			

Programming interfaces

When you configure your Communication Control Toolkit server, your Communication Control Toolkit users log on with user accounts based on Active Directory/Domains or with local user accounts on the Communication Control Toolkit server.

Communication Control Toolkit local users are configured in the Local users and Groups section of the Computer Management Tool on the Communication Control Toolkit server. To use local accounts on the Communication Control Toolkit server, the Communication Control Toolkit software must be installed using a local administrator account on the Communication Control Toolkit server. In this scenario the user name has the format <cctservername>\<username>.

Users who can access multiple domains can also access the Communication Control Toolkit client as long as trust is established between the domains; the user does not have to log on to separate domains to use the Communication Control Toolkit client.

Application programming interface

Communication Control Toolkit is software for installed and browser-based client integrations. Communication Control Toolkit delivers a single cross-portfolio multichannel Application Programming Interface (API) that facilitates the integration of Knowledge Worker, Self-Service, and Contact Center solutions for your client applications.

The Application programming interface (API) is published as Microsoft .NET types and is distributed as a Windows assembly, which is referenced by application developers.

You can use Communication Control Toolkit as next generation computer telephony integration (CTI) middleware and a next generation CTI toolkit. On the client, the API provides a set of interfaces, collectively known as the Full Communication Control Toolkit API. Two abstraction layers are also available:

- the Lite Communication Control Toolkit API
- the Graphical Communication Control Toolkit API

You can implement these layers using the Full Communication Control Toolkit API. They provide easy access to a subset of Communication Control Toolkit functions, which you can use for CTI functionality without having low-level CTI knowledge for the simple development of powerful integrations and applications such as

- desktop applications (for example, Call Control Toolbar)
- server applications (for example, Call Recording, Work Force Management)
- screen-pop utilities
- business application or Computer Resource Management (CRM) connectors

For more information about using the Communication Control Toolkit API, see the Nortel Communication Control SDK Programmers Reference Guide. The Nortel Communication Control SDK Programmers Reference Guide is a help file that accompanies the Software Development Kit. You must join the developer partner program and purchase the Communication Control Toolkit SDK to download the documentation from www.nortel.com.

One example of a Communication Control Toolkit client application is the Contact Center Agent Desktop. If your contact center is licensed to handle only telephony calls, you can install the Contact Center Agent Desktop telephony toolbar on the Communication Control Toolkit server to provide agents with a soft phone on their desktop. The Contact Center Agent Desktop telephony toolbar is a component on the Contact Center Multimedia server software.

Web services

The CCT Open Interfaces is a development environment that offers functionality similar to the CCT SDK but provides you with the flexibility of choosing your own development environment. The CCT Open Interface offers a series of service definitions using WSDL, which allows you to choose functionality similar to what is offered by the full API.

You can use these services to re-create Agent tools within your own applications or alternatively access call control functionality for Contact Center from any business process.

For more details, see the SDK documentation.

Communication Control Toolkit Reference Client

The Reference Client is an application installed automatically on the Communication Control Toolkit server that mimics a telephone device. You can use the Reference Client to simulate making telephone calls, transferring telephone calls, and other telephone events to test the functionality of the Communication Control Toolkit database.

Use the Reference Client to verify calls on one switch or calls transferred between switches.

Server settings configuration

During the initial commissioning of the Communication Control Toolkit server, most initial settings were configured. Commissioning tasks are as follows:

- Configure the license manager
- Configure the Contact Management Framework settings
- Load the Communication Control Toolkit database with resources and mappings from the switch, host server, and Contact Center agents.
- Configure logging to track warnings and errors in the log files

Use similar procedures in this chapter to change initial settings in the Nortel Communication Control Toolkit Console.

Navigation

- Configuring the licensing for Communication Control Toolkit (page 298)
- Installing and configuring MPS Manager software (page 301)
- Configuring the Contact Management Framework (page 302)
- Configuring the logging tool (page 303)
- Configuring the Communication Server 1000 service provider (page 305)

Configuring the licensing for Communication Control Toolkit

Configure the licensing for Communication Control Toolkit to point the Communication Control Toolkit server at the Contact Center license manager.

Attention: When Communication Control Toolkit co-resides with Contact Center Manager Server, you must configure Communication Control Toolkit licensing using Contact Center Manager Server configuration.

Prerequisites

- Contact Center License Manager is installed.

Procedure steps

Step	Action
1	Log on to the **Communication Control Toolkit** server.
2	Click **Start, All Programs**, **Nortel**, **Contact Center, Communication Control Toolkit**, **CCT Console**.
3	Expand **NCCT Admin**.
4	In the left pane of the CCT 7.0 console, click **CCT Server**.
5	In the right pane of the CCT 7.0 console, double-click **CCT Server**.
6	Click the **Licensing** tab.
7	Under **Primary License Manager Server**, in the **IP Address** box, type the IP address for the server on which the License Manager is installed.
8	Under **Secondary License Manager Server**, in the **IP Address** box, type the IP Address for the server on which the secondary License Manager is installed.

Attention: This option is only available if you have installed corporate licenses.

Step	Action
9	From the **License Type** list, select Nodal or Corporate.
10	In the **Log File** box, browse to the location in which to store the log files for the licensing trace logs.
11	In the **Logging Level** box, select the logging level to perform.
12	In the **Max Log File Size (in MB**) box, type the maximum log file size in megabytes.
13	Click **OK**.

--End--

Variable definitions

Variable	Value
License Type	The type of license for the License Manager. Nodal—The license applies to only one installation of Contact Center Manager Server. The Secondary License Manager cannot be configured for a Nodal license. Corporate—The license applies to a collection of Contact Center Manager Servers.
Logging Level	The level of logging to monitor for Communication Control Toolkit errors. You can choose one of the following: No Logging—No events are logged to LMService.log. If errors or warnings are received during LMService operation, the event is written to the LMService.log Errors Only—Only errors and warning events are logged to the LMService.log file. Debug—All events including informational messages are logged to the LMService.log file.
Primary License Manager Server IP Address	The IP address of the server on which the License Manager application is installed. If you install the Communication Control Toolkit co-resident with Contact Center Manager Administration Server, the License Manager Server Information (IP address or port number) fields are read-only.
Secondary License Manager Server IP Address	The optional IP address of the server on which the backup License Manager application is installed. If you install the Communication Control Toolkit co-resident with Contact Center Manager Administration Server, the Secondary License Manager Server Information (IP address or port number) fields are read-only.

Installing and configuring MPS Manager software

Install and configure the Media Processing Server (MPS) Manager software to configure the Communication Control Toolkit for the Media Processing Manager in a self-service environment where the MPS handles contacts without directing the call to an agent.

You must configure two packages:

- pdp (MPS Manager Data Provider) collects statistics and alarm data from notes and components in an MPS Manager network.
- view (MPS Manager) contains the MPS Manager suite of graphical tools for MPS administration, operation and control.

Prerequisites

- Ensure that you have the Nortel_SelfService CD-ROM that contains the Nortel_SelfService_3.0.0.3.6.msi file.

Procedure steps

Step	Action
1	Open the ivr-cti folder on the Nortel_SelfService CD-ROM.
2	Double-click **Nortel_SelfService_3.0.0.3.6.msi**.
3	In the **Configuration** window, click **MPS Manager Workstation**.
4	Click **Next**.
5	In the **Welcome** window, click **Next**.
6	In the **Program Maintenance** window, select **Modify**.
7	Click **Next**.
8	In the **Custom Setup** window, under CCTIVR, select **pdp** and **view**.
9	Click **Next**.
10	In the **Ready to Modify the Program** dialog box, click **Install**.
11	Click **Start**, **All Programs**, **Nortel**, **SelfService**, **MPS Manager**.
12	Confirm that the Communication Control Toolkit 7.0 services show as started.
13	Close the **Services** window.
14	Open the folder **C:\Program Files\Nortel\css1\etc**.
15	Open the **tls.cfg** file in **Notepad**.
16	Add the following lines of code to the tls.cfg file:

```
setmaxrequestqueuelag 32
setmaxdelayrequest 400
setdelayrequesttime 50
```

17 Save and close the tls.cfg file.

--End--

Configuring the Contact Management Framework

Configure the Contact Management Framework (CMF) for the Communication Control Toolkit server to manage the contact routing for your network configuration.

Prerequisites

- Understand the network requirements for your installation of Communication Control Toolkit (co-resident, stand-alone, or multimedia). For more information, see Contact Management Framework (page 292).
- Know how to stop and restart the Contact Center Manager services.
- Know how to stop and restart the core Communication Control Toolkit services.

Procedure steps

Step	Action
1	Log on to the Communication Control Toolkit server.
2	Click **Start**, **All Programs**, **Nortel**, **Contact Center, Communication Control Toolkit**, **CCT**.
3	Expand **NCCT Admin**.
4	In the left pane of the CCT 7.0 console, click **CCT Server**.
5	In the right pane of the CCT 7.0 console, double-click **CCT Server**.
6	In the **CCT Server Properties** dialog box, click the **CMF Configuration** tab.
7	Under **Communication Control Toolkit Deployment Type**, select your deployment option for Communication Control Toolkit.
8	In the **CCMS Server Name** box, type the name of the Contact Center Manager Server.
9	Click **Apply**.
10	Click **OK**.

11 If you selected the co-resident option (the first deployment type), restart the Contact Center Manager Server services.

12 Stop and restart the core Communication Control Toolkit services.

--End--

Variable definitions

Variable	Value
Communication Control Toolkit Deployment Type	Choose the deployment type for Communication Control Toolkit based on your network configuration. Choose CCT 7.0 Installation (Contact Center only) if your contact center is licensed for multimedia contacts and the Communication Control Toolkit server software is installed on the same server as Contact Center Manager Server. Choose Standalone CCT 7.0 Installation if your contact center is licensed for multimedia contacts and the Communication Control Toolkit server software is not installed on the same server as Contact Center Manager Server. Choose the last option if you are not licensed for multimedia contacts in your contact center.

Configuring the logging tool

Configure the logging tool to configure the maximum size and number of log files for each of the main Communication Control Toolkit components. The default values for each log file is five log files of 50 MB each. You can choose the location for the log files.

Procedure steps

Step	Action
1	Log on to the Communication Control Toolkit server.
2	Click **Start**, **All Programs**, **Nortel**, **Contact Center, Communication Control Toolkit**, **CCT Console**.
3	Expand **NCCT Admin**.

4 In the left pane of the CCT 7.0 console, click **Logging Tools**.

5 In the right pane of the CCT 7.0 console, double-click **Logging**.

6 In the **Logging Properties** dialog box, click the **Server** tab.

7 Select the logging options you require.

8 In the **Server Logs Folder** box, click **Browse** to navigate to the new path for the log files.

9 In the **Server Logs File Size (in MB)** box, type the log file size.

10 In the **Number of Retained Log Files** box, type the number of log files to retain.

11 In the **Logging Properties** dialog box, click the **Connector** tab.

12 In the **Connector Logs Folder** box, click **Browse** to navigate to the new path for the log files.

13 In the **Connector Logs File Size (in MB)** box, type the log file size.

14 In the **Number of Retained Log Files** box, type the number of log files to retain.

15 In the **Logging Properties** dialog box, click the **Snap-in** tab.

16 In the **Snap-In Logs Folder** box, click **Browse** to navigate to the new path for the log files.

17 In the **Snap-in Log File Size (in MB)** box, type the log file size.

18 In the **Number of Retained Log Files** box, type the number of log files to retain.

19 In the **Logging Properties** dialog box, click the **Data Access Layer** tab.

20 In the **DAL Logs Folder** box, click **Browse** to navigate to the new path for the log files.

21 In the **DAL Log File Size (in MB)** box, type the log file size.

22 In the **Number of Retained Log Files** box, type the number of log files to retain.

23 In the **Logging Properties** dialog box, click the **TAPI SP** tab.

24 In the **Service Provider Logs Folder** box, click **Browse** to navigate to the new path for the log files.

25 In the **SP Log File Size (in MB)** box, type the log file size.

26 In the **Number of Retained Log Files** box, type the number of log files to retain.

27 In the **Logging Properties** dialog box, click the **SMON** tab.

28 In the **SMON Logs Folder**, click **Browse** to navigate to the new path for the log files.

29 In the **SMON Log File Size (in MB)** box, type the log file size.

30 In the **Number of Retained Log Files** box, type the number of log files to retain.

31 Click **Apply**.

32 Click **OK**.

--End--

Variable definitions

Variable	Value
Log File Size	The size of each log file in megabytes.
Number of Retained Log Files	The number of retained log files. The files are archived until all of the log files are full. The oldest log file is discarded and new log files are created.

Configuring the Communication Server 1000 service provider

Configure the Communication Server 1000 service provider details for the switch connection. As part of the service monitoring, the link to the switch is monitored for consistent connections.

Prerequisites

- Understand the server provider details for the switch.

Procedure steps

Step **Action**

1 Log on to the Communication Control Toolkit server.

2 Click **Start**, **All Programs**, **Nortel**, **Contact Center, Communication Control Toolkit**, **CCT Console**.

3 Expand **NCCT Admin**.

4 In the left pane of the CCT console, click **SP for CS1K**.

5 In the right pane of the CCT console, double-click **SP for CS1K**.

6 In the **SP for CS1K Properties** dialog box, in the **Application Name** box, type the application name.

7 In the **Timeout in Seconds** boxes, type the **Initialization**, **Shutdown** and **Command** timeout settings in seconds.

8 In the **Call Data** boxes, type the **Size (in bytes)** and **Life Span (in minutes)** for the call data.

9 Select or clear the **Disable copy of call data to consultative call** check box.

10 Select or clear the **Login Status Discovery** check box to update the agent status.

11 Click the **CS1K Host** tab.

12 Complete the host name information for your switch or server.

13 Click **Apply**.

14 Click **OK**.

--End--

Variable definitions

Variable	Value
Agent Status	Select the Login Status Discovery to ensure Communication Control Toolkit to query the switch for the login status of each agent address upon DN registration and accurately reflect the status of the corresponding terminals. This feature is supported on Switch Release 6.0 and later and with Contact Center Manager Server (CCMS) 7.0. Enabling this feature without the correct CCMS and switch version results in failed DN registration for each agent address.
Application Name	The Meridian Link Services application name. You can enter up to 19 ASCII characters to identify the provider application. If you enter more than 19 characters, Meridian Link Services cannot operate. You must enter a different name for each server that connects to Contact Center Manager Server.
Call data	Call data is the information attached to calls routed from the switch. The default size of the call data is 4 096 bytes. The Life Span default is 10 minutes. This value must be less than the time required to recycle the CS 1000/Meridian 1 Call IDs. Use the Disable copy of call data to consultative call check box to avoid copying call data during consultative calls, but you can copy call data when calls are transferred or conferenced.

Variable	Value
Customer Number	The number of the customer for the switch. If multiple customers are configured, you can specify a particular one in this box.
Host Address	The host address of the server where the host table is configured. In a contact center environment, the host address is the IP address of the Contact Center Manager Server. In a direct-connect or knowledge-worker environment, the host address is the IP address of the ELAN port on the Communication Server 1000/ Meridian 1 switch.
Host Name	The host name of the Contact Center Manager Server or CS 1000/ Meridian 1 switch. The host name is case-sensitive and contains a maximum of 20 characters. Nortel recommends that you keep the default setting.
Host Port	The host port of the server you use to store the host table. In a contact center environment, the default host port value is 3000. In a direct-connect or knowledge worker environment, the default host port is 8888.
Machine Name	The host name of the server you use to store the host table. In a contact center environment, the name is the name of the Contact Center Manager Server. In a direct-connect or knowledge worker environment, the name is the name of the switch.
Meridian Link Release	The release number of Meridian Link software.

Variable	Value
Polling Interval	The interval that the Meridian Link Services checks for connection between Contact Center Manager and Symposium TAPI SP. If you set a link value of 1, the link is polled every 10 seconds. You must configure a link value greater than 0 to ensure the link is maintained. Nortel recommends a link value of 1. The Polling interval can 0 to 100.
Timeout in Seconds	Initialization—The length of time that the service provider waits to establish communication with the switch before generating an error. The default and minimum value is 32 seconds. If you use a large number of lines, you must increase this value accordingly. Shutdown—The length of time the service provider waits for shutdown to complete before generating an error. The default value and minimum value is 32 seconds. Command—The length of time that the service provider waits for a command response before generating an error. The default and minimum value is 5 seconds.

Resource management

Use the Communication Control Toolkit Administration Console to manage the resources in the database. The resources are used to map the voice and multimedia contacts to terminals and to route them to agents in the contact center. You can configure the resources manually or automatically from an XML file using the Data Management Tool.

Prerequisites to resource management

- Understand the licensed features for your contact center. Specific resource or resource types may be excluded from your license package.

Navigation

Importing Windows users from the Communication Control Toolkit domain

Import Windows users from the Communication Control Toolkit server to the Communication Control Toolkit administration console. After the resources are in the administration console, you can configure the resources in your contact center.

Prerequisites

- Ensure that the local administrator has access to the Communication Control Toolkit that is installed.
- Know how to stop Communication Control Toolkit services.
- Know how to restart Communication Control Toolkit services.

Procedure steps

Step	Action
1	Log on to the Communication Control Toolkit server.
2	Click **Start**, **Administrative Tools**, **Services**.
3	Stop the **NCCT SMON** service to stop all of the services on the Communication Control Toolkit server.
4	Start the **NCCT Data Access Layer** service.
5	Close the **Services** window.
6	Click **Start, All Programs**, **Nortel**, **Contact Center, Communication Control Toolkit**, **CCT Console**.
7	Expand **NCCT Admin**.
8	In the left pane of the CCT 7.0 console, click **Import/Export Tools**.
9	In the right pane of the CCT 7.0 console, double-click **Import Windows Users**.
10	In the **Location** box, select the domain or server on which to look for Windows users.
11	In the **Object Type** box, select the group of users to display. You can look for all users, a particular user name, a last name, or a first name.
12	In the **Object Name** box, type the text you use to search for Windows Users.
13	Click **Find Now**.
14	In the **Search Results** box, select the Windows users to import. To select multiple users, press the **Ctrl** key while you select each user. To select all Windows users, click **Add All.**
15	Click **Add**.

16 Click **Apply**.

17 Click **OK**.

18 Start the **NCCT SMON** service to start all of the Communication Control Toolkit services.

--End--

Variable definitions

Variable	Value
Object name	The criteria for selecting a small group of Windows user accounts to import to the Communication Control Toolkit.
Object type	The type of Windows user accounts to import to the Communication Control Toolkit administration tool. You can choose one of the following options: • Find All Users—find all Windows user accounts on the CCT server. • User Name—find all Windows user accounts where the user name or logon ID matches or contains the value in the Object Name box. • Last Name—find all Windows user accounts where the last name matches or contains the value in the Object Name box. • First Name—find all Windows user accounts where the first name matches or contains the value in the Object Name box.

Importing address and terminal data from the switch

Import address and terminal data from the switch to eliminate the manual creation of database entries.

Do not use the Communication Control Toolkit server to import the information directly from the switch: Hyperterminal, when installed, interferes with the Telephony services and they remain running.

Prerequisites

- Connect a COM cable from a server (not the Communication Control Toolkit server) to the switch.

- Install Hyperterminal.
- Know the user ID and password to log on to the switch.
- Apply all patches, specifically patch MPLR26704. Patch MPLR26704 drastically reduces the time to import address and terminal information to the text file. Only information that is relevant to Communication Control Toolkit is imported.
- Know how to stop Communication Control Toolkit services.
- Know how to restart Communication Control Toolkit services.

Procedure steps

Step **Action**

1 Open a text editor.

2 Create a new text file called **download.txt**.

3 Save the download.txt file in the \Program Files\Nortel\CCT\TAPI\ directory on the Communication Control Toolkit server.

4 Click **Start**, **All Programs**, **Accessories**, **Communications**, **HyperTerminal** to connect to the CS 1000/Meridian1 switch from the Communication Control Toolkit server.

5 Type a name for the connection.

6 On the **Connect To** dialog box, in the **Connect using** list, select COM1 or the COM port connected to the CS 1000/Meridian 1 switch.

7 In the **COM1 properties** dialog box, confirm the information is correct.

8 Verify the information in this dialog box, and make necessary changes.

9 Click **OK**.

10 From the **Transfer** menu, select **Capture Text**.

11 At the prompt, type **logi** to log on to the switch.

12 Type your user ID and your password for the switch.

13 If the prompt is not present, continue to press **Enter** until the prompt appears.

14 Browse to the download.txt file that you created earlier, and then click **Start**.

15 Type the following commands in LD 20:

```
At the logon prompt, type LD 20, press Enter.
At the REQ: prompt, type PRT, press Enter.
At the TYPE: prompt, type TNB, press Enter.
At the TN: prompt, press Enter.
At the CDEN: prompt, press Enter.
At the CUST: prompt, type 0 (or the customer number),
press Enter.
```

```
At the DATE: prompt, press Enter.
At the PAGE: prompt, type ON, press Enter.
At the DES prompt, press Enter.
```

Downloading information from the CS 1000/Meridian 1 overlay can take a long time.

16 To return to the prompt, enter **** (Shift + 8888).

17 Press **Enter**.

18 Type the following commands in overlay 23:

```
At the prompt, type LD 23, press Enter.
At the REQ: prompt, type PRT, press Enter.
At the TYPE: prompt, type CDN, press Enter.
At the CUST: prompt, type 0 (or the customer number),
press Enter.
At the CDN prompt, press Enter.
```

The information is downloaded from the overlays

19 Type **logo**.

20 Press **Enter**.

21 Copy the text file capture to the Communication Control Toolkit server.

22 Log on to the Communication Control Toolkit server.

23 Stop the CCT TAPI SP, ACDProxy, CCT Server Service and TAPI Connector services.

24 Click **Start, All Programs**, **Nortel**, **Contact Center, Communication Control Toolkit**, **CCT Console**.

25 Expand **NCCT Admin**.

26 In the left pane of the CCT 7.0 console, click **Import/Export Tools**.

27 In the right pane of the CCT 7.0 console, double-click **Import Addresses & Terminals**.

28 Click **Browse** to find the text file you created in step 2.

29 Click **Apply**.

30 Click **OK**.

--End--

Variable definitions

Variable	Value
Connect using	The communications (COM) port that connects your server to the Communication Server 1000/ Meridian 1 switch.

Importing Contact Center users from Contact Center Manager Administration

Import Contact Center users from Contact Center Manager Administration to the Communication Control Toolkit administration tool using the Import Contact Center Users utility so you can configure the resources in your contact center.

Prerequisites

- Configure a user in Contact Center Manager Administration.
- Know how to stop Communication Control Toolkit services.
- Know how to restart Communication Control Toolkit services.
- Contact Management Framework (CMF) Replication must be enabled and working with Contact Center Manager Server.
- Ensure the following service is running on the Contact Center Manager Server: CCMS_OAMCMF_Service.

Procedure steps

Step	Action
1	Log on to the Communication Control Toolkit server.
2	Click **Start, Administrative Tools**, **Services**.
3	Stop the **NCCT SMON** service to stop all of the services on the Communication Control Toolkit server.
4	Start the **NCCT Data Access Layer** service.
5	Close the **Services** window.
6	Click **Start, All Programs**, **Nortel**, **Contact Center, Communication Control Toolkit**, **CCT Console**.
7	Expand **NCCT Admin**.
8	In the left pane of the CCT 7.0 console, click **Import/Export Tools**.

9 In the right pane of the CCT 7.0 console, double-click **Import Contact Center Users**.

10 Select a Contact Center user from the Available Contact Center User list and click **Add**

OR

Click **Add All** to import all available Contact Center users.

11 Click **OK**.

12 In the confirmation dialog box, click **OK**.

13 Start the **NCCT SMON** service to start all of the Communication Control Toolkit services.

--End--

Importing workstations from the local domain

Import workstations from the local domain to the Communication Control Toolkit administration tool using the Import Workstations tool so you can configure the resources in your contact center. If the Communication Control Toolkit server is in a workgroup on a stand-alone server, you do not have to import workstations.

Prerequisites

- Ensure that the local administrator has user access for the domain where Communication Control Toolkit is installed to access and import domain resources in the CCT Console.
- Know how to stop Communication Control Toolkit services.
- Know how to restart Communication Control Toolkit services.

Procedure steps

Step **Action**

1 Log on to the Communication Control Toolkit server.

2 Click **Start**, **Administrative Tools**, **Services**.

3 Stop the **NCCT SMON** service to stop all services on the Communication Control Toolkit server.

4 Start the **NCCT Data Access Layer** service.

5 Close the **Services** window.

6 Click **Start**, **All Programs**, **Nortel**, **Contact Center, Communication Control Toolkit**, **CCT Console**.

7 Expand **NCCT Admin**.

8 In the left pane of the CCT 7.0 console, click **Import/Export Tools**.

9 In the right pane of the CCT 7.0 console, double-click **Import Work Stations**.

10 Select the workstations to import from the **Available Work Stations** list.

11 Click **Add**.

12 Click **OK**.

13 Start the **NCCT SMON** service to start all of the Communication Control Toolkit services.

--End--

Adding resources manually

Manually add resources such as Windows users, Windows users groups, Terminal, Terminal groups, Addresses, Address groups and Contact Center Users (Agents), Contact Center user groups and Network IVR ports to organize your resources in the database. Use groups to arrange common single resources in your database into groups.

Prerequisites

- Know the name, properties, and mappings for the resource you are about to add to the database.

Procedure steps

Step **Action**

1 On the Communication Control Toolkit server, click **Start, All Programs, Nortel, Contact Center, Communication Control Toolkit, CCT Console**.

2 In the **CCT 7.0 Console** window, expand **NCCT Admin**.

3 Select the resource type to add.

4 Right-click and choose **New**.

5 On the first tab of the properties dialog box, in the **Name** box, type a unique name that you can easily recognize later.

6	If the new resource is a group, assign the individual resources to the group.
7	Add the mappings to the other resources according to the requirements of your contact center.
8	Click **OK**.

--End--

Changing the properties of a resource

Change the properties of a resource, such as the mapping or assigned group if the information for your contact center changes.

The address name cannot be changed. You must delete an existing address and add a new address to use a new address name.

Procedure steps

Step	Action
1	On the Communication Control Toolkit server, click **Start, All Programs, Nortel, Communication Control Toolkit, CCT Console**.
2	In the **NCCT 7.0 Console** window, expand **NCCT Admin**.
3	On the left pane of the Console window, click the resource type to change.
4	From the list of resources in the right pane of the Console window, double-click the resource to change.
5	Make the changes to the mapping, name or assigned group using the tabs on the **Properties** dialog box.
6	Click **OK**.

--End--

Mapping resources

Map resources to each other in the Communication Control Toolkit administration tool to associate the resources with groups or other resource types.

Procedure steps

Step	Action
1	Log on to the Communication Control Toolkit server.
2	Click **Start, All Programs**, **Nortel**, **Contact Center, Communication Control Toolkit**, **CCT Console**.
3	Expand **NCCT Admin**.
4	In the left pane of the CCT 7.0 console, click the name of the resource to map.
5	In the right pane of the CCT 7.0 console, double-click the single resource to configure.
6	Click the tab that represents the resource to which you want to map the current resource.
7	Select the appropriate resource and resource groups from those in the **Available** column. Press **CTRL** and click users to select more than one user or user group.
8	Click **Add** to move the selected resource and resource groups to the **Mapped** column.
9	Click **OK**.

--End--

Example of mapping resources

Step	Action
1	Log on to the Communication Control Toolkit server.
2	Click **Start, All Programs**, **Nortel**, **Contact Center, Communication Control Toolkit**, **CCT Console**.
3	Expand **NCCT Admin**.
4	In the left pane of the CCT 7.0 console, click **Contact Center Users**.
5	Double-click the User to configure.
6	Click the **User Maps** tab.

7 Select the appropriate Users and User groups from those in the **Available Users and User Groups** column.

Press **CTRL** and click users to select more than one user or user group.

8 Click **Add** to move the selected Users and User groups to the **Mapped Users and User Groups** column.

9 Click **OK**.

The Users or User groups map to a Windows user, and the Windows user maps to the Users and User groups. You can verify the mappings in the User properties window, on the User Maps tab.

--End--

Unmapping resources

Unmap resources in your Communication Control Toolkit to remove the association between the resources to groups or other types of resources to delete resources efficiently.

Procedure steps

Step **Action**

1 Log on to the Communication Control Toolkit server.

2 Click **Start, All Programs**, **Nortel**, **Contact Center, Communication Control Toolkit**, **CCT Console**.

3 Expand **NCCT Admin**.

4 In the left pane of the CCT 7.0 console, click the name for the resource to remove mappings.

5 In the right pane of the CCT 7.0 console, double-click the single resource name.

6 Click the tab that represents the resource to which you want to unmap from the current resource.

7 Select the appropriate resource and resource groups from those in the **Mapped** column.

Press **CTRL** and click users to select more than one user or user group.

8 Click **Remove** to move the selected resource and resource groups to the **Available** column.

9 Click **OK**.

--End--

Deleting resources

Delete resources from your Communication Control Toolkit database that you no longer require to save space. You can remove groups or individual resources.

Procedure steps

Step	Action
1	On the Communication Control Toolkit server, click **Start, All Programs, Nortel, Contact Center, Communication Control toolkit, CCT 7.0 Console**.
2	Expand **NCCT Admin**.
3	Select the resource type to delete.
4	From the list of resources in the right pane of the Console window, select the resource to delete.
5	Right-click, and click **Delete**.
6	In the confirmation message dialog box, click **Yes**.

--End--

Variable definitions

Variable	Definition
Resource type	The type of resource (Windows user, Contact Center user, user groups, Terminal, Address, or Workstation to remove.

Importing bulk resources

Import bulk resources into the Communication Control Toolkit database from a CSV file, or a file that has delimited data format that separates fields or columns by a specific character to save time.

If the data exists in the database, new data is not inserted during the import.

Prerequisites

- Ensure that you have a CSV file that matches the required file format to import the resources to the Communication Control Toolkit database.

Procedure steps

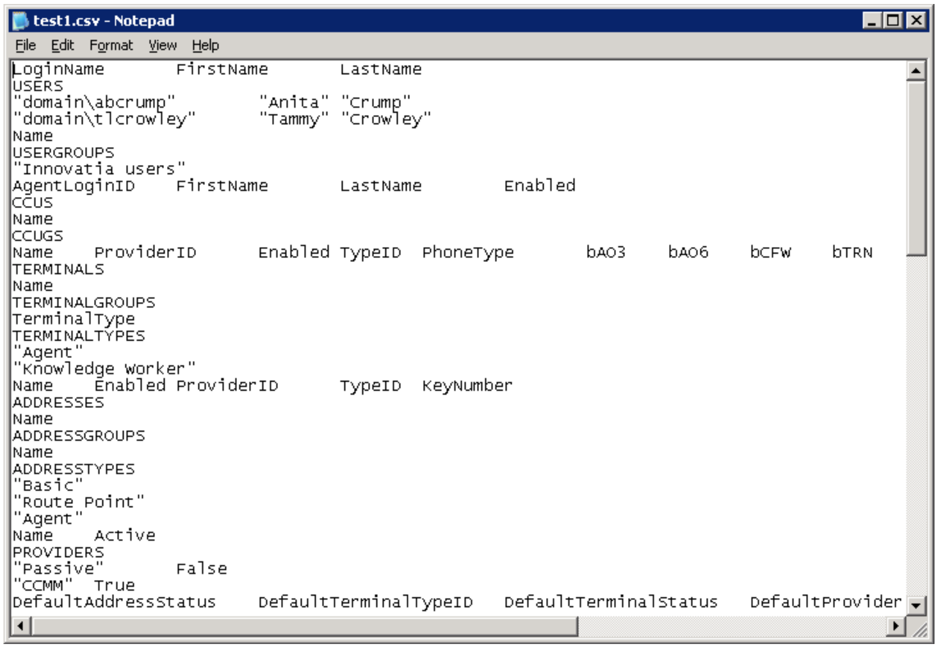
Step	Action
1	On the Communication Control Toolkit server, click **Start, All Programs, Nortel, Contact Center, Communication Control Toolkit, CCT Console**.
2	In the **CCT 7.0 Console** window, expand **NCCT Admin**.
3	Click **Import/Export Tools**.
4	In the right pane of the NCCT 7.0 Console window, double-click **Import Configuration**.
5	On the **Import Configuration Properties** dialog box, click **Import**.
6	In the **Open** box, navigate to the file to import.
7	Click **Open**.
8	When the import is complete, click **OK**.
9	Click **OK** to close the **Import Configuration Properties** dialog box.

--End--

Procedure job aid

The following image shows a sample text file for importing bulk resources into the Communication Control Toolkit database.

Sample text file for importing



```
LoginName       FirstName       LastName
USERS
"domain\abcrump"        "Anita" "Crump"
"domain\tlcrowley"      "Tammy" "Crowley"
Name
USERGROUPS
"Innovatia users"
AgentLoginID    FirstName       LastName        Enabled
CCUS
Name
CCUGS
Name    ProviderID      Enabled TypeID  PhoneType       bAO3    bAO6    bCFW    bTRN
TERMINALS
Name
TERMINALGROUPS
TerminalType
TERMINALTYPES
"Agent"
"Knowledge Worker"
Name    Enabled ProviderID      TypeID  KeyNumber
ADDRESSES
Name
ADDRESSGROUPS
Name
ADDRESSTYPES
"Basic"
"Route Point"
"Agent"
Name    Active
PROVIDERS
"Passive"       False
"CCMM"  True
DefaultAddressStatus    DefaultTerminalTypeID   DefaultTerminalStatus   DefaultProvider
```

Exporting resource configuration to a CSV file

For data analysis, export resource configuration data and the data mappings to a single file or a file for each resource by using the build resource configuration tool.

Procedure steps

Step	Action
1	On the Communication Control Toolkit server, click **Start, All Programs, Nortel, Contact Center, Communication Control Toolkit, CCT Console**.
2	In the **CCT 7.0 Console** window, expand **NCCT Admin**.
3	Click **Import/Export Tools**.
4	In the right pane of the NCCT 7.0 Console window, double-click **Export Configuration**.
5	In the **Export Configuration Properties** dialog box, select the Mappings, Resources, and System Information to include in the data file.
6	Under **Export File Format**, select **XML** to change the default format.
7	Under **Export File Mode**, select the format in which to export data.
8	Click **OK**.

--End--

Variable definitions

Variable	Value
Mappings	The mappings recorded in the Communication Control Toolkit database between users, terminals, address, contact center users, user groups, terminal groups, address groups and contact center groups. You can choose all mappings or individual mappings by selecting the appropriate check boxes under Mappings.
Resources	The resources recorded in the Communication Control Toolkit database such as users, terminals, address, contact center users, workstations, user groups, terminal groups, address groups and contact center groups. You can choose all resources or individual resources by selecting the appropriate check boxes under Resources.
System Information	The system information recorded in the Communication Control Toolkit database includes information about types of providers, terminals, addresses, phones and default values. You can choose to import all system information or individual data components by selecting the appropriate check boxes under System Information.
Export File Format	The final output of the exported data. You can choose from two formats: • TAB: a text file containing data separated by spaces • XML; a text file containing data separated by XML tags
Export File Mode	The number of files that your Communication Control Toolkit data to which your data is exported: • a single file • multiple files, one for each resource type

Contact Center Multimedia

Contact Center Multimedia fundamentals

Use the contact Center Multimedia server to allow the contact center to accept e-mail messages, outbound contacts, and contacts through a Web page interface and instant messaging.

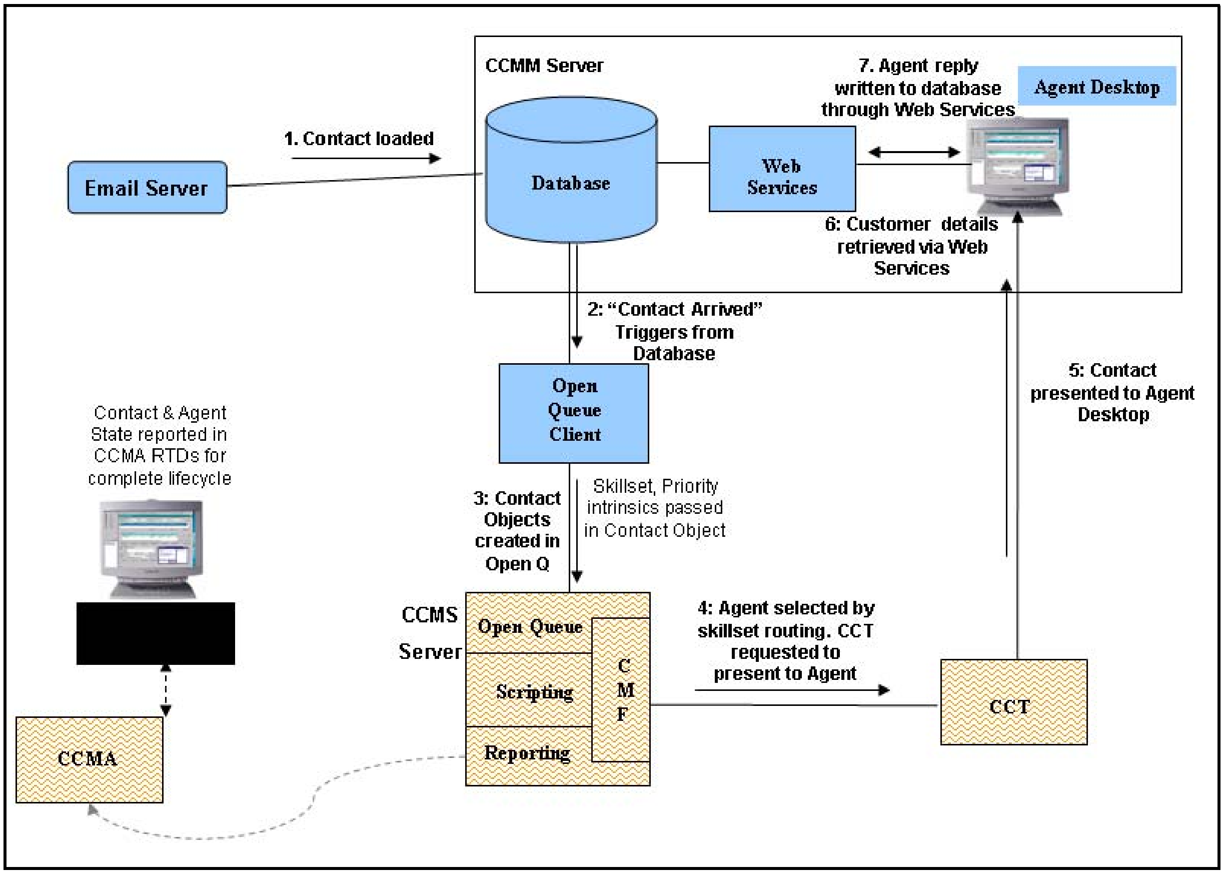
For information about supported languages, see *Nortel Contact Center Planning and Engineering* (NN44400-210).

Navigation

E-mail contact type

The e-mail contact type is a licensed feature of Contact Center Multimedia. You can use e-mail to communicate with clients using an e-mail provider such as Microsoft exchange.

E-mail contact lifecycle


CCMM Server
7. Agent reply written to database through Web Services
Agent Desktop
1. Contact loaded
Email Server
Database
Web Services
6: Customer details retrieved via Web Services
2: "Contact Arrived" Triggers from Database
5: Contact presented to Agent Desktop
Open Queue Client
Contact & Agent State reported in CCMA RTDs for complete lifecycle
[redacted]
3: Contact Objects created in Open Q
Skillset, Priority intrinsics passed in Contact Object
CCMS Server
Open Queue
Scripting
Reporting
C M F
4: Agent selected by skillset routing. CCT requested to present to Agent
CCT
CCMA

E-mail contacts require configuration for routing contacts with specific information and an appropriate language using rules. You can configure the rules to route the contact, based on the content of the incoming e-mail message and the recipient address, to a skillset, and thus an agent who can handle contacts for that skillset. You can use rules to provide automatic assistance to the sender using an automatic response.

The e-mail contact type has several components:

- E-mail rules (page 328)
- Recipient mailboxes (page 328)
- Inbound e-mail settings (page 328)

You must configure e-mail settings for e-mail leaving your contact center as a campaign, or in response to customer e-mail messages.

- Outbound e-mail settings (page 329)
- Encoding for outgoing e-mail (page 329)

The e-mail message contact type also requires specific information to configure for international languages, see Asian e-mail (page 329).

E-mail rules

Rules determine how a multimedia contact is to be routed based on information about the e-mail message (input) and configurations in your contact center (output).

A basic rule considers the first recipient address of the contact and can assign a skillset. You can further enhance the routing by searching for specific keywords in the body of an e-mail or by looking at who sent the message (sender address). You can also enhance the routing by selecting additional output details for your contact center, such as automatic responses. You can configure a maximum of 1 000 rules.

If an e-mail message is sent to more than one recipient address, only the first rule that matches the recipient list runs. The automatic responses and skillset assignment for the e-mail is based on the first matched recipient address. Configuring additional rules is optional.

Example 1: A magazine advertises an investment strategy. Customers can learn more about the investment by sending an e-mail with “Good Investing” in the subject line to a specific address. Create a rule to search incoming e-mail messages for “Good Investing.” If the e-mail subject line contains “Good Investing,” then a brochure is sent to the customer. No interaction from an agent is required.

Recipient mailboxes

Contact Center Multimedia polls specific recipient mailboxes on the e-mail server based on a list of mailboxes defined in the Multimedia Administrator recipients list. The e-mail retrieved from these mailboxes is routed based on defined rules applied to either enabled or alias mailboxes. You must ensure that enabled e-mail addresses you configure in the Email Manager are already configured on your corporate e-mail server.

Inbound e-mail settings

Perform this optional configuration if you are licensed for e-mail contacts.

You can configure optional e-mail settings:

- how frequently you scan the e-mail server for new messages
- where the attachments are stored
- the text searched when you use keywords for rules

Outbound e-mail settings

Configure outgoing e-mail mailbox settings to identify who is responding to the customer’s e-mail message. For outgoing e-mail, you can also change the encoding of the message.

The response can contain the e-mail address to which the customer sent the original e-mail message, or a general corporate e-mail address that is configured for each skillset. Agent-initiated messages are always sent from an e-mail address associated with a skillset.

Note: E-mail messages must be relayed through the e-mail server, not forwarded to another party if managing e-mail messages on behalf of an external source. Sending e-mail messages preserves the original To address which is used for e-mail rule administration and outgoing e-mail addresses.

Encoding for outgoing e-mail

The Contact Center Multimedia Email Manager replies to an e-mail message using the same characters as the inbound e-mail. For example, if an e-mail arrives to the contact center with Latin-1 encoding, the reply from the agent desktop or the automatic response is sent in Latin-1. The customer e-mail client can understand the format of the message sent from the contact center.

If the customer sends an e-mail in English and receives either an agent response or an automatic response in another character set, you have no way to know if the customer e-mail client can decode the new character set. Nortel recommends that if you use an automatic response, you use rules to search for words in the expected languages (for example, Japanese or English) to ensure that the response sent matches the language of the inbound e-mail.

If the original e-mail is encoded with the Latin-1 characterset (ISO-8859-1), you can choose to reply in Latin-9 character set (ISO-8859-15) to provide support for the Euro Currency Symbol. The Euro Currency Symbol is not included in the Latin-1 character set, instead, it is represented by a question mark (?). Not all recipients understand the Latin-9 character set, and the reply e-mail can be perceived as a blank e-mail. Nortel recommends that only contact centers in Europe use Latin-9 encoding.

Asian e-mail

Internationalized domain names (IDN) can include characters from East Asian languages. Using the characters from East Asian languages is dangerous because of phishing sites. A phishing site is an e-mail message with a link to www.aib.ie can point you to a site that has the i and a b in the domain but some other character that resembles an a.

The World Wide Web Consortium uses punycode to implement IDNs. Punycode is an ASCII equivalent to the domain name. Normally, the client (Web browser or e-mail client) accepts the IDN in native characters and converts it to punycode; for example, xn--jp-cd2fp15c@xn--fsq.com. The receiving client identifies the sender as being a punycode string and interpret the native characters.

Contact Center Multimedia supports IDNs. You or a customer can enter a punycode e-mail address. The receiving client can render the native characters.

Not all Administrator controls are Unicode-aware. The following controls do not accept Asian characters:

- Auto-Responses: Attachment file name
- Skillset Settings: Auto-signature Template file name
- Rule Precedence: Exported rules file name
- Certain error dialog boxes, which can render Asian characters as question marks

For Auto-Response attachments, Auto-signature templates, Exported rules, the name of the file must be in English when it is configured in the Administrator; however, the content of the files can contain Asian characters.

Contact Center Agent Desktop

Agents use Contact Center Agent Desktop to process e-mail contacts. When an e-mail arrives at the contact center, contacts are routed to Agent Desktop, and agents can perform the following activities:

- Accept or reject an e-mail message.
- Review and update customer information.
- Create a reply.
- Select a activity code to record the result of the customer contact.

For more information about Contact Center Agent Desktop, see the *Nortel Contact Center Agent Desktop User Guide* (NN44400-114).

Contact Center Manager Administration

Use Real-Time Reporting and Historical Reporting in Contact Center Manager Administration to create and run real-time and historical reports for campaigns.

For more information about the reporting and performance statistics, see the following documents:

- *Nortel Contact Center Performance Management Data Dictionary* (NN44400-117)
- *Nortel Contact Center Performance Management* (NN44400-710)
- *Nortel Contact Center Manager Administration – Client Administration* (NN44400-611)

Real-Time Reporting displays real-time and up-to-date statistics information regarding a campaign, such as the number of waiting contacts, the number of answered contacts, or the average answer delay.

Web services

The Open Interfaces provide Web services for integrating third-party agent applications with the Contact Center Multimedia server for the processing of e-mail contacts received into monitored mailboxes.

The Web services provide the following functions for external applications:

- Agent authentication with CCMM Database
- Ability to Read Email Contacts
- Ability to Reply to and Forward e-mail contacts

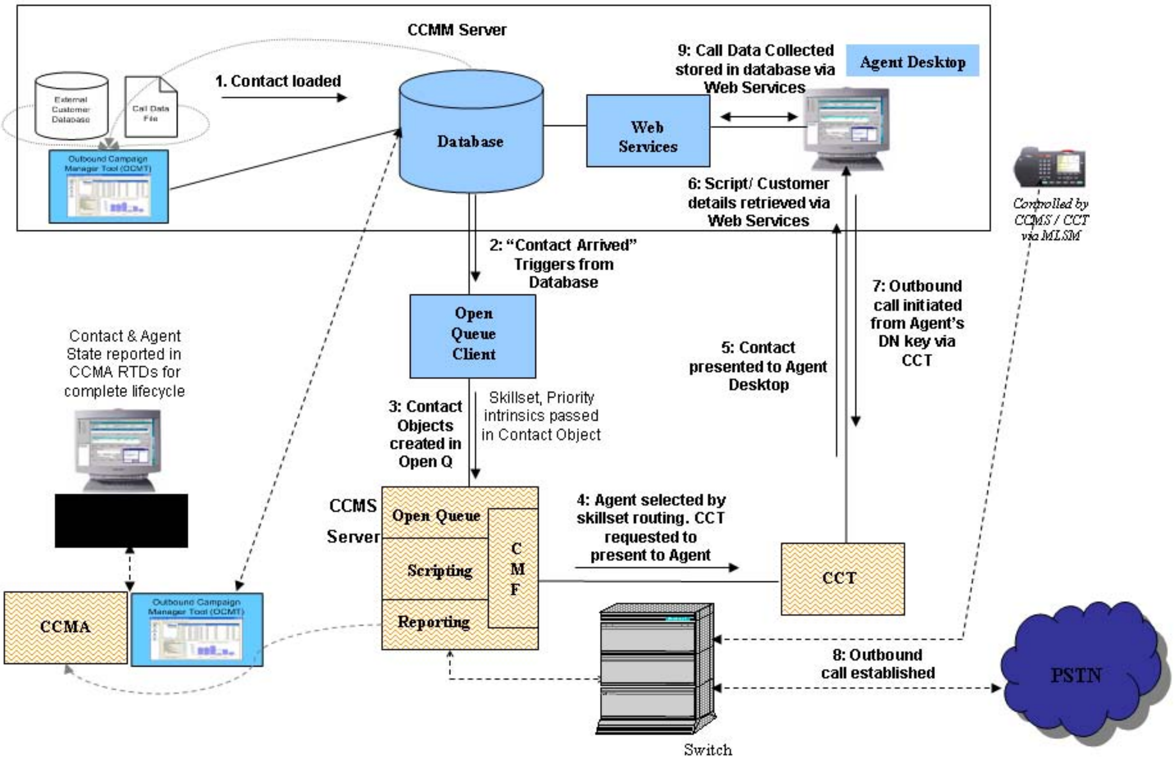
For more details, see the SDK documentation.

Outbound contact type

The outbound contact type is an outgoing call made by agents to customers for sales or marketing.

The following figure shows how outbound contacts interact with Contact Center Manager Administration, Contact Center Multimedia, and Contact Center Manager Server.

Outbound contact type routing


CCMM Server
1. Contact loaded
External Customer Database
Call Data File
Outbound Campaign Manager Tool (OCMT)
Database
Web Services
9: Call Data Collected stored in database via Web Services
Agent Desktop
6: Script/ Customer details retrieved via Web Services
Controlled by CCMS / CCT via MLSM
2: "Contact Arrived" Triggers from Database
Open Queue Client
Contact & Agent State reported in CCMA RTDs for complete lifecycle
3: Contact Objects created in Open Q
Skillset, Priority intrinsics passed in Contact Object
5: Contact presented to Agent Desktop
7: Outbound call initiated from Agent's DN key via CCT
CCMS Server
Open Queue
Scripting
Reporting
C M F
4: Agent selected by skillset routing. CCT requested to present to Agent
CCT
CCMA
Outbound Campaign Manager Tool (OCMT)
8: Outbound call established
PSTN
Switch

The Outbound Campaign Management Tool is not available in a SIP-enabled contact center.

Contact Center Outbound consists of several components:

- Outbound Campaign Management Tool (page 332)
- Campaign Scheduler (page 333)
- Contact Center Agent Desktop (page 333)
- Contact Center Manager Administration (page 334)

Outbound Campaign Management Tool

Use the Outbound Campaign Management Tool in Contact Center Manager Administration to create, modify, and monitor outbound campaigns. You can configure a maximum of 100 simultaneous outbound campaigns with 20 000 contacts in each campaign.

A contact center administrator or supervisor can use the Outbound Campaign Management Tool to create and monitor outbound campaigns. The Outbound Campaign Management Tool provides the following main functions:

- Define a campaign.

- Import call data.
- Create disposition codes.
- Review outbound call data.
- Create and preview optional agent scripts.
- Review campaign progress.

Campaign Scheduler

This Contact Center Multimedia server component determines when to queue contacts to the Contact Center Manager Server. The Campaign Scheduler monitors the status of each campaign and performs the following actions:

- Assigns the campaign status to running and queues contacts to Contact Center Manager Server when the campaign start time or daily start time occurs.
- Assigns the campaign status to nonrunning and removes contacts from Contact Center Manager Server when the daily end time occurs.
- Assigns the campaign status to expired and removes contacts from Contact Center Manager Server when the daily end time occurs.
- Assigns the campaign status to completed when all contacts are processed.

Contacts are queued to Contact Center Manager Server at the configured rate. By default, the Campaign Scheduler presents outbound contacts every 60 seconds. Use the Campaign Scheduler Configuration window in the Contact Center Multimedia Administrator to change the interval length.

Contact Center Agent Desktop

Agents use Contact Center Agent Desktop to process outbound contacts. When a campaign runs, outbound contacts are routed to Agent Desktop, and agents can perform the following activities:

- Accept or reject an outbound contact.
- Review and update customer information.
- Make the outbound voice call.
- Follow an agent script and record customers answers and comments.
- Select a disposition code to record the result of the call.

For more information about Contact Center Agent Desktop, seethe *Nortel Contact Center Agent Desktop User Guide* (<Doc Number>).

Contact Center Manager Administration

Use Real-Time Reporting and Historical Reporting in Contact Center Manager Administration to create and run real-time and historical reports for campaigns.

Real-Time Reporting displays real-time and up-to-date statistics information regarding a campaign, such as the number of waiting contacts, the number of answered contacts, or the average answer delay.

Web services

The Outbound Open Interfaces provide an open interface for integrating third-party applications with Outbound Campaigns

The open interfaces provide the following functions for external applications:

- ability to add contacts to an existing campaign
- ability to close contacts already created as part of a campaign

The most common use of these interfaces is to automatically load a caller list to an existing outbound campaign.

For more details, see the SDK documentation.

Web communications

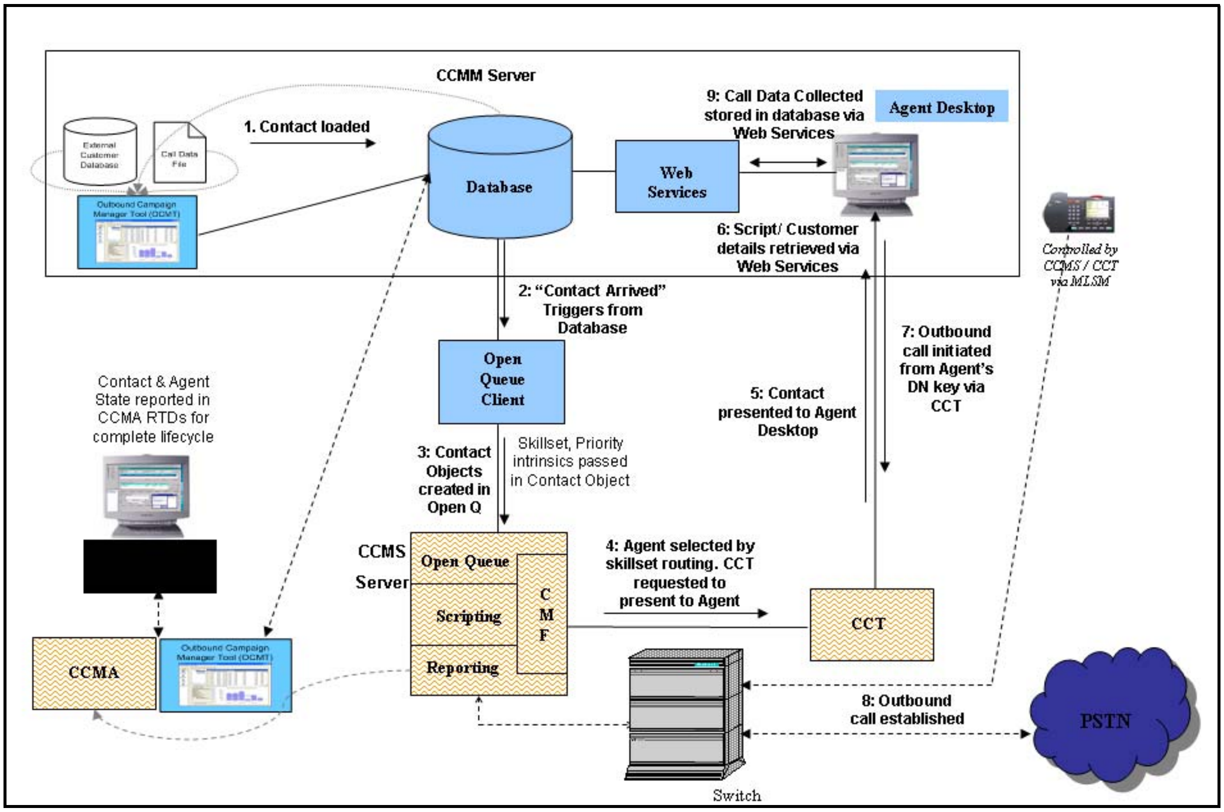
Use the Web Communications Manager to communicate with customers over the Internet. Agents and customers directly communicate in real time by conducting a two-way conversation by exchanging text messages using Javascript- and frame-compliant Web browsers. The Web Communications Manager provides the following functions:

- intelligent routing of customer communications to the agent who has the subject knowledge to respond
- an Agent Desktop interface for agents to respond efficiently to customers
- easy referencing of the thread of conversation between the customer and the agent in a text chat session
- an optional customer-centered multimedia presentation to the customer’s browser while the customer waits for an agent
- push Web pages to the other party during conversations for discussions

You must configure the skillset and configure the Web server to configure the Web Communications Manager.

The following figure shows how outbound contacts interact with Contact Center Manager Administration, Contact Center Multimedia, and Contact Center Manager Server.

Web communications lifecycle


CCMM Server
External Customer Database
Call Data File
Outbound Campaign Manager Tool (OCMT)
1. Contact loaded
Database
Web Services
9: Call Data Collected stored in database via Web Services
Agent Desktop
6: Script/ Customer details retrieved via Web Services
Controlled by CCMS / CCT via MLSM
2: "Contact Arrived" Triggers from Database
Open Queue Client
7: Outbound call initiated from Agent's DN key via CCT
5: Contact presented to Agent Desktop
Contact & Agent State reported in CCMA RTDs for complete lifecycle
3: Contact Objects created in Open Q
Skillset, Priority intrinsics passed in Contact Object
[redacted]
CCMS Server
Open Queue
Scripting
Reporting
C M F
4: Agent selected by skillset routing. CCT requested to present to Agent
CCT
CCMA
Outbound Campaign Manager Tool (OCMT)
8: Outbound call established
PSTN
Switch

Instant Messaging

The automatic text for an instant message communication includes a welcome message for customers who initiate a session, and a disconnect message for the customer in the text-based conversation. You can configure default instant messages for individual skillsets.

Maximum attachment size formula

The maximum attachment size formulas use the following variables and the approximate values for these variables, used when calculating how much memory to reserve to process an e-mail message.

Variable	Description	Value
Encoding adjustment	The factor by which the attachment size increases when the attachment is encoded and attached to an e-mail message.	1.3 (this can vary slightly based on the encoding used)
Memory adjustment	The factor by which the encoded size increases when an e-mail message is loaded into the internal representation of the e-mail message in memory.	1.2 (this factor decreases slightly, the larger the e-mail is, but it has been left as a fixed value)
Buffer memory	The memory required by the parts of the application not involved in processing inbound e-mail messages, which is fairly static.	20 MB

When the following sections specify an attachment size, they mean the total size of all attachments of an e-mail message. Also, the size of the body of an e-mail lowers the supported attachment size by the size of the content of the message. In most cases, the content of an e-mail is negligible compared to large attachments.

JVM size – Buffer memory / Memory adjustment / Encoding adjustment = Maximum attachment size

JVM sizes (MB)	Maximum attachment sizes (MB)
128	69.2
256 (default)	151.3
512	315.4
1024	643.6

Minimum JVM size formula

Attachment size * Encoding adjustment * Memory adjustment + Buffer memory = Minimum JVM size

Attachment sizes (MB)	Minimum JVM sizes (MB)
10	35.6
20	51.2
30	66.8
40	82.4
50	98
60	113.6
70	129.2
80	144.8
90	160.4
100	176
500	800

CCMM Dashboard utility

Use the CCMM Dashboard utility to perform of one of the following tasks:

- Monitor the number of contacts for optimum performance
- Troubleshoot contact routing errors

Outbound configuration

To create, monitor, and add data to an outbound campaign, use the Outbound Campaign Management Tool. You can configure a maximum of 100 simultaneous outbound campaigns with 20 000 contacts in each campaign.

You must use the Multimedia Administration tool to configure how contacts are routed to a particular contact type, and thus to an agent. The data maintained about Outbound contacts are saved in the Contact Center Multimedia database. This chapter discusses the outbound settings required to manage outbound campaigns in the Multimedia database.

Prerequisites for Outbound configuration

- Ensure that you are licensed for Outbound contacts in your contact center.
- Outbound skillsets are configured in the Contact Center Manager Administration.
- Ensure that the route points (DN) are configured in Contact Center Manager Administration.
- Log on to the Contact Center Multimedia Administrator application.

Navigation

- Configuring a route point for an Outbound skillset (page 338)
- Configuring the outbound scheduler (page 339)

Configuring a route point for an Outbound skillset

Configure a route point for an outbound skillset to route outbound contacts to a particular direction. Skillsets are used to assign the contacts to agents.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** application, expand **Contact Center Multimedia**.
2	Expand **General Administration**.
3	Double-click **Skillset Settings**.
4	In the **Skillset Settings** dialog box, select the skillset for which to assign a route point. The skillset must have the prefix OB.
5	Click **Edit**.
6	In the **Edit Skillset** dialog box, in the **Route Point** list, select the route point to assign to the outbound skillset.
7	Click **Save**.
8	After all skillsets with the prefix OB are configured with route points, click **Close**.

--End--

Variable definitions

Variable	Value
Route point	A location on the open queue that enables incoming calls to be queued and run through a script on the Contact Center Manager Server.

Configuring the outbound scheduler

Configure the global setting for the length of time you want the outbound scheduler to wait between presenting outbound contacts to the Contact Center Manager Server.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** application, expand **Contact Center Multimedia**.

2 Expand **Outbound Administration**.

3 Double-click **Outbound Scheduler Configuration**.

4 In the **Sleep Duration** box, type the number of hours and minutes to wait between presenting outbound contacts to the Contact Center Manager Server.

5 Click **Save**.

--End--

Variable definitions

Variable	Value
Sleep duration	The number of hours and minutes to wait between presenting outbound contacts to the Contact Center Manager Server.

E-mail configuration

E-mail configuration requires many components in Contact Center Multimedia.

You must configure e-mail server names to ensure that e-mail messages arrive at the contact center Multimedia server and can be sent from the server.

You must configure the properties of the routing for e-mail messages by configuring skillsets and the associated route points for routing e-mail messages to the appropriate agents.

You must configure e-mail rules that designate how each e-mail message is assigned to each skillset based on information in the content of the message, to address, and the from address. You can configure the selection criteria in addition to the rules.

You can configure general e-mail settings to minimize space and format special characters for other languages.

Prerequisites for e-mail configuration

- Ensure that you are licensed for e-mail contacts.
- Log on to the Contact Center Multimedia Administrator.

Navigation

E-mail server names configuration

- Configuring the e-mail server names (page 343)
- Adding an e-mail server (page 344)
- Deleting an e-mail server (page 345)

E-mail skillset configuration

- Configuring skillsets for e-mail (page 346)
- Adding an auto-signature to a skillset (page 347)

E-mail rules configuration

E-mail selection criteria configuration

- Creating or changing a recipient (page 378)
- Deleting a recipient mailbox (page 350)
- Configuring holidays (page 380)
- Configuring office hours (page 381)

Other E-mail

- Enabling SSL on the Email Manager (page 381)
- Enabling SMTP Authentication on your e-mail server (page 384)
- Determining if SMTP Authentication is enabled (page 384)

Configuring the e-mail server names

Configure the e-mail server names to identify the inbound server (POP3) for e-mail messages received by the contact center and the outbound server (SMTP) for e-mail messages sent by the contact center.

If you configured the e-mail servers during installation, and the names of the inbound and outbound e-mail servers remain unchanged, you can skip this procedure.

You can configure secondary inbound and outbound e-mail servers. If a failure of the primary e-mail server occurs, the e-mail retrieved during the failure of the primary server is duplicated in the Multimedia database when you restore the primary server.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator**, expand **Contact Center Multimedia**.
2	Expand **General Administration**.
3	Double-click **Server Settings**.
4	In the **Server Settings** window, double-click **Inbound Mail Server (POP3)**.
5	In the **Primary Hostname** box, type the name of the server that receives e-mail messages.
6	In the **Server Type** box, select **POP3** for inbound e-mail servers. **OR**

Select **SMTP** for outbound e-mail servers.

7 In the **Port Number** box, type the port number for the e-mail server.

8 If you have a backup e-mail server, in the **Secondary Hostname** box, provide a host name for the backup server.

9 Select the SMTP authentication, if required, for your outbound e-mail server.

10 Click **Save**.

--End--

Variable definitions

Variable	Value
Port Number	Port number for the e-mail server.
Primary Hostname	The name of the server that receives e-mail messages.
Secondary Hostname	Name of a secondary e-mail server, if one is available in your contact center.
Server Type	The type of server for inbound and outbound e-mail messages. Use POP3 for inbound and SMTP for outbound e-mail servers.

Adding an e-mail server

Add or update the e-mail server for your Contact Center Multimedia server to You can poll multiple e-mail servers in your contact center for e-mail messages to be routed. You can retrieve e-mail messages for the contact center only if you are licensed to use the e-mail feature.

Prerequisites

- Know the name of the e-mail server you want to add.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator**, expand Contact Center Multimedia.

2 Expand **General Administration**.

3 Double-click **Server Settings**.

4 Click **New Server**.

5 In the **Primary Hostname** box, type the host name of the e-mail server you want to add.

6 In the **Server Type** box, choose either POP3 or SMTP as your server type.

7 In the **Port Number** box, type the port number for the e-mail server to add.

8 In the **Secondary Hostname** box, type the host name for your alternative secondary e-mail server.

9 In the **SMTP Authentication** box, select the SMTP Authentication, if required.

10 Click **Save**.

11 Click **Close**.

--End--

Deleting an e-mail server

You can delete an e-mail server or other non-essential server only if the server is no longer required.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator**, expand **Contact Center Multimedia**.
2	Expand **General Administration**.
3	Double-click **Server Settings**.
4	Select the sever you want to delete.
5	Click **Delete**.
6	Click **OK** to confirm the deletion.
7	Click **Close**.

--End--

Configuring skillsets for e-mail

Configure a route point for each skillset, and to use the skillsets in rules.

An auto-signature is text automatically added at the bottom of an outgoing message. For example, you can encourage customers to visit your customer support Web site by adding the URL and other promotional information or disclaimer text to every message.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** application, expand **Contact Center Multimedia**.
2	Expand **General Administration**.
3	Double-click **Skillset Settings**.
4	Select a skillset for which to assign a route point.
5	Click **Edit**.
6	From the **Route Point** list, select the route point to assign to the skillset.
7	If applicable, type an auto-signature for the skillset.
8	Click **Save**.
9	When all skillsets are configured, click **Close**.

--End--

Adding an auto-signature to a skillset

You must use the Multimedia Administrator application to configure a route point for a skillset. You cannot change other skillset properties.

To change the name of the skillset, use Contact Center Manager Administration.

A route point is a location on the open queue that enables incoming calls to be queued and run through a script on the Contact Center Manager Server.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **General Administration**.
3	Double-click **Skillset Settings**.
4	Select a skillset, and then click **Edit**.
5	In **Auto Signature** dialog box, type the signature to assign to the skillset.
6	Click **Save**.
7	Click **Close**.

--End--

Creating a recipient mailbox

Create a recipient e-mail box to ensure that at least one e-mail box is configured for your contact center. You must configure one e-mail box to allow Contact Center to poll a mailbox on the e-mail server and handle contacts appropriately within the enabled or aliased address.

Prerequisites

- Ensure that any enabled e-mail address you want to configure in the Email Manager is already configured on your corporate e-mail server.
- Understand the difference between an alias and an enabled e-mail box.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Email Administration**.
3	Double-click **Recipient Addresses**.
4	Click **New**.
5	On the New Recipient window, in the **Mailbox Name** box, type the name of a mailbox set up on the e-mail server.
6	In the **Email Domain** box, type the domain for your e-mail server.
7	In the **Password** box, enter the password for the mailbox.

Attention: When you change a password on the e-mail server, you must update this password in the Multimedia Administrator.

8	In the **Confirm** box, type the same password you typed in the **Password** box.
9	In the **Display Name** box, type the name to appear in the e-mail From address.
10	In the **POP3 Server** box, ensure that the host name of your POP3 server appears.
11	In the **SMTP Server** box, ensure that the host name of your SMTP server appears.
12	Select **Enabled** or **Alias** to configure this mailbox.
13	In the **Process Up to** box, enter the maximum number of e-mail messages to be retrieved from the mailbox every scan interval. You can enter a different value for this variable for each mailbox. The default value is 10.
14	Select the **Use alternative username for SMTP Authentication** box if you are configuring an inbox as an alias. If SMTP authentication is enabled on your e-mail server, and you use aliases, log on to the SMTP server with a different user name.
15	In the **Username** box, type the SMTP server logon name.
16	Click **Save**.

--End--

Variable definitions

Variable	Value
Alias	An alias is an address that forwards all e-mail messages it receives to another e-mail account. For example, the mailbox general@magscripts.com can have the aliases carz@magsubscriptions.com and planez@magsubscriptions.com. E-mail messages addressed to either of these aliases are forwarded to the general@magscripts.com mailbox. The Email Manager routes the e-mail messages according to the rules based on the alias mailboxes. Aliases can be useful to filter e-mail messages. For example, you can define an alias for a short promotional period after which e-mail messages that arrive at that alias are discarded.
Display Name	The name to appear in the e-mail From address. For example, Sales Department.
E-mail Domain	The domain name for the e-mail server.
Enabled	The e-mail mailbox is in the set of mailboxes on the server from which incomng e-mail is retrieved.
Mailbox Name	The name of a mailbox on the e-mail server. If the Contact Center Multimedia server is in the same domain as the e-mail server, in the Mailbox Name box, type the address, and in the Email Domain box, type the domain name. If the Contact Center Multimedia server is not in the same domain as the e-mail server, and you are using Windows 2000, in the Mailbox Name box, type the address in the format domain\user. If the Contact Center Multimedia server is not in the same domain as the e-mail server, and you use a version of Windows later than Windows 2000, in the Mailbox Name box, type the address in the format user@domain. **Attention:** Mailbox names are case-sensitive. You must type the mailbox name exactly as it appears on your server.
Password	The password used to access the mailbox on the e-mail server.

Variable	Value
Process up to	The maximum number of e-mail messages to be retrieved from the mailbox every scan interval. You can enter a different value for this variable for each mailbox. The default value is 10.
Username	The SMTP server log on ID.

Deleting a recipient mailbox

Delete a recipient mailbox from your system if you no longer require it to monitor e-mail. Removing extra mailboxes saves space in your database.

Prerequisites

- Before you delete a mailbox, you must ensure that no e-mail messages are sent to the inbox or any aliases directed to that mailbox.
- Nortel recommends that you archive all contacts associated with a recipient before you delete the recipient.

Procedure steps

Step **Action**

1 In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.

2 Expand **E-mail Administration**.

3 Double-click **Recipient Addresses**.

4 Select an address from the recipient list.

5 Click **Delete**.

A warning dialog box appears informing you the number of contacts sent to the recipient and that deleting the recipient disassociates that recipient and rules from the contacts.

6 Click **Yes** to confirm to delete the recipient.

7 Click **Close**.

--End--

Updating the system default rule

Update the system default rule to ensure that an e-mail arriving at each configured recipient mailbox is assigned a skillset and can be routed.

When you create a recipient mailbox, the system default rule is copied as the last regular rule into the list of rules for the recipient mailbox.

The automatic signature is text appended to each e-mail message sent from the contact center in addition to the agent message. The text in the automatic signature contains corporate disclaimer information and must be in fixed-width font. The autosignature appears in an e-mail message after any personal signature, which is configured in the Agent Desktop application.

Prerequisites

- Ensure that you know the default settings for the system delivery failure rule:
  - — use the e-mail default skillset, EM_Default_Skillset
  - — use no autoresponse
  - — assign priority 3 (medium high)
- Use caution when you change the properties of the system default rule:
  - — If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - — If you delete the skillset associated with the default rule, EM_Default_Skillset is used.
  - — If you delete EM_Default_Skillset, the system stops processing e-mail messages.
- Configure the route points for the skillset you assign to the system default rule. For more information, see Configuring skillsets for e-mail (page 346).

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Rule Administration**.
3	Double-click **System Default Rule**.
4	From the **Select Skillset** list, select a skillset name. You can accept the current default.
5	Click **Properties** to open the skillset properties to change the route point.

6 In the **Route Point** list, select a different route point.

7 Under **Auto-Signature**, type an automatic signature (optional).

8 Click **Save**.

9 To change the automatic response settings, under **Select Optional Auto-Responses**, select another automatic response from the list.

10 To change the priority, under **Select Priority**, select a different priority for the contact.

11 Click **Save**.

--End--

Variable definitions

Variable	Value
Auto-Response	A message sent to a customer with no agent interaction. An automatic response can be an intelligent response, such as a sales promotion flyer, or an acknowledgement, such as, “We received your e-mail and will respond to you within three days.”
Auto-Signature	Text appended to e-mail messages sent from the contact center in addition to the agent message. The text in the auto-signature contains corporate disclaimer information and must be in fixed-width font. The auto-signature appears at the end of the e-mail history, whereas the personal signature, which is configured in the Agent Desktop application, appears at the end of the agent’s latest message.
Route Point	A location on the open queue that queues incoming calls to and runs through a script on the Contact Center Manager Server.
Select Priority	The priority given to a request for a skillset agent. The lower the number of the priority, the greater the priority. The values of the priorities range from 1 to 6. For example, a call with priority 1 is handled before a call with priority 6.
Skillset	A label applied to a set of skills, capabilities, or knowledge that an agent requires to respond to a request. The skillsets are retrieved from the Contact Center Manager database. You must select a route point for a skillset used to route outbound contacts.

Updating the system delivery failure rule

Update the system delivery failure rule to ensure that any e-mail message that contains particular phrases such as undeliverable, returned mail, unknown recipient, delivery failure, or delivery report is deleted and not assigned to an agent.

When you create a recipient mailbox, the system delivery failure rule is copied as the first regular rule into list of rules for the recipient mailbox.

Prerequisites

- Ensure that you are licensed to handle e-mail messages.
- Ensure that you know the default settings for the system delivery failure rule:
  - — use the e-mail default skillset, EM_Default _Skillset
  - — use keyword group delivery failure keywords
  - — assign priority 6 (lowest)
- Use caution when you change the properties of the system default rule:
  - — If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - — If you delete the skillset associated with the default rule, EM_Default_Skillset is used.
  - — If you delete EM_Default_Skillset, the system stops processing e-mail messages.
- Configure the route point for the skillset you plan to assign to the system delivery failure rule. See Configuring skillsets for e-mail (page 346).

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Rule Administration**.
3	Double-click **System Delivery Failure Rule**.
4	From the **Select Skillset** list, select a skillset name. You can accept the current default.
5	Click **Properties** to open the skillset properties to change the route point.
6	In the **Route Point** list, select a different route point.
7	Below **Auto-Signature**, type an automatic signature (optional).
8	Click **Save**.
9	To change the keyword group, under **Select Keyword Group**, select an existing keyword group from the list.
10	To change the priority, under **Select Priority**, select a different priority from the list for the contact.

11 Select the check box **This Rule will close the Contact** if you want the rule to close the contact.

12 Click **Save**.

13 Continue with the contact configuration using the Getting Started window.

--End--

Variable definitions

Variable	Value
Auto-Signature	Text appended to e-mail messages sent from the contact center in addition to the agent message. The text in the auto-signature contains corporate disclaimer information and must be in fixed-width font. The auto-signature appears at the end of the e-mail history, whereas the personal signature, which is configured in the Agent Desktop application, appears at the end of the agent's latest message.
Keyword group	A list of words or groups of words that you can search in an e-mail message. Keyword groups associate keywords and expressions considered important by the contact center to be handled in a particular way— assign a skillset, close the contact, or send an auto-response. A keyword group cannot be defined with an infinite number of keywords, so additional rules with other keyword groups can be defined to extend the number of keywords that can be checked for any recipient address. The additional rules can be configured with matching skillset settings, so all rules used perform the same routing function.
Route Point	A location on the open queue that queues incoming calls to and runs through a script on the Contact Center Manager Server.
Select Priority	The priority given to a request for a skillset agent. The lower the number of the priority, the greater the priority. The values of the priorities range from 1 to 6. For example, a call with priority 1 is handled before a call with priority 6.
Skillset	A label applied to a set of skills, capabilities, or knowledge that an agent requires to respond to a request. The skillsets are retrieved from the Contact Center Manager database. You must select a route point for a skillset used to route outbound contacts.

Viewing the sequence and status of rules

View the sequence and status of e-mail rules for the configured mailbox to determine how to route e-mail messages in the contact center.

Procedure steps

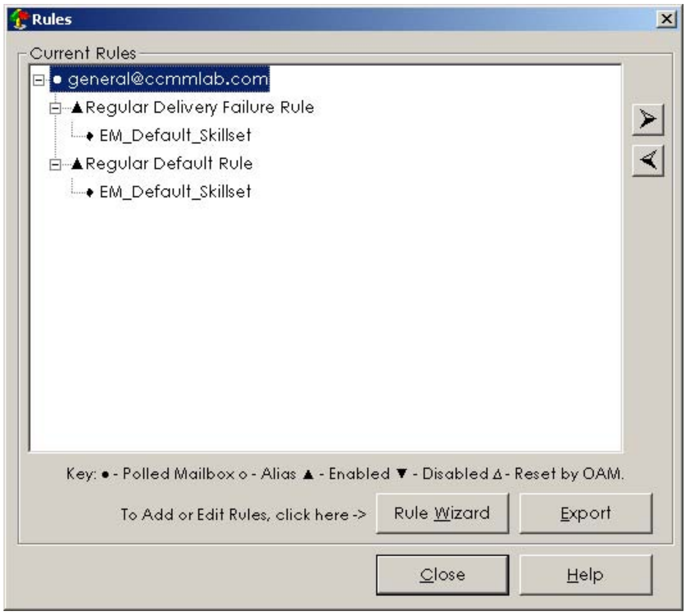
Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Rule Administration**.
3	Double-click **Rule Precedence**.
4	In the **Rules** window, review the rule summary. The legend at the bottom of the window explains the symbols next to the rule names.
5	Click **Close**.

--End--

Procedure job aid

The following dialog box summarizes the rules for your contact center.

Rules dialog box with the status of the rules



Current Rules

- ● general@ccmmlab.com
  - ▲Regular Delivery Failure Rule
    - ♦ EM_Default_Skillset
  - ▲Regular Default Rule
    - ♦ EM_Default_Skillset

Key: ● - Polled Mailbox o - Alias ▲ - Enabled ▼ - Disabled Δ - Reset by OAM.

To Add or Edit Rules, click here ->

Creating a rule

Use the Rule Configuration Wizard to create a single new rule for routing contacts in your Contact Center.

Prerequisites

- Create recipients. See Creating a recipient mailbox (page 347).

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
1	Expand **Rule Administration**.
2	Double-click **Rule Configuration Wizard**.
3	Select **Configure Individual Recipient Rules** to create a rule.
4	Click **Next**.
5	In the **Rule Configuration Wizard**, click **Next**.
6	Click **New** to configure a new rule.
7	Configure the properties of your rule.

--End--

Deleting a rule

Permanently delete a rule. After you delete the rule, you cannot use the rule for routing e-mail messages.

If you permanently delete a rule, existing contacts for the rule can no longer be archived by rule and any Contacts by Rule reports no longer work. Nortel recommends that you archive all contacts associated with a rule before you delete the rule.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator window**, expand **Contact Center Multimedia**.

2	Expand **Rule Administration**.
3	Double-click **Rule Configuration Wizard**.
4	Select **Configure Individual Recipient Rules**, and then click **Next**.
5	On the **The Rule Configuration Wizard - Recipients** dialog box, select the recipient for which you want to delete a rule.
6	Click **Next**.
7	On the **The Rule Configuration Wizard - Rules** dialog box, select the rule to delete.
8	Click **Delete**. A warning dialog box appears informing you of the number of contacts created using the rule and that deleting the rule disassociates the rule from those contacts.
9	In the confirmation dialog box, click **Yes**.
10	Click **Finish**.

--End--

Configure a rule for multiple mailboxes

Configure a rule that applies to more than one mailbox.

Procedure steps

Step	Action
1	Log on to the **Multimedia Administrator**.
2	Expand **Contact Center Multimedia**.
3	Expand **Rule Administration**.
4	Double-click **Rule Configuration Wizard**.
5	Select **Create a New Rule for Multiple Recipients**.
6	Click **Next**.
7	Select the recipient addresses to which you want to add a new rule by selecting the check box next to each recipient name.
8	In the **Rule Configuration Wizard**, click **Next**.
9	Configure the properties for the group of rules.

--End--

Creating a keyword group

You must assign at least one keyword to a keyword group before you can save the keyword group.

The keyword search in an e-mail message is not case-sensitive. If you add the word John, the Email Manager also matches JOHN and john.

The Keyword box supports the Unicode UTF-8 character set.

Keyword groups support only asterisks (*) and question marks (?) as wildcard characters. The asterisk (*) represents multiple characters. For example, t* specifies a list of all the words that start with t. The question mark (?) represents a single character. For example, p?t specifies all three letter words that start with p and end with t.

A keyword does not support the following characters: # + - & I ! ( ) { } [ ] ^ " ~ : and \. If you use any of these characters in your keywords, you receive an error message stating that the keyword contains invalid characters.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **E-mail Administration**.
3	Double-click **Keyword Groups**.
4	Click **New**.
5	On the **New Keyword Group** dialog box, in the Name box, type a unique name for the keyword group (maximum 64 characters).
6	In the **Keyword** box, type a word or a group of words related to the keyword group you create.
7	Click **Add**. The keyword or expression is added to the list, and the keyword group is created.
8	Repeat steps 5 through 7 to add keywords to the list.

9	Click **Save**.
10	Click **Close**.

--End--

Inserting keyword groups into the rule

A keyword group is a list of words or groups of words that you can search in an e-mail message. Keyword groups associate keywords and expressions considered important by the contact center to be handled in a particular way—assign a skillset, close the contact, or send an auto-response.

Keyword groups are optional; however, you can use up to three keyword groups as input parameters for your rule.

A keyword group cannot be defined with a number of keywords, so additional rules with other keyword groups can be defined to extend the number of keywords that can be checked for any recipient address. The additional rules can be configured with matching skillset settings, so all rules used perform the same routing function.

Prerequisites

- Create keyword groups for the rule.See Creating a keyword group (page 360).

Procedure steps

Step	Action
1	On the **Rule Configuration Wizard - Input Criteria** window, under **Available Keyword Groups**, select a keyword group to use for this rule.
2	With the selected keyword highlighted, click the black arrow to insert the keyword group name into the selection box.
3	Repeat step 2 for each keyword group to add.
4	Between each keyword group selection, click AND or AND NOT to create a logical expression for your keyword groups.

Attention: If the same word appears in two keyword groups separated by a NOT operator, the rule fails. The e-mail is evaluated by the next rule configured for the recipient mailbox.

--End--

Changing a keyword group

You must assign at least one keyword to a keyword group before you can save the keyword group.

The keyword search in an e-mail message is not case-sensitive. If you add the word John, the Email Manager also matches JOHN and john.

The Keyword box supports the Unicode UTF-8 character set.

Keyword groups support only asterisks (*) and question marks (?) as wildcard characters. The asterisk (*) represents multiple characters. For example, t* specifies a list of all the words that start with t. The question mark (?) represents a single character. For example, p?t specifies all three letter words that start with p and end with t.

A keyword does not support the following characters: # + - & I ! ( ) { } [ ] ^ “ ~ : and \. If you use any of these characters in your keywords, you receive an error message stating that the keyword contains invalid characters.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **E-mail Administration**.
3	Double-click **Keyword Groups**.
4	To change an existing keyword group, select a keyword group name.
5	Click **Edit**.
6	In the **Name** box, type a unique name for the keyword group (maximum 64 characters).
7	In the **Keyword** box, type a word or a group of words related to the keyword group you create.
8	Click **Add**. The keyword or expression is added to the list, and the keyword group is created.

9	Repeat steps 6 through 8 to add keywords to the list.
10	Click **Save**.
11	Click **Close**.

--End--

Clearing a keyword group from a rule

Clear a keyword group from a rule when you no longer require the group.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Rule Administration**.
3	Double-click **Rule Configuration Wizard**.
4	Click **Configure Individual Recipient Rules**.
5	Click **Next**.
6	Select a recipient for which you want to change the rule.
7	Click **Next**.
8	Select the rule to change.
9	Click **Edit**.
10	Under **Keywords**, click **Clear** to clear all of the keyword entries.
11	Click **Next**.
12	Click **Save**.

--End--

Deleting a keyword from a keyword group

Remove a keyword from a keyword group. The remaining keywords and phrases in the keyword group remain active for rules.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **E-mail Administration**.
3	Double-click **Keyword Groups**.
4	Select a keyword group from the list.
5	Click **Edit**.
6	On the **Edit Keyword Group** dialog box, select the keyword from the **Keywords in Group** list.
7	Click **Remove**.
8	Click **Save**.

--End--

Deleting a keyword group

Delete a keyword group. After you remove the keyword group from the rule configuration tool, you cannot use it in any rules. Rules that use the deleted keyword group may not route the contact as expected.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **E-mail Administration**.
3	Double-click **Keyword Groups**.
4	Select a keyword group.
5	Click **Delete**.

6 Click **OK**.

7 Click **Close**.

--End--

Creating a sender group for the rule

You must place any sender addresses that you want to track in a sender group. You can use sender groups to route important sender e-mail addresses to skillsets.

Using a sender group in the rule is optional.

Sender groups support only asterisks (*) as a wildcard character when it is placed before the address at symbol (@) in the e-mail address. You cannot use the wildcard characters at the end of a sender group address.

Nortel recommends that you have a maximum of 20 sender e-mail addresses in one sender group.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **E-mail Administration**.
3	Double-click **Sender Addresses**.
4	On the **Sender Addresses** dialog box, click **New.**
5	On the **New Sender Group** dialog box, in the **Name** box, type a unique name for the sender group (maximum 64 characters).
6	In the **E-mail Address** box, type an e-mail address.
7	If you know the user is in the contact database, start typing an e-mail address, and then click **Lookup**. E-mail addresses that match the characters you typed, appear in the list.
8	Click **Add** to insert the e-mail address you looked up, or click **Add Freeform** to add your typed e-mail address to the sender group. This text box supports unicode language. For example, you can enter Chinese text.

9	Repeat steps 6 through 9 to add sender addresses to this sender group.
10	Click **Save**.
11	Click **Close**.

--End--

Inserting sender groups into the rule

You must place any sender addresses that you want to track in a sender group. Sender groups can be used to route important sender e-mail addresses to skillsets.

Using a sender group in the rule is optional.

Nortel recommends that you have a maximum of 20 sender e-mail addresses in one sender group.

Prerequisites

- Create sender groups for the rule. See Creating a sender group for the rule (page 365)

Procedure steps

Step	Action
1	On the **Rule Configuration Wizard - Input Criteria** window, under **Available Sender Groups**, select a sender group to use for this rule.
2	When a sender group is highlighted, click the black arrow to insert the sender group name into the selection box.

--End--

Changing a sender group

A sender is the person who sends the e-mail message to the contact center. A sender group is a group of addresses that represent people who send e-mail to the contact center. You can use sender groups to route an e-mail message.

You can use an asterisk (*) as a wildcard to represent none to any number of characters in a word. You can use only one asterisk in each address, and it must appear before the at symbol (@) in your e-mail address. You cannot start an e-mail address with the wildcard, unless it is the only character before the at symbol in your e-mail address. For example, *@nortel.com, joe*@nortel.com, or j*e@nortel.com are acceptable.

Nortel recommends that you have a maximum of 20 sender e-mail addresses in one sender group.

Prerequisites

- You must have a sender group. See Creating a sender group for the rule (page 365).

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **E-mail Administration**.
3	Double-click **Sender Addresses**.
4	In the **Current Senders (From Addresses)** list, select the sender.
5	Click **Edit**.
6	In the **Name** box, type a unique name for the Sender group (maximum 64 characters long).
7	In the **E-mail Address** box, type an e-mail address.
8	If you know the user is in the contact database, start typing an e-mail address, and then click **Lookup**. E-mail messages that match the characters you typed appear in the list.
9	Click **Add** or **Add Freeform** to add the e-mail address to the sender group. This text box supports Unicode language. For example, you can enter Chinese text.
10	When you add free-form text, you can type in a full e-mail address or use a wildcard
11	Click **Save**.

12 Click **Close**.

--End--

Configuring rule output actions

You must assign an e-mail that matches a particular rule to a skillset or close it. You can create an automatic response to reply to the e-mail.

You can create only one out-of-office-hours rule.

Prerequisites

- Configure a skillset for the rule. See Configuring skillsets for e-mail (page 346).

Procedure steps

Step	Action
1	On the **Rule Configuration Wizard - Output** actions dialog box, in the Rule **Name** box, type the name of your rule. The name of your rule must be unique.
2	In the **Skillset** box, select a skillset to assign the contact to if the contact matches the rule.
3	In the **Contact Type** box, select the type to assign to the contact if the contact matches the rule.
4	In the **Contact Priority** box, select the priority for the contact if the contact matches the rule.
5	To configure a rule that is applied when the contact center is closed, select the **This rule will use Office Hours** check box.
6	Default hours are configured for office hour times in your contact center. For information about changing the open and close times, see your **Multimedia Administrator** online Help.
7	To close the contact when a match to the rule is found, select the **This Rule will close the Contact** check box.

--End--

Creating a new automatic response for a rule

Automatic responses are used to send messages to a sender.

An automatic response can perform one of the following objectives:

- provide the customer with their Web logon ID and password (password reminder auto-response)
- inform a customer the office is closed (out-of-office automatic response)
- acknowledge the receipt of an e-mail contact (regular automatic response, or an automatic acknowledgement)
- provide specific information in response to rule inputs (regular automatic response)

A password reminder automatic response and an out-of-office automatic response are configured by default. You cannot delete the default automatic responses. You can create the number of regular automatic responses your contact center requires.

Configuring an auto-response for a rule is optional.

Procedure steps

Step	Action
1	On the **Rule Configuration Wizard - Output Criteria** window, under **Autoresponses**, click **More**.
2	Click **New**.
3	In the **Name** box, type the name of the auto-response.
4	In the **Subject** box, type the subject of the response e-mail message.
5	In the **Body** box, type the message to include in the response.
6	Click **Save**.
7	Click **Close**.

--End--

Adding an automatic response to the rule

Automatic responses are used to send messages to a sender. When you add an automatic response to a rule, the message is sent to the sender according to the routing properties of the e-mail rule.

Prerequisites

- Create an automatic response for the rule. See Creating a new automatic response for a rule (page 369).

Procedure steps

Step	Action
1	On the **Rule Configuration Wizard - Output Criteria** window, under **Autoresponses**, select a response to use for this rule.
2	When the selected automatic response is highlighted, click the black arrow to insert the selected automatic response name into the selection box.
3	Click **Save**.
4	Click **Finish**.
5	Repeat this process to configure other rules.

--End--

Printing a rule summary

You can view and print a list of the rules you configure. Review the order in which the rules are applied to each recipient contact. You can also see the status of each rule.

You can export the rules from the Rule Precedence window to a text file for printing.

Procedure steps

Step	Action
1	Log on to the **Multimedia Administrator**.
2	On the **Utilities** menu, click **Export Rules**.
3	Browse to a file location on your server to store the file.

4 Click **Save**.

5 Go to the file named Rules.txt, saved on your desktop.

6 Double-click to open the file.

7 On the **File** menu, click **Print**.

--End--

Making rules inactive

Make rules active and inactive. An inactive rule remains configured, but is not used to route incoming e-mail until the rule is active again.

Prerequisites

- Configure one or more rules. See Creating a rule (page 358) or Configure a rule for multiple mailboxes (page 359).

Procedure steps

Step	Action
1	In the **Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Rule Administration**.
3	Double-click **Rule Configuration Wizard.**
4	Select **Configure Individual Recipient Rules**.
5	Click **Next**.
6	In the **Available Recipients** box, select the recipient.
7	Select the rule.
8	Click the check mark icon to activate the rule or go to step 9.
9	Click the X icon to make a rule inactive.

--End--

Clearing a sender address from a rule

Delete a sender group. After you remove the sender group from the rule configuration tool, you cannot use it in any rules. Rules that use the deleted sender group may not route the contact as expected.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **E-mail Administration**.
3	Double-click **Sender Addresses**.
4	Select a sender group.
5	Click **Delete**.
6	Click **OK**.
7	Click **Close**.

--End--

Deleting a sender

Remove a sender address from a sender group. The remaining addresses in the sender group remain active for rules.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **E-mail Administration**.
3	Double-click **Sender Addresses**.
4	Select a sender group from the list.
5	Click **Edit**.
6	On the **Edit Sender Group** dialog box, select the e-mail address from the list.

7	Click **Remove**.
8	Click **Save**.
9	Click **Close**.

--End--

Deleting an auto-response from a rule

You can delete a regular or an out-of-office automatic response. After you remove the automatic response from the rule configuration tool, you cannot use it in any rules. For rules that currently have a deleted automatic response, no response is sent to the customer.

You cannot delete the password reminder automatic response.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **E-mail Administration**.
3	Double-click **Auto-Responses**.
4	On the **Auto-Responses** dialog box, select an auto-response from the list provided.
5	Click **Delete**.
6	Click **OK**.
7	Click **Close**.

--End--

Clearing an automatic response from a rule

Clear an automatic response from a rule if you no longer require it.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Rule Administration**.
3	Double-click **Rule Configuration Wizard**.
4	Click **Configure Individual Recipient Rules**.
5	Click **Next**.
6	Select a recipient for which you want to change the rule.
7	Click **Next**.
8	Select the rule to change.
9	Click **Edit**.
10	Under **Auto-Response**, click **Clear**.
11	Click **Next**.
12	Click **Save**.

--End--

Changing an automatic response

The automatic responses are in plain text, fixed font, and apply to rules. If a rule successfully matches with the contents of an e-mail message, then a skillset is assigned and an auto-response can be sent.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **E-mail Administration**.
3	Double-click **Auto Responses**.
4	On the **Auto-Responses** dialog box, select the auto-response.
5	Click **Edit**.

6 In the **Name** box, type the name of the auto-response.

7 In the **Subject** box, type the subject of the response e-mail message.

8 In the **Type** box, select the type of auto-response: out-of-office automatic responses to use during the time the office is closed, password reminders automatic responses to use for customer password information and regular automatic responses.

9 In the **Body** box, type the message to include in the response.

10 Click **Save**.

--End--

Adding an attachment to an auto-response

Add attachments only from the designated outbound mail folder. You cannot add attachments from subfolders. The designated outbound mail folder is displayed in the E-mail Manager properties window.

A list of the attachments for the automatic response is listed in the window.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **E-mail Administration**.
3	Double-click **Auto-Responses**.
4	Select the auto-response to which you want to add an attachment.
5	Click **Edit**.
6	On the **Insert** menu, click **Attachment**.
7	On the confirmation dialog box, click **OK**.
8	Click **Save**.
9	Click **Close**.

--End--

Inserting data into an auto-response

You can use data in an auto-response message to customize a response.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **E-mail Administration**.
3	Double-click **Auto-Responses**.
4	Select the auto-response message into which you want to insert data.
5	Click **Edit**.
6	Place the cursor in the subject or body where you want to insert the data.
7	To add a date, on the **Insert** menu, click **Date**.
8	On the **Date** dialog box, select a date and time format.
9	Click **Insert**.
10	The code for the date or time appears in the message. **Multimedia Email Manager** inserts the current date or time when it sends the message.
11	To add another data item, choose **Insert**, **Data Item**.
12	On the **Data Item** dialog box, from the **Data Item** list, select the item to insert.
13	Click **Insert**.
14	The code for the selected field appears in the message text. The Email Manager queries the contact record and inserts the values found in the selected boxes.
15	Click **Save**.
16	Click **Close**.

--End--

Removing attachments from an automatic response

Remove attachments from an automatic response. The attachment file is stored on the Multimedia server to be used later.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **E-mail Administration**.
3	Double-click **Auto-Responses**.
4	Select the auto-response from which you want to remove an attachment.
5	Click **Edit**.
6	Select the attachment to delete.
7	Under the **Attachments** box, click **Remove**.
8	Click **Save**.
9	Click **Close**.

--End--

Applying a rule when the office is closed

Create one rule that applies to e-mail messages when the office is closed.

If you configure a new rule for when the office is closed, the new rule replaces and makes invalid any previous rule.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Rule Administration**.
3	Double-click **Rule Configuration Wizard**.
4	On the **Rule Configuration Wizard Begin** dialog box, select **Configure Individual Recipient Rules** to create a rule.
5	Click **Next**.
6	On the **Rule Configuration Wizard Recipients** dialog box, click **Next**.

7 On the **Rule Configuration Wizard Rules** dialog box, click **New**.

8 On the **Rule Configuration Wizard Input Criteria** dialog box, add a keyword group.

9 Add a sender group.

10 Click **Next**.

11 On the **Rule Configuration Wizard - Output Actions** dialog box, in the **Rule Name** box, type the name of your rule. The name of your rule must be unique.

12 In the **Skillset** box, choose a skillset to assign the contact to if the contact matches the rule.

13 In the **Contact Type** box, select the type to assign to the contact if the contact matches the rule.

14 In the **Contact Priority** box, select the priority for the contact if the contact matches the rule.

15 Select **This rule will use Office Hours**.

16 Click **Save**.

17 View the list of rules.

18 Click **Finish**.

19 Repeat this process to configure other rules.

--End--

Creating or changing a recipient

You can use the SMTP Logon when you configure an inbox as an alias and it is disabled. The SMTP server rejects the alias inbox name and instead uses the logon name of the mailbox. The skillsets mapped to this inbox log on to the SMTP server using the alternative name but they appear to come from the same inbox.

You can have inboxes on more than one e-mail server. Each e-mail server is polled for the mailboxes it hosts.

When the Email Manager starts, it looks to the POP3 host for the mailbox. The outbound e-mail is sent through the specified SMTP host.

Procedure steps

Step **Action**

1 In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.

2 Expand **E-mail Administration**.

3 Double-click **Recipient Addresses**.

4 Click **New**.

5 In the **Mailbox Name** box, type the name of a mailbox set up on the POP3 server. Mailbox names are case-sensitive. You must type the mailbox name exactly as it appears on your e-mail server.

6 In the **E-mail Domain** box, type the domain name of the POP3 server. The domain name is case-sensitive.

7 In the **Password** box, type the password for the Windows domain user account that you specified as the owner of the mailbox. When you change a password, you must update this password in the **Contact Center Multimedia Administrator**.

8 In the **Confirm** box, type the same password you typed in the Password box.

9 In the **Display Name** box, type the friendly name to appear in the e-mail From address (for example, Customer Support). You must enter a display name for each mailbox.

10 In the **POP3 Server** box, type the host name of the POP3 e-mail server.

11 In the **SMTP Server** box, type the host name of the SMTP server.

12 To add this mailbox as a mailbox that stores messages and from which incoming mail is retrieved, select **Enabled**.

13 To add this mailbox as an alias, select **Alias**. Use an alias for rules configuration and outbox mapping. The alias does not contain e-mail, but provides a link to a general mailbox.

14 In the **Process Up To** box, enter the maximum number of e-mail messages to be retrieved from the mailbox every scan interval.

You can enter a different value for this variable for each mailbox. The default value is 10.

15 Select the Alternative Username for SMTP Authentication check box if you plan to log on to the SMTP server with a user name different from the one you configured as the inbox name. In the Username box, type the user name for the SMTP authentication.

16 Click **Save**.

--End--

Configuring holidays

Apply a single rule to e-mail messages when the office is closed. You must first configure the office hours and holidays for your contact center.

Invalid dates are not permitted. February 29 is accepted as a valid date, so you must check to ensure that the year is a leap year before you configure a holiday.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Rule Administration**.
3	Double-click **Office Hours Rule**.
4	Under **Holiday Hours**, click the plus sign (**+**) to add a new day.
5	In the **Name** box, type a meaningful name for the holiday.
6	In the **Day** box, select the date of the holiday (day, month, and year).
7	If the contact center is closed all day, click **The Contact Center is closed All Day**.
8	The **Holiday Time** box contains 00:00, and the End Time contains End of Day.
9	To configure an opening time for the contact center, in the **Start Time** box, select the time, using the 24-hour clock, that your contact center opens. If the contact center does not open during the selected day, select 00:00
10	In the **End Time** box, select the time, using the 24-hour clock, that your contact center closes.
11	Click **Save**.
12	On the **Office Hours Rule** box, click **Save**.
13	Click **Close**.

--End--

Configuring office hours

Apply a single rule to e-mail messages when the office is closed. You must first configure the office hours and holidays for your contact center.

To change the hours for a particular day, you must delete the day, and then add it again with the new hours.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand Contact Center Multimedia.
2	Expand **Rule Administration**.
3	Double-click **Office Hours Rule**.
4	Under **Normal Office Opening Hours**, click the plus sign (**+**) to add a new day.
5	To remove the selected day, click the minus sign (**–**).
6	In the **Day** box, select the day of the week.
7	In the **Start Time** box, select the time, using the 24-hour clock, that your contact center opens.
8	In the **End Time** box, select the time, using the 24-hour clock, that your contact center closes.
9	Click **Save**.
10	Click **Close**.

--End--

Enabling SSL on the Email Manager

Enable Secure Sockets Layer (SSL) on the Email Manager. Contact Center Multimedia/Outbound supports Secure Sockets Layer (SSL) to protect data traveling between the e-mail server and the Contact Center Multimedia/ Outbound server.

Although SMTP is secure, when e-mail traverses the Internet, it becomes unsecure. Implementations of secure SMTP vary as does the port number. For more information, see the documentation for your e-mail server.

If an error is reported in the EmailManager.log file: javax.net.ssl.SSLHandshakeException: Could not find trusted certificate indicating that the target mail server's SSL certificate was signed with a certificate from a signing authority that is untrusted or you are using a test certificate, you must enable SMTP Authentication on your e-mail server.

Prerequisites

- Nortel recommends that you use a false connection on the fallback. If you assign fallback to false, a secure connection cannot be established and the operation fails. If you assign the fallback to true, during a failure the connection is unsecure.

Procedure steps

Step	Action
1	Open the mailservice.properties file. The mailservice.properties file is in X:\Nortel\Contact Center\Multimedia Server\Server Applications\EMAIL; X is the drive on which you installed your Multimedia server software.

2	Copy the following lines into mailservice.properties file.
	`mail.pop3.socketFactory.class=javax.net.ssl.SSLSocketFactory`
	`mail.pop3.socketFactory.fallback=false`
	`mail.pop3.socketFactory.port=995`

3	Log on to the **Multimedia Administrator**.
4	Expand **Server Administration**.
5	Double-click **Server Configuration**.
6	In the **Server Settings** window, double-click **Inbound Mail Server (POP3)**.
7	In the **Primary Hostname** box, type the name of the server that receives e-mail messages.
8	In the **Server Type** box, for the inbound e-mail server, select **POP3**.
9	In the **Port Number** box, type the standard port number for the e-mail server, which is 995.
10	In the **Secondary Hostname** box, if you have a backup e-mail server, provide a host name for the backup server.
11	Click **Save**.

12	Copy the following lines into mailservice.properties file.
	`mail.smtp.socketFactory.class=javax.net.ssl.SSLSocketFactory`
	`mail.smtp.socketFactory.fallback=false`
	`mail.smtp.socketFactory.port=25`
	The configuration is complete.

13 Use Java keytool to enable trust for a signing authorities certificate. By default, Java application SSL implementations automatically trust many of the major certificate authorities such as Verisign or Thawte. However, if you use a test certificate you must add the following text to C:\Program Files\Java\jrel.5.0\lib\security\cacerts:

```
keytool -import -alias mycacert -file mycacert.cer -
keystore
```

14 When you are prompted for a keystore password, use the default install password for the JRE trust keystore, **changeit**.

15 After the certificate details are printed, you are prompted to Trust this certificate.

16 Type y or yes, and then press return to update the keystore.

The file appears as follows:

```
Owner: OU=For VeriSign authorized testing only. No
assurances (C)VS1997, OU=www.verisign.com/repository/
TestCPS Incorp. By Ref. Liab. LTD., O="VeriSign, Inc"
Issuer: OU=For VeriSign authorized testing only. No
assurances (C)VS1997, OU=www.verisign.com/repository/
TestCPS Incorp. By Ref. Liab. LTD., O="VeriSign, Inc"
Serial number: 52a9f424da674c9daf4f537852abef6e
Valid from: Sun Jun 07 01:00:00 BST 1998 until: Wed Jun
07 00:59:59 BST 2006
Certificate fingerprints:
MD5:
40:06:53:11:FD:B3:3E:88:0A:6F:7D:D1:4E:22:91:87
SHA1:
93:71:C9:EE:57:09:92:5D:0A:8E:FA:02:0B:E2:F5:E6:98:6C:6
0:DE
Trust this certificate? [no]: y
Certificate was added to keystore
```

17 Enter the keystore password **changeit**.

18 Restart the **Email Manager** service.

19 To change the default password for security reasons, type the following command and you are prompted for a new password:

```
keytool -storepasswd -new changeit -keystore
C:\Program Files\Java\jre1.6.07\lib\security\cacerts
```

--End--

Enabling SMTP Authentication on your e-mail server

Enable SMTP authentication for Microsoft Exchange Server 5.5. SMTP Authentication is a mechanism to restrict non authenticated clients from relaying messages outside your organization. Agents who want to send external e-mail must provide their logon credentials to the e-mail server before their e-mail is relayed. Failure to authenticate leads to either an immediate message from the e-mail server indicating that relaying is prohibited or a later nondelivery report e-mail. Organizations generally implement SMTP authentication to prevent SPAM messages being relayed through the networks. For more information, see the Microsoft Knowledge Base article Q197869.

SMTP authentication varies from e-mail server to e-mail server.

Procedure steps

Step	Action
1	Log on to the **Microsoft Exchange Server** with domain administrative privileges.
2	Start the **Microsoft Exchange Administrator** program.
3	On the **Configuration** branch, double-click **Internet Mail Service**.
4	On the **Routing** tab, click **Routing Restrictions**.
5	Ensure you select the **Only Hosts and Clients** who successfully authenticate check box.
6	Restart the **Microsoft Exchange Internet Mail Service**.

--End--

Determining if SMTP Authentication is enabled

Use Telnet to verify whether the server response to the SMTP commands is enabled on an e-mail server.

After a successful logon, you can send a mail using the MAIL, RCPT, and DATA commands.

Procedure steps

Step **Action**

1 Start Telnet and connect to the IP Address or host name of the mail server. Connect using the well-known port for SMTP (Port 25). Ensure that your Telnet application is enabling a local echo.

The following message appears:

```
220 SERVERNAME.DOMAIN.COM ESMTP Server (Microsoft
Exchange
Internet Mail Service 5.5.2650.21) ready
```

2 Type HELO.

3 Try to send an e-mail message to an external address using the MAIL command:

```
MAIL FROM: anymailbox
250 OK - mail from <anymailbox>
```

4 Specify recipients using the RCPT command.

If SMTP Authentication is enabled, you see the following:

```
RCPT TO: anyone@externaladdress.com
550 Relaying is prohibited
```

Otherwise, you receive the message:

```
RCPT TO: anyone@externaladdress.com
250 OK - Recipient <anyone@externaladdress.com>
```

5 If you find that SMTP Authentication is not enabled, you can continue to send an e-mail message using the DATA command:

```
DATA
354 Send data. End with CRLF.CRLF
```

6 Conclude the e-mail message by typing **<ENTER> . <ENTER>**

The e-mail message is sent.

```
250 OK
```

7 If the SMTP Authentication is enabled, you must reconnect to your e-mail server.

8 Enter the EHLO command after you reconnect:

```
EHLO
250-SERVERNAME.DOMAIN.COM Hello [LocalMachineName]
250-XEXCH50
250-HELP
250-ETRN
250-DSN
250-SIZE 0
250-AUTH LOGIN
```

```
250 AUTH=LOGIN
```

9 Type the AUTH LOGIN command:

```
AUTH LOGIN
334 VXNlcm5hbWU6
```

10 Type your user name encoded using Base64.

A base64 encoded prompt for password appears:

```
AUTH LOGIN
334 VXNlcm5hbWU6
dGVzdA==
334 UGFzc3dvcmQ6
dGVzdA==
235 LOGIN authentication successful
```

Attention: The “dGVzdA==” above represents the word “test” when base64-encoded. The responses shown here are examples. Use the base64 representation of your user name and password that is specific to your e-mail mailbox account.

11 Confirm the user name and password.

--End--

Outgoing E-mail configuration

Configure the outgoing e-mail message settings for responses to incoming e-mail messages or a contact initiated because of another type of contact.

Navigation

Configuring Microsoft Exchange 2007 for sending outgoing e-mail

Configure Microsoft Exchange 2007 if it is installed on your e-mail server to send outgoing e-mail from the Contact Center Multimedia agent desktops.

If you use Microsoft Exchange 2003, additional configuration is not required.

Prerequisites

- Ensure that you use Microsoft Exchange 2007 on your e-mail server.

Procedure steps

Step	Action
1	Log on to the Multimedia server Administrator.
2	Expand **General Administration**.
3	Double-click **Server Settings**.
4	Select the **Outbound Mail Server (SMTP)**.
5	Click **Edit**.
6	Under **Advanced SMTP Settings**, select **Base 64 Encoded Authentication**.
7	Click **Save**.
8	Click **Close** to close the Server Settings dialog box.
9	Log on to the Exchange 2007 server.
10	Open the Exchange Management Console.
11	Click **Server Configuration**, **Hub Transport**, **Receive Connectors Tab**.
12	Right-click **Default <Servername>** and click **Properties**.
13	Click the **Authentication** tab.
14	Disable all authentication except: • Basic Authentication • Exchange Server Authentication • Integrated Windows Authentication
15	Close the Exchange Management Console.

--End--

Configuring the e-mail settings

Configure optional e-mail settings:

- how frequently you scan the e-mail server for new messages
- where the attachments are stored
- which text is searched when you use keywords for rules

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **E-mail Administration**.
3	Double-click **E-mail Configuration**.
4	To configure a different Mailbox Scan Interval, type the time in minutes or seconds.
5	To change the Attachment Files locations, type the new path into the fields provided.
6	Select or clear the **Customer ID** check box or **Contact ID** check box or both. If you select the check box, the identification number is included in the message subject of all e-mail messages.
7	Select or clear the **Include email Body in Keyword Search** check box. If you select the check box, the keyword search for rules applies to both the subject and the body of the e-mail message. You can also select the number of characters in the e-mail message to search.
8	Click **Save**.

--End--

Configuring the outgoing mailbox for responses

Configure outgoing e-mail mailbox settings to identify who responds to the customer's e-mail message. For outgoing e-mail, you can also change the message encoding.

The response can contain the e-mail address to which the customer sent the original e-mail message, or a general corporate e-mail address that is configured for each skillset. Agent-initiated messages are always sent from an e-mail address associated with a skillset.

E-mail messages must be relayed through the e-mail server, not forwarded to another party if the e-mail server manages e-mail messages on behalf of an external source. Sending e-mail messages preserves the original To address which is used for e-mail rule administration and outgoing e-mail addresses.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **E-mail Administration.**
3	Double-click **Outgoing E-mail**.
4	Select a skillset.
5	Click **Set Mapping**.
6	To send customer responses from an address specified for the skillset, click **Send both Agent-initiated Contacts and Customer Responses from this Email address**, and then select the e-mail address for the outgoing e-mail. This e-mail address must be defined as a mailbox on the Email Manager.
7	To send customer responses from the address that the customer used, click **Respond to Customer Contacts with the Recipient address of the original email**, and then select the e-mail address for the outgoing e-mail for agent-initiated e-mail messages. This e-mail address must be defined as a mailbox on the Email Manager.
8	Click **Save**.

--End--

Changing the encoding for outgoing e-mail

Change the encoding of outgoing e-mail to reply to an e-mail message using the same character set as the inbound e-mail. For example, if an e-mail arrives to the contact center with Latin-1 encoding, the reply from the agent desktop or the auto-response is sent in Latin-1. The customer e-mail client can understand the format of the message sent from the contact center.

Prerequisites

- Nortel recommends that only contact centers in Europe use Latin 9 encoding.
- Ensure that you have language pack W2K3.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **E-mail Administration**.
3	Double-click **E-mail Encoding**.
4	In the **Encoding** list, select the type of encoding to use.
5	To select the Latin 9 encoding for replies, select the **Reply to Latin 1 as Latin 9** check box.
6	Click **Save**.
7	Click the **Start** menu of the Multimedia server, click **All Programs**, **Administrative Tools**, **Services**.
8	Right-click **CCMM Email Manager.**
9	Click **Restart**.
10	Close the **Services** window.

--End--

Changing the encoding of e-mail replies

The Email Manager uses the original character set of the inbound e-mail for agent replies. For example, if an agent receives an e-mail message encoded in UTF-8, the agent reply is also encoded in UTF-8. However, if the original e-mail message is encoded with the Latin 1 character set (ISO-8859-1), an option is available to reply in Latin 9 (ISO-8859-15). Use Latin 9 to provide support for the Euro currency symbol, as this character is not included in the Latin 1 character set. Outgoing e-mail messages encoded in Latin 1 that include the Euro symbol, deliver the symbol as a question mark. However, not all recipient clients understand Latin 9 and can receive what is perceived as a blank e-mail message. Therefore, Nortel recommends that contact centers in Europe use the option for Latin 9 encoding while contact centers outside Europe avoid it.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **E-mail Administration**.
3	Double-click **E-mail Encoding**.
4	Under **Customer Replies**, select the **Reply to Latin 1 as Latin 9** check box.
5	Click **Save**.

--End--

Selecting the outgoing e-mail address

You can send e-mail messages from the e-mail address to which the original message was sent, or from a general e-mail address in the contact center.

You can choose the response e-mail address based on a skillset.

Procedure steps

Step	Action
1	In the Contact **Center Multimedia Administrator** window, expand Contact Center Multimedia.
2	Expand **E-mail Administration**.
3	Double-click **Outgoing E-mail**.
4	Select a skillset.
5	Click **Set Mapping**.
6	Select one of the following options: • Send both agent-initiated and customer responses from the e-mail address • Respond to customer contacts with the recipient address of the original e-mail, and send Agent-Initiated Contacts from this address.
7	Select the appropriate e-mail address.

8	Click **Save**.
9	Click **Close**.

--End--

Barring e-mail addresses

Configure Contact Center Multimedia to block certain e-mail addresses. When you bar an e-mail address, automatic replies and agent e-mail messages are not sent to the barred address.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **E-mail Administration**.
3	Double-click **Outgoing E-mail**.
4	Click the **Barred Outgoing Addresses** tab.
5	Click **New**.
6	Type the e-mail address to block, and then click **Save**. The address appears in the list of Barred Addresses.
7	Click **Save.**
8	Click **Close**.

--End--

Deleting a barred e-mail address

Remove a blocked e-mail address from the barred e-mail address list.

Prerequisites

- Ensure that removing a barred address does not violate local governing for do-not-call lists.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **E-mail Administration**.
3	Double-click **Outgoing E-mail**.
4	Click the **Barred Outgoing Addresses** tab.
5	Select a barred e-mail address from the list provided.
6	Click **Delete**.
7	Click **OK** to confirm the deletion.
8	Click **Close**.

--End--

Changing a barred e-mail address

Correct a typographical error or change the information in a barred e-mail address.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **E-mail Administration**.
3	Double-click **Outgoing E-mail**.
4	Click **Barred Outgoing Addresses**.
5	Select a barred e-mail address from the list provided.
6	Click **Edit**.
7	Make the necessary changes to the e-mail address.

8 Click **Save**.

9 Click **Close**.

--End--

Web communications and instant message configuration

The Contact Center Multimedia server supports text-based conversations between the customer and agent using Instant messaging in a Microsoft OCS environment, or Web communications text chat in a Communications Server 1000/DMS switch environment.

You can use auto-phrases to configure text for agents to automatically insert in the instant message or Web communications contacts.

The page push URLs are designated URLs that the agent can automatically insert in a Web communications contact.

Prerequisites for Web communications and instant message configuration

- Ensure that you have a license for Web communications or instant messaging.
- Log on to the Contact Center Multimedia Administrator.

Navigation

- Assigning development Web server name (page 397)
- Creating an automatic phrase (page 398)
- Deleting an automatic phrase (page 399)
- Creating a page push URL (page 399)
- Deleting a page push URL (page 400)
- Configuring contact timers (page 401)
- Configuring automatic text (page 402)
- Configuring customer notification log (page 404)
- Creating WebComms Web On Hold URLs groups (page 405)
- Changing the sequence of a WebComms Web On Hold URLs group (page 406)

- Deleting a URL from a WebComms Web On Hold group (page 407)
- Deleting a WebComms Web On Hold group (page 407)

Assigning development Web server name

Configure the external Web server name to identify the external Web server for Web contacts received by the contact center.

If you configured the external Web server during installation, and the name of the server is unchanged, you can ignore this procedure. If you move your external Web site from a test computer to the production server, you must configure the external Web server name.

Prerequisites

- Know the name of your development Web server and the production Web server.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **General Administration**.
3	Double-click **Server Settings**.
4	In the **Server Settings** dialog box, double-click **External Web Server (HTTP)**.
5	In the **Server Name** box, type the name of the external Web server where you plan to install the sample Web customer interface and develop your custom Web site.
6	In the **Server Port** box, type the port number for the external Web server you use to develop your custom Web site.
7	Click **Save**.
8	Click **Close**.

--End--

Variable definitions

Variable	Value
Server Name	The name of the external Web server where you plan to install the sample Web customer interface and develop your custom Web site.
Server Port	The port number for the external Web server for your custom Web site.

Creating an automatic phrase

Configure an automatic phrases by skillset. You can create a list of commonly used phrases for agents to insert into their Web communications or instant message sessions instead of typing the responses.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **WebComms & IMs Administration**.
3	Double click **Auto-Phrases**.
4	In the **Auto-Phrases** dialog box, select the skillset for which you want to add new phrases.
5	Click **Edit**.
6	In the **Edit Auto-Phrase** dialog box, in the **Previously Configured Auto-Phrase** box, review the phrases for all skillsets. You can add auto-phrases to the current skillset from other skillsets.
7	In the **Name** box, type a name to represent this auto-phrase. The name of the auto-phrase appears in the Contact Center Agent Desktop for the selected skillset so it must be descriptive.
8	In the **Phrase Text** box, type the text that is commonly used for the contacts based on the selected skillset.
9	Click **Add**.
10	Click **Save**.
11	Click **Close**.

--End--

Deleting an automatic phrase

Delete the automatic phrase to remove it from the list of automatic phrases available to the agents in the Contact Center Agent Desktop.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **WebComms & IMs Administration**.
3	Double-click **Auto-Phrases**.
4	In the **Auto-Phrases** dialog box, select the skillset for which you want to change the phrases.
5	Click **Edit**.
6	In the **Edit Auto-Phrases** dialog box, in the **Phrases in Group** box, select the auto-phrase to delete.
7	Click **Remove**.
8	Click **Save**.
9	Click **Close**.

--End--

Creating a page push URL

In the Contact Center Agent Desktop, the agent can choose from a list of Web pages that are specified for the skillset assigned to the Web communication or instant message contact.

You can configure the Web pages listed in the Contact Center Agent Desktop in the Contact Center Multimedia Administrator application.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **WebComms & IMs Administration**.
3	Double-click **Page Push URLs**.
4	In the **Page Push URLs** dialog box, select the skillset for which you want to add new URLs.
5	Click **Edit**.
6	In the **Edit Push Page URL** dialog box, in the URL box, type the URL for the Web site to add to the list appearing in Contact Center Agent Desktop for the selected skillset.
7	In the **Description** box, type a description for the Page Push URL that describes the URL that the agent can push. The description field cannot be blank. *Agents can use the URL or the description in the Contact Center Agent Desktop to select the URL that they want to push.*
8	Click **Add**.
9	Click **Save**.
10	Click **Close**.

--End--

Deleting a page push URL

Delete a page push URL to remove it from the list of pages the agent can push to customers during an instant message or Web communications.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **WebComms & IMs Administration**.
3	Double-click **Page Push URLs**.

4	In the **Page Push URLs** dialog box, select the skillset for which you want to change the URLs.
5	Click **Edit**.
6	In the **Edit Page Push URLs** dialog box, in the **URL** box, select the URL to delete.
7	Click **Remove**.
8	Click **Save**.
9	Click **Close**.

--End--

Configuring contact timers

Configure the contact timers for Web communications or instant message conversations in your Contact Center.

You can configure the following:

- the interval in minutes and seconds between heartbeat pulses that check to see if both ends of the instant message are open
- the refresh time for Agent Desktop instant messages
- the time after which the conversation indicator on the Agent Desktop changes color to indicate that the desirable time for an agent response was exceeded
- the time after which the conversation indicator on the Agent Desktop changes color to indicate that the desirable time for a customer response was exceeded

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator window**, expand **Contact Center Multimedia**.
2	Expand **WebComms & IMs Administration**.
3	Double-click **WebComms Configuration**.

4 In the **WebComms Configuration** dialog box, in the **Keep Alive** box, type the interval in minutes and seconds between heartbeat pulses that check to see if both ends of the instant message are open.

5 In the **Message Refresh** box, type the refresh time for Agent Desktop instant messages.

6 In the **Desirable Response (Customer awaiting Agent)** box, type the time after which the conversation indicator on the Agent Desktop changes color to indicate that the desirable time for an agent response was exceeded.

7 In the **Desirable Response (Agent awaiting Customer)** box, type the time after which the conversation indicator on the Agent Desktop changes color to indicate that the desirable time for a customer response was exceeded.

8 Click **Save**.

--End--

Variable definitions

Variable	Value
Message Refresh	The refresh time for Agent Desktop instant messages.
Keep Alive	The interval in minutes and seconds between heartbeat pulses that check to see if both ends of the instant message are open.
Desirable Response (Agent to Customer)	The time after which the conversation indicator on the Agent Desktop changes color to indicate that the desirable time for an agent response was exceeded.
Desirable Response (Customer to Agent)	The time after which the conversation indicator on the Agent Desktop changes color to indicate that the desirable time for a customer response was exceeded.

Configuring automatic text

The automatic text for a Web communications or instant message session includes a welcome message for customers who initiate the contact, and labels for the agent and customers in the text conversation.

Configure the welcome message for all skillsets, or for a single skillset. The customer chooses the skillset when they initiate the contact.

Procedure steps

Step	Action
1	In the Contact Center Multimedia Administrator application, expand **Contact Center Multimedia**.
2	Expand **WebComms & IMs Administration**.
3	Double-click **WebComms Resources**.
4	In the **WebComms Resources** dialog box, in the **Welcome Message** box, type the message to appear at the beginning of every contact. The maximum size for this message is 200 characters.
5	In the **Agent Label** list, select the label to appear at the beginning of the agent contact list.
6	In the **Customer Label** box, type the text to appear at the beginning of the customer responses in the contact.
7	To create a customer welcome message for a skillset, under **Custom Welcome Messages**, select a skillset.
8	Click **Edit**.
9	In the **Welcome Message** box of the **Edit Welcome Message** dialog box, type the welcome message for the skillset.
10	Click **Save**.

--End--

Variable definitions

Variable	Value
Agent Label	The label that appears beside the text typed for the agent. • Agent Label: Type the text to appear at the beginning of the agent responses in the contact. The maximum size of this label is 50 characters. • First Name: The first name of the agent appears at the beginning of the agent responses in the contact (for example, John). • First Name Last Name: The first and last name of the agent appear at the beginning of the agent responses in the contact (for example, John Smith). • Last Name, First Name: The last name of the agent, followed by the first name of the agent appears at the beginning of the agent responses in the contact (for example, Smith, John).
Customer Label	The text to appear at the beginning of the customer responses in the contact. The maximum size of the Customer Label is 50 characters.

Configuring customer notification log

Configure the customer notification log information to prepare to send an e-mail to the customer of the written conversation.

Prerequisites

- Configure an outgoing e-mail address to use to send the log file to the customer.
- Configure the Web communication skillsets.

Procedure steps

Step	Action
1	In the Contact Center Multimedia Administrator application, expand **Contact Center Multimedia**.

2	Expand **Webcomms & IMs Administration.**
3	Double-click **WebComms Configuration**.
4	The **WebComms Configuration** dialog box appears.
5	Under **Chat Conversation**, select **E-mail Chat Log to Customer**.
6	Click **Save**.

--End--

Creating WebComms Web On Hold URLs groups

Web-on-hold is a sequence of URLs presented automatically to a customer's Web browser while the customer waits for an agent for an instant message. You can define the time that each URL appears on the customer's Web browser.

Web-on-hold URLs can include multimedia formats, such as video clips (Quick Time) or audio files (MPEG3). However the customer's browser must be able to play these formats. Customers are responsible for plug-ins needed to run multimedia files.

Nortel recommends that you use no more than 25 URLs in each Web-on-hold group.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **WebComms & IMs Administration**.
3	Double-click **WebComms Web On Hold URLs**.
4	In the **WebComms Web on Hold URLs** dialog box, click **New**.
5	In the **New Web On Hold URL Group** dialog box, in the **Tag** box, type a name for the new Web-on-hold group.
6	In the **Description** box, type a description for the Web-on-hold group.
7	In the **Hold Time** box, type the number of seconds to display each URL in the Web-on-hold group on the customer's browser.

8 In the **Sequence** box, type a number, from 1 to 10 that represents the order of the URL you are configuring.

9 In the **URL** box, type the URL to display on the customer's Web browser.

10 Click **Add**.

11 After you add all URLs to the current Web-on-hold group, click **Save**.

12 Click **Close**.

--End--

Changing the sequence of a WebComms Web On Hold URLs group

Change the sequence of a Web-on-hold group to change the order in the list of Web pages that appear to customers.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **WebComms & IMs Administration**.
3	Double-click **WebComms Web On Hold URLs**.
4	In the **Current Web On Hold URLs** window, select a URL.
5	In the **WebComms Web On Hold URLs** dialog box, click **Edit**.
6	In the **Edit Web On Hold URL Group** dialog box, in the **Web On Hold URL Group Properties** box, select the URL to change the order of appearance.
7	In the **Sequence** box, type a number from 1 to 10 that represents the order of the URL you are configuring.
8	After you change the sequence of a URL, click **Save**.
9	Click **Close**.

--End--

Deleting a URL from a WebComms Web On Hold group

Delete a URL from a Web-on-hold group if the URL is not available.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **WebComms & IMs Administration**.
3	Double-click **WebComms Web On Hold URLs**.
4	In the **WebComms Web On Hold URLs** dialog box, select the Web-on-hold group to delete the URL from.
5	Click **Edit**.
6	In the **Edit Web On Hold URL Group** dialog box, in the **URLs in Group** box, select the URL to delete.
7	Click **Remove**.
8	Click **Save**.
9	Click **Close**.

--End--

Deleting a WebComms Web On Hold group

Delete a Web-on-hold group to avoid displaying the Web pages to the customer during Web communications contacts.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **WebComms & IMs Administration**.
3	Double-click **WebComms Web On Hold URLs**.
4	In the **WebComms Web On Hold URLs** dialog box, select the Web-on-hold group to delete the URL from.

5 Click **Edit**.

6 In the **Edit Web On Hold URL Group Properties** dialog box, in the **URLs in Group** box, select the URL to delete.

7 Click **Remove**.

8 Click **Save**.

9 Click **Close**.

--End--

Web communications customer interface configuration

If you use Web communications in your contact center, you can use the Sample Customer Interface (CI) Web site implementation to help you develop pages for your corporate Web site. The Web services architecture is a platform-independent interface that customers can access from both Microsoft .NET and Java applications. Customer Web sites or third-party applications use the open interface for integration with the Nortel Contact Center Multimedia system.

In development, you can access the Web services from either ASP.NET or JSP Web applications.

The Customer Interface Web services provide a range of methods to perform the following functions:

- register new customers in the Contact Center Multimedia database
- log on or log off existing customers
- update customer logon credentials
- create customer contacts
- update customer details
- read customer information
- review a customer contact history
- request immediate or scheduled callback requests
- read a contact
- create and maintain a Web communications chat session

For developers who want to integrate with the Nortel Contact Center Multimedia system using Web Services, the following items are available on the Nortel Developer Partner Program Web site:

- Web Service documentation including an API reference in HTML format
- an installation package for the Sample Customer Interface Web site

You can use the sample implementation as a reference to help you develop a live customer Web site.

This section contains the following topics:

- functionality and .jsp pages available in the reference implementation
- customizable settings for the Sample Customer Interface
- steps to test the customer interface Web site

Navigation

Using the sample customer interface Web site

Use the sample Customer Interface (CI) Web site to demonstrate the basic functions available through the Web services and to test the Contact Center Multimedia in a lab environment.

Prerequisites

- You must create customer user names in the format of a valid e-mail address, such as user@nortel.com. You must use valid user names to test the sample CI Web site and to deploy custom Web sites.
- Create scheduled callbacks with an outbound skillset (OB_) as scheduled callback contacts are licensed under the outbound license. Agents must have an Outbound license to originate a call to a customer.
- You must convert the time to the local time for the customer who receives the outbound call. The time displayed on Contact Center Manager Administration is in Greenwich Mean Time (GMT).
- The To address of an e-mail message must be a recipient mailbox configured in Contact Center Multimedia Administrator.

- The EM_Default_Skillset must have an outgoing e-mail address mapped in the Multimedia Administrator for password reminder requests from the sample CI Web site.

Procedure steps

Step	Action
1	Access the sample CI Web site using the URL: http://<webserver>:8080/CI_Sample_Website; <webserver> is the host name of the Web server where you installed the sample CI Web site.

Attention: The default port for Apache Tomcat server is 8080. For information about changing the default port, see the Apache Tomcat documentation.

Step	Action
2	View the sample CI Web site pages to understand how the CI web site functions.

--End--

Procedure job aid

Pages and functions available in the sample CI Web site

Page	Function	Notes
registerNewCustomer.jsp	New customers can register their contact information in the Contact Center Multimedia database	Customers can enter their title, first name, last name, e-mail address, password, postal address, and telephone number. When the form is submitted, the information is passed to registerNewCustomer_WSClient.jsp, which invokes the registerNewCustomer Web method to create the new customer in the Contact Center Multimedia database.
loginCustomer.jsp	Existing customers can enter their user name and password to log on.	When the form is submitted, the user name and password are passed to loginCustomer_WSClient.jsp, which invokes the customerLogin Web method. If the customerLogin method returns an error code indicating that the customer is already logged on, and then the customerAlreadyLoggedIn.jsp page is displayed. If the customer chooses Yes to continue, then the loginCustomer_WSClient.jsp is loaded again with the forceLogoff parameter equal to True. The page logs off the customer using the CustomerLogoff Web methods and then logs on the customer again using the CustomerLogin Web method. The customerLogin Web method returns a session key if the customer logs on successfully. The session key is required to call other Web methods for the customer, so it is stored as a session variable that can be used by other .jsp pages in the sample CI Web site. When the customer logs on to the Web site, the sample page appears. Customers use the opening page to request a text chat, a callback, or an e-mail message from the contact center.

Pages and functions available in the sample CI Web site

Page	Function	Notes
logoffCustomer.jsp	This page contains the user name and Logoff button and is used to log off existing customers.	When the form is submitted, the user name is passed to the page logoffCustomer_WSClient.jsp, which invokes the customerLogoff Web method to log the customer off the Web site.
readCustomerDetails_WSClient.jsp	Existing customers can add or edit details in their contact information.	When the customer adds or updates information and clicks Update Details, the form is passed to updateCustomer_WSClient.jsp, which invokes the Web methods updateCustomer, updateAddress, updateEmailAddress, and updatePhoneNumber. If the information in the fields is new, updateCustomer_WSClient.jsp invokes the Web methods addAddress, addEmailAddress, and addPhoneNumber. The results of the updates appear in the updateCustomer_WSClient.jsp page.
updateCustomerLogin.jsp	Existing customers can change their user name and password.	When the form is submitted, the old password and new password are passed to updateCustomerLogin_WSClient.jsp, which invokes either the updateUsername or updatePassword Web method, depending on the information the customer updates.

Pages and functions available in the sample CI Web site

Page	Function	Notes
readCustContactHist_WSClient.jsp	Existing customers can display their contact history and view the last 20 contacts associated with a customer.	The customer can navigate blocks of 20 contacts by using the navigation arrows above the contact history. You can configure the number of contacts displayed on this page by modifying the NO_OF_CONTACTS_TO_DISPLAY property in the web.xml file in the webapps\CI_Sample_Website|WEB_INF folder. This page uses one of four web methods to retrieve the correct block of contacts: • ReadFirstBlockOfContacts • ReadLastBlockOfContacts • ReadNextBlockOfContacts • ReadPreviousBlockOfContacts The Web method that is called is controlled by the parameter pageControl which can have the value of first, last, next, or previous, depending on the navigation arrow the customer clicks. Another parameter, startContactID, is called when pageControl is either previous or next to call the Web methods ReadPreviousBlockOfContacts and ReadNextBlockOfContacts, with the correct contact ID used as a starting point. When a customer clicks any contact ID in the history list, the readContact_WSClient.jsp page invokes the readContact Web method to read the contact details from the Contact Center Multimedia database and display the information.

Pages and functions available in the sample CI Web site

Page	Function	Notes
requestTextChat.jsp	Customers can request a text chat session with an agent.	When the customer requests a text chat session, the skillset, subject, and objective are passed to requestTextChat_WSClient.jsp. The requestTextChat_WSClient.jsp page uses the IsSkillsetInService Web method to verify whether the selected skillset is in service before creating the Web communications contact. If the skillset is in service, then the contact is routed to the skillset. The Web contact is created as a new contact in the Contact Center Multimedia database using the requestTextChat Web method with the createAsClosed parameter equal to False. The customer is directed to the Web communications URL http://<webserver>:8080/WebComms/jsp/index.jsp; <webserver> is the host name of your Web server. The requestTextChat Web method passes the session key of the currently logged on customer and the contact ID of the new Web communication contact to the Web communications URL. The text chat page appears on the customer desktop. For example, your Web communications URL can be http://<webserver>:8080/WebComms/jsp/index.jsp?sessionKey=2qrc3E7a00&contactID=637142 To display the customer text chat window, the customers are redirected to this URL using the session key and contact ID parameters. If the skillset is not in service, then a message appears indicating that the requested skillset is not in service and a closed Web communications contact is created as a record of the customer’s attempt to request a text chat. The closed Web contact is created using the RequestTextChat Web method with the createAsClosed parameter equal to True.

Pages and functions available in the sample CI Web site

Page	Function	Notes
requestScheduledCallback .jsp	Customers can request a scheduled callback at a specified date and time from an agent.	The getOutboundSkillsets_WSClient.jsp Web method within this page displays a list of outbound skillsets. The time for the callback appears in the Outbound Campaign tool on Contact Center Manager Administration on the Progress and Results screen. The time appears in Greenwich Mean Time (GMT). When the form is submitted, the Callback Time is converted to milliseconds. This value is stored in a hidden form input variable called callback_time_milliseconds, which is passed along with the values of the other fields to the RequestScheduledCallback_WSClient. jsp page. The RequestScheduledCallback_WSClient jsp page calls the requestScheduledCallback Web method to create the scheduled callback contact in the Contact Center Multimedia database.

Pages and functions available in the sample CI Web site

Page	Function	Notes
requestImmediateCallback.jsp	Customers can request an immediate callback from an agent.	The getOutboundSkillsets_WSClient.jsp page displays a list of outbound skillsets. An immediate callback is treated as a scheduled callback contact with the current Multimedia server date and time entered as the callback date and time. When the form is submitted, the values of the fields are passed to the requestImmediateCallback_WSClient.jsp page, which first verifies whether the chosen skillset is in service using the IsSkillsetInService Web method. If the skillset is not in service, then the scheduled callback contact is created using the requestImmediateCallback and a message appears indicating that the callback request is handled when the skillset is in service. If the skillset is in service, then the scheduled callback contact is created using the RequestImmediateCallback method and the confirmation message appears.
submitHTMLForm.jsp	Customers can submit HTML forms as an e-mail message to an agent.	When this form is submitted, the values of the input fields are passed to sendmail.jsp. The sendmail.jsp page uses the JavaMail libraries and SMTP server (configured during installation) to send an e-mail message to the specified To address using the customer default e-mail account. The values in the Text Field 1, Text Field 2, Choice 1, Choice 2, and Text Area fields in the form are sent in the body of the e-mail message. No CI Web service methods are used to send the HTML form as an e-mail message. You can configure the Contact Center Multimedia rules to route these e-mail messages to a specific skillset based on keywords in the e-mail subject.

Pages and functions available in the sample CI Web site

Page	Function	Notes
passwordReminder.jsp	Customers can enter their e-mail address and retrieve their password to log on to the Web site.	When this form is submitted, the e-mail address entered by the customer is passed to the passwordReminder_WSClient.jsp page. The sendPasswordReminder Web method resets the customer password and sends the customer the password reminder auto-response configured in the Contact Center Multimedia Administrator. The EM_Default_Skillset must have an outgoing e-mail address mapped in the Multimedia Administrator for password reminder requests from the sample CI Web site. You can configure a different skillset for password reminder requests by configuring the PASSWORD_REMINDER_SKILLSET property in the web.xml file in the webapps\CI_Sample_Website\WEB_INF folder. The text of the password reminder is configured in the Contact Center Multimedia Administrator in auto-responses. If the e-mail address entered in the form does not correspond to the e-mail address of an existing customer in the Multimedia database, the customer receives a message indicating that they cannot log on.
loginCustomer_timeout.jsp	If the customer attempts to use the sample pages after a session expires, a session timeout message displays and the customer can log on again.	A customer session on the sample CI Web site times out after 10 minutes of inactivity. You can change the session timeout value in the web.xml file for the sample CI Web site.

Pages and functions available in the sample CI Web site

Page	Function	Notes
Web-on-hold	Web-on-hold automatically displays a Web page or group of Web pages to customers while they are waiting for an agent to begin their text chat.	You can define the length of time that each URL appears on the customer Web browser. You can use business logic (such as region of customer or time of year) to program which Web-on-hold page or group of pages to display to various users. When the agent joins the conversation, the Web-on-hold page is replaced and the session is in progress.
Text chat frame	The text chat frame displays a complete record of the current chat conversation between an agent and a customer.	Only four or five lines of text are visible in the frame, but you can scroll up or down to view the entire text of the conversation. The frame displays the URL of any pages viewed or pushed by the agent or the customer.

Configuring properties for the sample customer interface Web site

Configure properties for the sample customer interface by editing the web.xml file. Various settings are customizable, including host name, port number, and Web site path.

Procedure steps

Step	Action
1	Access the web.xml file for the sample customer interface Web site in the webapps\CI_Sample_Website\WEB_INF folder of the Tomcat Servlet container.
2	Configure the items to customize.
3	Save and close the web.xml file.

--End--

Procedure job aid

Sample customer interface Web site items available for configuration

Item	Description
CCMM_HOSTNAME	The name of the Contact Center Multimedia server on which the customer interface Web services are located.
EMAILSERVER_HOSTNAME	The host name of the e-mail server used to send e-mail using Java mail and Standard Mail Transfer Protocol (SMTP). The sendmail.jsp page uses SMTP to send e-mail messages to a Multimedia recipient address. The e-mail server must be able to relay e-mail messages to an e-mail server configured in Contact Center Multimedia.
PASSWORD_REMINDER_SKILLSET	The value of PASSWORD_REMINDER_SKILLSET is used by the passwordReminder_WSClient.jsp page. Password reminder e-mail contacts are created as closed contacts within this defined skillset. By default, the password reminder skillset is set to EM_Default_Skillset.
WEBCOMMS_HOSTNAME	The host name of the Web server hosting the Web communications application.
WEBCOMMS_PORT	The port number used by the Web communications application. The default value is 8080.
WEBCOMMS_PATH	The URL path used to access the Web communications application. The default path is /WebComms/jsp/index.jsp.
HTML_FORM_TO_ADDRESS	The default To e-mail address on the page submitHTMLForm.jsp. The HTML_FORM_TO_ADDRESS must be a valid Multimedia recipient address.
HTML_FORM_SUBJECT	The default subject on the page submitHTMLForm.jsp. The default subject is HTML Form Submitted from the Web.
HTML_FORM_RESULT_HEADER	The value used as the first line in the body of e-mail messages sent from the sendmail.jsp page. The default body text is Results of HTML Form Submitted from the Web.
TEXT_CHAT_SUBJECT	The default subject displayed on the requestTextChat.jsp page. The default subject is Text Chat Submitted from the Web.
NO_OF_CONTACTS_TO_DISPLAY	The number of contacts to display on the Read Customer Contact History page.
<session-timeout>10</session-timeout>	The number of minutes before a customer chat session expires on the Customer Interface Web site. If the customer session expires, the customer must log on again. The default value is 10 minutes.

Testing the customer interface Web site

Test the customer interface Web site to verify that the Web site is installed properly. First, go to the Web site. After the home page opens, you must test procedures to ensure the customer interface Web site works:

- creating a customer
- testing request text chat
- testing request callback functionality
- testing e-mail from Web pages

Prerequisites

- You must have at least one Web communications skillset configured and at least one agent configured who can handle contacts with the Web communications skillset.

Procedure steps

Step	Action
1	Start your Web browser from the Tomcat homepage. If you use the default port for the Apache Tomcat server, the url for the Tomcat homepage is http://<webservername>:8080.
2	Confirm that the sample customer interface homepage opens to http://<webservername>:8080/CI_Sample_Website/.

--End--

Creating a test customer

Create a test customer, using a predefined e-mail and phone number, to use with testing procedures on the customer interface Web site.

Prerequisites

- Ensure that you create an e-mail address and phone number available for the test customer you defined.

Procedure steps

Step	Action
1	Click **Register New Customer**.
2	Enter the **Title**, **First Name**, **Last Name**, **Username**, **Password**, **E-mail Address**, **Confirm Password**, and **Number** for your test customer. You can add other details about the customer.
3	To log on this customer immediately after you create, select the **Login Customer** check box. **OR** Click **Log in Customer** to log on this customer now.
4	In the **Username** box, type the test customer user name.
5	In the **Password** box, type the test customer password.
6	Click **Log on**.

--End--

Testing request text chat

Text request text chat to ensure that a customer can submit chat and a Contact Center agent can receive the Web communications content.

Prerequisites

- Ensure that an agent is configured who has the Web communications skillset and can receive contacts.

Procedure steps

Step	Action
1	Log on the test customer.
2	Log an agent who can handle a Web communications skillset on to the **Contact Center Agent Desktop**. Make the agent available to receive contacts.
3	Click **Request Text Chat** to create a text chat contact.
4	In the **Skillset** box, select a skillset that your agent from step 2 is eligible to handle.
5	In the **Subject** box, type a subject for the text chat.

6 Click **Submit**.

7 On the **Contact Center Agent Desktop**, confirm that the logged on agent receives the Web communications contact from the test customer.

8 Close the test contact.

9 Log off the test customer.

--End--

Procedure job aid

Various Web communications settings prevent blocked invitations to ensure that customers with limited Internet access can chat with a Contact Center agent. The following customer settings and processes enable customers and agents to use chat processes effectively:

- The Web Communications Manager relies on the HTTP protocol to transport messages between the agent and customer using Web service read and write calls. Because all traffic goes through port 80, no new ports need to be opened through the firewall. This means that customers based in corporations with limited Internet access can chat with an agent.
- Initially, a customer is placed in Web-on-hold to wait for an agent to join the call. The customer browser is redirected to a frame-based Web page that displays video and interactive content while the customer waits for the agent. The customer Web browser is redirected to the chat conversation when the agent joins the session.
- Among the exchanged messages, a request can be made to have a Web page pushed to the other party. The message asks the customer or agent to load a URL. The agent and customer loads separate copies of the same URL thus safeguarding privacy by not sharing cookies or personalized pages. In addition, existing controls in place by customer or agent internet access is respected. For example, an agent cannot push sites barred by a contact center IT department to an agent by a customer.
- The capability of many browsers to prevent pop-up windows do not affect the text chat conversations between customers and agents. All pages pushed from the agent to the customer load within the central frame above the text chat conversation and no separate pop-up windows appear.
- As with any Internet connection, it is important for customers and contact centers to maintain current antivirus definitions and antispyware.

Testing request callback functionality

Test request callback functionality to ensure that a customer can submit a request for a callback and that a Contact Center agent can receive the request.

Prerequisites

- Ensure that an agent is configured who has an Outbound skillset and can receive contacts.

Procedure steps

Step	Action
1	Log on the test customer.
2	Log an agent who can handle an Outbound skillset on to the **Contact Center Agent Desktop.** Make the agent available to receive contacts.
3	Click **Request Immediate Callback** to create an outbound contact.
4	In the **Skillset** box, select a skillset that the agent from step 2 is eligible to handle.
5	In the **Subject** box, type a subject for the outbound contact.
6	In the **Objective** box, type a summary of the reason for the callback.
7	Click **Submit**.
8	On the **Contact Center Agent Desktop**, confirm that the logged on agent receives the outbound contact from the test customer.
9	Close the test contact.
10	Log off the test customer.

--End--

Testing e-mail from Web pages

Test e-mail from Web pages to ensure that a customer can submit an e-mail and that a Contact Center agent can receive the e-mail.

Prerequisites

- Ensure that an e-mail message box is already configured that assigns e-mail messages to the skillset to which you log on your Contact Center agent.

Procedure steps

Step	Action
1	Log on the test customer.
2	Log an agent who can handle an e-mail message skillset on to the Contact Center Agent Desktop. Make the agent available to receive contacts.
3	Click **Submit HTML Form** to create an e-mail contact.
4	In the **Mail To** box, type an e-mail message to be forwarded to the agent who is logged on.
5	In the **Subject** box, type a subject for the e-mail message.
6	Click **Submit**.
7	On the **Contact Center Agent Desktop**, confirm that the logged on agent receives the e-mail message from the test customer.
8	Close the test contact.
9	Log off the test customer.

--End--

Contact Center Agent Desktop configuration

Contact Center Multimedia administrator has settings that you can use to configure properties in the Contact Center Agent Desktop (CCAD) to help the agents access database information.

You can edit the file CCADIntrinsicSettings.xml to configure the following CCT Intrinsic items:

- CCT application list
- CCT intrinsics
- Auto Launch applications

Use the procedures in this chapter to configure the Contact Center Agent Desktop settings.

Prerequisites for CCAD configuration

- Log on to the Contact Center Manager Administration application.

Navigation

Resetting an agent password

Reset an agent password if the agent forgets it or if you need to reset the password for any other reason.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia.**
2	Expand **General Administration.**
3	Double-click **Agent Settings.**
4	The **Agent Settings** window appears.
5	Select the agent whose password you want to reset.
6	Click **Reset Password.** The default password is the same as the agent's logon ID.
7	Click **Save**.
8	Click **Close**.

--End--

Creating or changing custom fields in CCAD

You can add a custom field to the Contact Center Agent Desktop for multimedia contacts that pertains to your contact center. For example, if your customers subscribe to a magazine, you can view information about each customer's subscription expiry date.

The value entered by the contact center agent for each customer appears in the custom field, the same as any other customer-entered information such as e-mail address or telephone numbers.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administration** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Customer Custom Fields**.
4	If you create a new field, click **New**.
5	If you edit an existing field, click **Edit**.
6	In the **Field** box, type the label for your custom field.
7	Click **Save**.
8	Click **Close**.

--End--

Deleting a custom field in CCAD

Delete a custom field from the Contact Center Agent Desktop when it is not required.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administration** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Customer Custom Fields**.
4	Select a custom field.
5	Click **Delete**.
6	In the confirmation dialog box, click **OK**.
7	Click **Close**.

--End--

Configuring the active contact timer

Configure the hours and minutes that you want a contact to remain open on a desktop without activity.

When this time expires, the contact is automatically placed into pending state. The default time in the Contact Center Multimedia (CCMM) configuration is 1 hour (60 minutes). The actual time that the contact can be open on the desktop without activity is 1 hour less than the maximum open duration for contacts as defined on Contact Center Manager Server.

The default maximum open duration on the Contact Center Manager Server is 2 hours. See the Contact Center Manager Server documentation for more information about the Contact Center Manager Server maximum open duration.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administration** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Agent Desktop Configuration**.

4	In the **Open Duration** box, type the maximum number of hours and minutes that you want contacts to be active before they move to pending state.
5	Click **Save**.

--End--

Configuring the callback timer

Configure the default time in days, hours, and minutes to wait before re offering a pending contact to agents. An agent can delay the contact, or place the contact into pending state because they are waiting for additional information to complete the contact.

The callback timer can be 2 minutes to 200 days (about 6 months). The default range provides the limits to which the you configure the callback time. The actual time value is chosen in the Contact Center Agent Desktop application when the agent reschedules the contact.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administration** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Agent Desktop Configuration**.
4	In the **Minimum Time** box, if required change the default number of minutes to wait before presenting contacts that the agent places into pending state.
5	In the **Maximum Time** box, if required change the default number of days to wait before presenting contacts to the agent again.
6	Click **Save**.

--End--

Configuring the callback trunk access

Configure the callback trunk access to ensure that you can create a callback to the customer you work with in your Web communications contact. The customer can request a callback, and you can schedule callbacks.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Contact Center Agent Desktop**.
3	Double-click **WebComms Configuration**.
4	The **WebComms Configuration** dialog box appears.
5	In the **Trunk Access Code** box, type the number an agent needs to dial to access an external line.
6	Click **Save**.

--End--

Specifying the attachment size

Specify the maximum size of the attachments that an agent can attach to an e-mail message.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administration** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Agent Desktop Configuration**.
4	In the **Attachment Upload Size** box, type the maximum number of kilobytes (KBs) that each file can be.
5	Click **Save**.

--End--

Configuring Agent Desktop behavior

You can configure whether the Agent Desktop is given focus when a new contact arrives.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administration** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Agent Desktop Configuration**.
4	Under **New Contact Presentation**, select the check boxes that describe the presentation.
5	Click **Save**.

--End--

Variable definitions

Variable	Value
New Contact Presentation	The method in which contacts are presented: • Bring to Front: The Agent Desktop moves to the front upon arrival of a new contact. If Bring to Front is disabled, the Agent Desktop makes a warning sound and the toolbar flashes, but it is not brought to the front. • Give Focus: The Agent Desktop window is the active window when it moves to the front. The Bring to Front check box must be selected for the Give Focus check box to be enabled.

Configuring audible alerts

Configure your Contact Center Agent Desktop so that an agent can hear a beep when a contact arrives at their desktop. The agent's computer must contain an appropriate sound card.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administration** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Agent Desktop Configuration**.
4	Under **New Contact Presentation**, select the **Audible Alert** check box.
5	Click **Save**.

--End--

Configuring the visual alert

Configure your Contact Center Agent Desktop so that an agent can see the incoming contact when it arrives at their desktop. You can configure the Contact Center Agent Desktop to move to the front of the desktop to cover all current windows, and give focus to the Contact Center Agent Desktop window so that actions in other windows stop. To give focus to the window, select the Bring to Front check box.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia** Administration window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Agent Desktop Configuration**.
4	To bring the **Contact Center Agent Desktop** window to the front, under **New Contact Presentation**, select the **Bring to Front** check box.

5 To make the **Contact Center Agent Desktop** window active, under **New Contact Presentation**, select the **Give Focus** check box.

6 Click **Save**.

--End--

Configuring the state of the Agent terminal on log off

Configure the agent terminal to be in either idle or busy state when the agent logs off of the Contact Center Agent Desktop.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administration** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Agent Desktop Configuration**.
4	Under **Logoff Terminal State**, select **Idle** or **Busy**.
5	Click **Save**.

--End--

Configuring hotdesking

Configure your contact center so that an agent can sit at a different desk every day and log on to the Contact Center Agent Desktop. With hotdesking enabled and properly configured, when agents start the Contact Center Agent Desktop, they automatically map to the relevant terminal and addresses without user intervention.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administration** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Hot Desking**.
4	Under **Hot-Desking**, select the **Enabled** check box.
5	Click **Save**.

--End--

Configuring hotdesking in a Citrix environment

When hotdesking is configured for a Citrix environment, agents are see a dialog box that asks them to enter a string that identifies their workstation. The string must be the same as the string that is configured as the workstation name in the Communication Control Toolkit configuration. You must configure the dialog box in a Citrix environment.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administration** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Hot Desking**.
4	If you work in a Citrix environment, select the **Prompt for WorkStation** check box.
5	Click **Save**.

--End--

Creating or changing a closed reason

Indicate a reason for closing a contact.

If no closed reasons are configured in the Administrator application, then the agent is not required to choose a closed reason. If one or more closed reasons are configured, then the agent must choose a closed reason to close the contact.

By default, no closed reasons are configured.

You can also assign a default closed reason to each contact type. The default reason is selected in the Agent Desktop application. The agent can choose another closed reason when closing a contact.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Closed Reasons**.
4	To change a closed reason, select the closed reason, and then click **Edit**.
5	To create a new closed reason, click **New**.
6	In the **Closed Reason Text** box, type the text for the closed reason (maximum 50 characters). The text should be as descriptive as possible.
7	In the **Contact Type** box, select the type of contact to which you want to apply the closed reason text. You can choose e-mail, Web communications, or all types of contacts.
8	Click **Save**.
9	In the **Default Closed Reason**s box, beside **E-mail**, select the configured closed reason to apply to e-mail messages by default.
10	In the **Default Closed Reasons** box, beside **Web Comms**, select the configured closed reason to apply to Web communications contacts by default.
11	Click **Save**.
12	Click **Close**.

--End--

Deleting a closed reason

Delete a closed reason if you do not want the reason to appear in the Agent Desktop application.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.

3	Double-click **Closed Reason**.
4	Select a closed reason from the list.
5	Click **Delete**.
6	In the confirmation dialog box, click **OK**.
7	Click **Close**.

--End--

Configuring Multiplicity

Configure Multiplicity feature to allow agents in your contact center to use this feature.

Prerequisites

- Ensure that you have Contact Center Multimedia Administrator.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Multiplicity Settings**.
4	In the Multiplicity Settings dialog box, click **Enable Multiplicity** checkbox.
5	In the **Maximum number of simultaneous contacts** field, type <max contacts>.
6	In the **Time Delay for Additional Contact Button** field, type <seconds>.

--End--

Variable definitions

Variable	Value
<max contacts>	The maximum number of web communications contacts that you allow each agent to accept. You can configure one to five additional contacts.
<seconds>	The delay in seconds between the time that an agent accepts a web communications contact and the Additional Contact button enables. You can configure zero to 600 seconds.

Importing an Active Directory user to CCMM

To add an agent to the Experts list, you must import the agent to CCMM.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Expert Administration**.
4	In the **Expert Administration** window, in the **Connect to AD as** section, type your username and password.
5	In the **Connect to CCMM as section**, type your username and password.
6	Select the agents' names to import.
7	Click **Import**. The agent name appears in the Experts list.

--End--

Creating an expert group

After you create an experts group, agents in your contact center can consult Instant Experts groups after they log on to CCAD.

Prerequisites

- Log on to CCMM.
- Ensure that you have agent names in the Experts list.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Expert Administration**.
4	In the **Groups** section, click the New button.
5	In the **New Expert Group** dialog box, type the <group name>.
6	Click **OK**.

--End--

Variable definitions

Variable	Value
<group name>	There are three types of Instant Experts groups: • Groups that automatically display after an agent logs on to CCAD. These group names begin with an underscore (_), for example, _autoload. • Groups that automatically display with associated skillsets. • Groups that display after an agent clicks on a highlighted keyword in a text chat with a contact.

Adding an agent to an expert group

After you create an Instant Experts group, add the agents that you require for the group.

Prerequisites

- Log on to CCMM.
- Ensure that you have existing expert groups.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Expert Administration**.
4	In the **Experts** list, click the agent name to add to the experts group.
5	In the **Groups** section, click the required group name.
6	Double-click **Group**.
7	In the **Groups** section, click the Refresh button. The agent name appears in the Contains Experts list.

--End--

Deleting an agent from an expert group

If an agent is no longer available, remove the agent name from the Experts list.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Expert Administration**.

4	In the **Groups** section, click the group name to modify.
5	In the **Contains Experts** section, click the agent name to remove from the group.
6	Under the **Contains Experts** section, click **Remove**.
7	In the **Groups** section, click the Refresh button. In the **Contains Experts** section, the agent name no longer appears.

--End--

Deleting an agent from a skillset associated group

If an agent is no longer available, remove the agent name from a skillset associated group.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Expert Administration**.
4	In the **Skillset** list, click the required skillset.
5	In the **Contain Experts** list, click the agent name to remove.
6	Under the **Contains Experts** section, click **Remove**.
7	In the **Skillset** section, click the refresh button. The agent name no longer appears in the Contains Experts list.

--End--

Configuring the CCT intrinsic application list

Configure a CCT Intrinsic application list to launch an application from the list after an agent accepts a voice contact.

Prerequisites

- Log on to CCMM server.
- Ensure that you have the file CCADInstrinsicSettings.xml.

Procedure steps

Step	Action
1	Double-click CCADInstrinsicSettings.xml file.
2	After <ApplicationShortcut>List, enter <ApplicationShortcut>.
3	Type **<Name>**.
4	Type (Applicationname).
5	Enter **</Name>**.
6	Type **<path>**.
7	Type (path).
8	Enter **%VALUE% </path>**.
9	Enter **<ForceLaunch>(condition)</Forcelaunch>.**
10	Enter **<\ApplicationShortcut>**.
11	Repeat step 2 to step 10 for each application which you need to add for the CCT intrinsics.
12	On the menu toolbar, click **File**, **Save**.

--End--

Configuring CCT intrinsics

Configure CCT intrinsics that agents can access during a voice contact.

Prerequisites

- Log on to CCMM server.
- Ensure that you have the file CCADInstrinsicSettings.xml.

Procedure steps

Step	Action
1	Double-click CCADInstrinsicSettings.xml file.
2	After </ApplicationShortcutList>, enter <IntrinsicDetails>.
3	Enter <Name> skillset </Name>.
4	Enter <FriendlyName> skillset </FriendlyName>.
5	Enter <Display> true <Display>.
6	Enter <ForceLaunchIntrinsic> false </ForceLaunchIntrinsic>.
7	Enter </IntrinsicDetails>.
8	Repeat step 3 to step 7 for each CCT intrinsic.
9	Type </IntrinsicDetailsList>.

--End--

Configuring an Auto Launch application

To authorize agents to enable or disable the Auto Launch Application, configure Auto Launch Application.

Prerequisites

- Log on to CCMM server.
- Ensure that you have the file CCADInstrinsicSettings.xml.

Procedure steps

Step	Action
1	Double-click CCADInstrinsicSettings.xml file.
2	To authorize agents to disable an Auto Launch application, after </IntrinsicDetailsList>, enter <ApplicationForceEditable> true </ApplicationForceEditable>.
3	To restrict agents from editing an Auto Launch application, after </IntrinsicDetailsList>, enter <ApplicationForceEditable> false </ApplicationForceEditable>.

--End--

Predictive Outbound Administration

In a Predictive Outbound environment, the Pacing Algorithm forecasts the availability of an agent and originates calls on their behalf in order to maximize agent productivity. The Pacing Algorithm cannot guess the inbound call volume. After the Pacing Algorithm originates an outbound call on behalf of the agent, that agent cannot be consumed by a new arriving inbound call. Therefore, agents are exclusive to predictive outbound for a period of time. Agents cannot have an inbound and outbound skillset at the same time.

Predictive Outbound supports an advanced blending capability with which agents can move seamlessly between inbound and outbound queues as traffic levels change.

Predictive Outbound supports real-time blending of agents between inbound voice traffic and outbound dialing on a real-time basis, reacting to changes in inbound call volumes. The solution offers highly flexible agent blending to allow you to blend some/all agents between inbound voice queues and outbound dialing.

For more information, see *Nortel Contact Center Predictive Outbound* (NN44400-106).

Prerequisites

- Ensure that you have administrator access rights.

Navigation

- Configuring predictive blending settings (page 447)
- Configuring RTD Multicast settings (page 449)
- Configuring predictive outbound agent scripts (page 450)

Configuring predictive blending settings

The blending threshold class can include settings for multiple thresholds such as Average Wait Times, Agents Available, Abandoned Calls, and Service Levels. The next step is to identify which threshold to trigger the blending capability from.

Prerequisites

- Create a blending threshold class.

  For more information, see *Nortel Contact Center Predictive Outbound* (NN44400-106).

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Multimedia Server**.
2	Type your username and password.
3	Expand **Predictive Outbound Administration**.
4	Double-click **Blending Configuration**.
5	Select the **Enable Blending** check box.
6	From the **Threshold to Monitor** list, select a threshold class.

Attention: The blending service can monitor most of the thresholds listed in the following table.

Threshold Class	Notes
%Service_Level_for_Ans_Calls	—
Average_Answer_Delay_S	—
%Service_Level_S	—
Calls Waiting	—
Total Wait Time	—
Max Wait Time	—
Expected Wait Time	—
Calls Answered	—
Calls Answd Aft Threshold	—
Total Answered Delay	—
Agent Available	—
Agent In Service	—

Threshold Class	Notes
Longest Wait Since Last Call	Not available
Longest Wait Since Login	Not available
Agent Not Ready	—
Agent On This Skillset Call	—
Agent On DN Call	Not available
Agent Unavailable	—
Agent On Other Skillset Call	—
Agent On ACD-DN Call	Not available
Agent On NACD-DN Call	Not available
Call Offered	—
Call Abandon	—
Call Abandon Delay	—
Call Aband Delay Aft Threshold	—

7 In the **Skillset Monitor Settings** section, in the **Polling Interval** field, type the number of seconds.

8 In the **Skillset Monitor Settings** section, in the **Number of Agents to Reassign** field, type the number of agents to be assigned to the inbound skillset when the Level 2 threshold exceeds.

9 In the **Skillset Reversal Settings** section, in the **Polling Interval** field, type the number of agents you want the blending service to check inbound skillsets.

10 In the **Skillset Reversal Settings** section, in the **Number of Agents to Reassign** field, type the number of agents to return to the predictive outbound skillset when traffic falls below the Level 1 threshold.

--End--

Variable definitions

Variable	Value
Polling Interval (In the Skillset Monitor Settings section)	The frequency for which the inbound skillsets with the Blending_Template threshold assigned to are checked to determine if active predictive outbound agents are reassigned.
Number of Agents to Re-assign (In the Skillset Monitor Settings section)	The number of active predictive outbound agents who are also in standby priority on the inbound skillset and return to inbound if the Level 2 threshold exceeds.
Polling Interval (In the Skillset Reversal Settings section)	The frequency for which the inbound skillsets with the Blending_Template threshold assigned to is checked to determine if agents are returned to outbound (if, for example, the real-time value falls below the Level 1 threshold.)
Number of Agents to Re-assign (In the Skillset Reversal Settings section)	The number of transitioned agents that return to outbound in a polling cycle.

Configuring RTD Multicast settings

Configure the RTD Multicast settings for the real-time stream that the blending service monitors. These settings must match the multicast and port settings on Contact Center Manager Server.

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Multimedia Server**.
2	Type your username and password.
3	Expand **Predictive Outbound Administration**.
4	Double-click **Blending Configuration**.
5	Select the **Enable Blending** check box.
6	Click **Advanced**.
7	On the **RTD Multicast Configuration** window, in the **Multicast IP** box, type the IP address to which Contact Center Manager Server sends real-time statistics.

8 In the **Port Number** box, type the port number that the blending service monitors to receive real-time statistics.

9 Click **Save**.

--End--

Configuring predictive outbound agent scripts

After an agent receives an outbound contact, Contact Center Agent Desktop (CCAD) presents a script associated with the campaign. The script contains details from the customer record, and captures additional data during the course of the call. Also, the script can serve as a workflow, for the agent that branches to different pages depending on the progress of the call. These scripts are Web-based and are published on the CPSE2 Application Server.

CCAD needs to know the base URL where the scripts are published. Each campaign script is in a subdirectory of the base URL.

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Multimedia Server**, **CCMM Administrator**.
2	Enter your username and password.
3	Click **Login**.
4	Expand **Predictive Outbound Administration**.
5	In the **Predictive Agent Script Configuration** dialog box, enter the <URL> to the agent scripts.

Attention: On your browser, verify that the URL is correct.

6 Click **Save**.

7 Close **CCMM Administrator**.

--End--

Managing Security

Security Fundamentals

Secure the Contact Center Release 7.0 to enable the user to secure the different applications available.

Navigation

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a protocol that provides a systematic way to monitor and manage a computer network. The SNMP model consists of four components:

- managed nodes, which can be any device (such as a host, a router, or printer), that is capable of communicating status to network-management systems through an SNMP management process called an SNMP Agent
- management stations, which can be computers running special network management software that interact with the Agents for status
- management information, which is conveyed through exact specifications and format of status specified by the MIB
- Management Protocol or SNMP, which sends messages called protocol data units (PDUs)

Event viewer settings

Events are log entries that record activities in the Contact Center suite of application servers, such as sending or receiving messages, opening or closing applications, and errors. Some events are for information only, while others can indicate problems. You can filter events by several categories, such as severity and event code range. You can also limit the display to the most recent events.

Event Severity

The system assigns one of the following severity levels to each event.

Information

These events indicate that something noteworthy happened on the system but do not indicate a problem. For example, an information-level event can indicate that a service started or stopped. These events appear in the Event Browser but not in the Alarm Monitor.

Minor

These events indicate that a non-service-affecting fault condition exists and that you must take corrective action to prevent a more serious fault. For example, a minor event is generated when the file system is 90 percent full.

Major

These events indicate that a condition exists which affects services and you must take corrective action. The event condition can cause severe degradation in server performance, and you must restore full capacity. For example, a major event is generated when the file system is 100 percent full.

Critical
These events indicate that a condition which affects services exists and you must immediately take corrective action. Critical events are reported when a component is completely out of service, and you must take immediate action to restore it. For example, a critical event is generated when the file system crashes.

Security template

Security is a critical task for all organizations and it is always mandated to secure all networked servers by locking down the server operating system setting and services. You can secure Windows Server 2003 by applying a predefined security template either locally to the computer or through a network Group Policy Objects (GPO) instead of securing manually.

Nortel Contact Center 7.0 provides a set of predefined Windows Server 2003 security templates that can be deployed quickly to secure the Contact Center 7.0 suite of application servers.

A set of security templates is available for the Contact Center 7.0 suite of application servers. You can apply the security template to the defined Contact Center 7.0 application server to secure the Windows Server 2003 and meet the minimum security requirements for the Contact Center 7.0 application operation.

For more information, see *Nortel Contact Center 6.0 Security Templates User Guide*.

Event Browser and Alarm Monitor

The Event Browser and Alarm Monitor show events that occur on the server. These programs provide many common features to view events. For more information about the features, see Event Browser versus Alarm Monitor features (page 103).

You can configure the Alarm Monitor to automatically appear in the foreground of the desktop when an event occurs and you can specify whether the Alarm Monitor appears in the foreground for only critical events, major and critical events, or all events, or whether it stays in the background for all events.

In the Alarm Monitor, you can filter events by severity only. The Alarm Monitor does not display information events.

Logon warning message (CCMA and UCM)

The logon message is the standard message used by Microsoft Windows. This is the same Microsoft Windows message that appears when you log on to Microsoft Windows.

In CCMA, you can configure the message title and text of the warning message if you do not have a domain security policy in place with a logon warning message configured.

UCM also provides the text for the logon warning message that a security administrator can change. For more information, see *Nortel Unified Communications Management Common Services Fundamentals* (NN43001-116).

Systems Management Server security file (Multimedia)

The Systems Management Server (SMS) also known as the Nortel Multimedia security policy file, CCMM_Security_Policy.msi (Microsoft Installer), contains a policy level for the client to download and run assemblies with a particular strong name. A strong name consists of the assembly identity (name, version number, private key) and a public key. The Outbound Campaign Management Tool and the Contact Center Agent Desktop assemblies are digitally signed with a strong name based on the private key. After it is installed, the CCMM_Security_Policy.msi file instructs the clients to trust the assemblies with the strong name assigned to the Outbound campaign Management Tool and the Contact Center Agent Desktop. You can install the CCMM_Security_Policy.msi file while you are logged on to the server as the local administrator.

To install the security policy, you must install the current Nortel CCMM_Security_Policy.msi file that is included in the most recent service update. Nortel recommends the SMS to install the msi file on multiple clients.

Because installation procedures through an SMS system can vary from one company to the next, follow your company guidelines to install the CCMM_Security_Policy.msi file for the SMS clients on your network. For more information, see the SMS documentation on the Microsoft Web site at www.microsoft.com.

Experienced system administrators can deploy the CCMM_Security_Policy.msi file.

Group policy

In addition to using an SMS server, a system administrator can install the CCMM_Security_Policy.msi file on clients within the same domain using a Windows group policy. For details, see document 324750 on the Microsoft knowledge base.

Server Utility to view events on CCMS

The Server Utility allows you to monitor and maintain Contact Center Manager Server Release 7.0. The Server Utility also provides functionality that is not available through Contact Center Manager Administration.

The Server Utility maintains the look and feel of the Symposium Call Center Server Classic Client. You can install it on a stand-alone Windows Server 2003, Windows 2000 Professional or Windows XP Professional PC, or it can co-reside with the Contact Center Manager Server. In a network, the Contact Center Server Utility can co-reside with the Network Control Center Server.

Data collection and management

The Contact Center Multimedia database contains all multimedia contacts including the routing information, customer details, and contact details for e-mail, outbound, instant messages, and Web communications. Regular maintenance is required to ensure that the database operates with maximum efficiency. You can archive the information in the database periodically to reduce the data in the multimedia database.

You can archive data in the database by

- outbound campaign
- e-mail rule
- closed reason
- skillset

Prerequisites for data collection and management

- Determine which type of archive or restore to use.
- Shut down the Multimedia services to prevent issues.

Attention: If you modify the data generated from an archive, the data can become corrupt causing future restores to fail. For this reason, Nortel cannot support issues with the application arising from manual modification of the data generated by an archive.

- If your Contact Center Multimedia server is in a domain, you can archive or restore your Contact Center Multimedia database on a network share drive. If your Contact Center Multimedia server is in a workgroup, you cannot use the network drives for the archived data.

Navigation

- Starting the archive utility (page 458)
- Archiving by outbound campaign (page 458)
- Archiving by e-mail rule (page 459)

Starting the archive utility

Start the archive utility to configure your archiving settings and perform the archive or restore of the Contact Center Multimedia database.

Prerequisites

- Log on to the Contact Center Multimedia Administrator.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Database Administration**.
3	Double-click **Archive/Restore Utility**.

--End--

Archiving by outbound campaign

Multiple campaigns can be archived at one time.If you attempt to archive an active campaign, you receive an error message. However, inactive, completed, or cancelled campaigns can be archived.

The Archive utility archives campaign-level information, such as the agent script and associated questions to a file named CampaignArchive.txt, and the all contact data associated with the campaign, such responses to script questions and disposition code data to a file named ContactArchive.txt.

A log file of the archive, ArchiveLogFile.txt, is stored in the archive folder you choose.

Prerequisites

- Start the archive utility. See Starting the archive utility (page 458).
- Close the Outbound Campaign Management Tool.

Procedure steps

Step	Action
1	In the archive utility, click the **Archive By Outbound Campaign** tab.
2	From the **Inactive Campaign List**, select the outbound campaign to archive.
3	Click the right arrow to move the selected campaign to the list of campaigns to archive.
4	To include customer data for the contacts in the outbound campaign, clear the **Delete Customer Data** check box.
5	In the **Archive Description or Comments** box, type comments or information about this archive.
6	Under **Archive to Folder**, browse to the folder in which to store the current archive. The folder location you choose for the archive must contain no other files.
7	Click **Archive**.
8	On the calendar, select the date to create your archive.
9	Click **Close**.

--End--

Archiving by e-mail rule

Archive data by e-mail rule. When you choose to archive by e-mail rule, the archive date, by default is six months prior to the current date. When you archive data, you cannot select the current date. Only closed contacts within your selected date range are archived.

Attachment files for e-mail messages are archived in an attachment folder under the folder selected for the archive. All data is archived to a single flat file named ContactArchive.txt. A log file of the archive, ArchiveLogFile.txt, is stored in the archive folder you choose.

Prerequisites

- Start the archive utility. See Starting the archive utility (page 458).

Procedure steps

Step	Action
1	On the **Contact Center Archive & Restore Utility** window, click **Archive\Restore Email Rule**.
2	Click the **Archive By Email Rule** tab.
3	Under the **Email Rules List**, navigate through the list of mailboxes and select the rules to archive.
4	Click the right arrow to move the selected rule to the list of items to archive.
5	Repeat steps 3 and 4 for each rule to archive.
6	Under **Contacts Closed on or Before**, click the last date for which you want to archive contacts.
7	To include customer data for the contacts with the selected items, clear the **Delete Customer Data** check box.
8	In the **Archive Description or Comments** box, type comments or information about this archive.
9	Under **Archive to Folde**r, type or browse to the folder in which to store the current archive. The folder location you choose for the archive must contain no other files.
10	Click **Archive**.
11	On the calendar, select the date to create your archive.
12	Click **Close**.

--End--

Archiving by skillset

Select a skillset from which to archive data. When you choose to archive by skillset, the archive date, by default six months prior to the selected date. When you archive data, you cannot select the current date. Only closed contacts within your selected date range are archived.

Skillsets that are marked as deleted appear with an asterisk (*).

All contact data is archived to a single flat file named ContactArchive.txt. A log file of the archive, ArchiveLogFile.txt, is stored in the archive folder you choose.

Prerequisites

- Start the archive utility. See Starting the archive utility (page 458).

Procedure steps

Step	Action
1	On the **Contact Center Archive & Restore Utility** window, click **Archive\Restore Skillset**.
2	Click the **Archive By Skillset** tab.
3	Under the **Skillset** list, click a skillset to archive. Skillsets in the Skillset list marked with an asterisk are no longer in service.
4	Click the right arrow to move the selected skillset to the list of items to archive.
5	Repeat steps 3 and 4 for each skillset to archive.
6	Under **Contacts Closed on or Before**, click the last date for which you want to archive contacts.
7	To include customer data for the contacts with the selected items, clear the **Delete Archive Customer Data** check box.
8	In the **Archive Description or Comments** box, type comments or information about this archive.
9	Under **Archive to Folder**, type or browse to the folder where you want to store the current archive. The folder location you choose for the archive must contain no other files.
10	Click **Archive**.
11	On the calendar, select the date time to create your archive.
12	Click **Close**.

--End--

Archiving by closed reason

Select a closed reason for which you want to archive data. When you choose to archive by closed reason, the archive date, by default six months prior to the selected date. When you archive data, you cannot select the current date. Only closed contacts within your selected date range are archived.

Closed reasons that are marked as deleted appear with an asterisk (*).

All contact data is archived to a single flat file named ContactArchive.txt. A log file of the archive, ArchiveLogFile.txt, is stored in the archive folder you choose.

Prerequisites

- Start the archive utility. See Starting the archive utility (page 458).

Procedure steps

Step	Action
1	On the **Contact Center Archive & Restore Utility** window, click **Archive\Restore Closed Reason**.
2	Click the **Archive By Closed Reason** tab.
3	Under the **Closed Reason List**, click a closed reason to archive. Closed reasons in the Closed reasons list marked with an asterisk are no longer in service.
4	Click the right arrow to move the selected closed reason to the list of items to archive.
5	Repeat steps 3 and 4 for each closed reason to archive.
6	Under **Contacts Closed on or Before**, click the last date for which you want to archive contacts.
7	To include customer data for the contacts with the selected items, clear the **Delete Customer Data** check box.
8	In the **Archive Description or Comments** box, type comments or information about this archive.
9	Under **Archive to Folder**, type or browse to the folder in which to store the current archive. The folder location you choose for the archive must contain no other files.
10	Click **Archive**.
11	On the calendar, select the date to create your archive.
12	Click **Close**.

--End--

Suspending an archive activity

You can suspend an archive activity if you want to delay the archive process.

This features allows you to archive at a later time, during a non-peak or off period of the call center. The archive later feature also allows you to set a future time to run an archive.

Prerequisites

- Start the archive utility. See Starting the archive utility (page 458).

Attention: The archive later feature is only a timer that delays the archive activity. You must reconfigure the setting each time that you want to suspend an archive activity.

Procedure steps

Step	Action
1	On the **Contact Center Archive/Restore Utility** window, click **Archive/ Restore by Skillset**.
2	Click the **Archive Skillset** tab.
3	Click the **Archive Later** button.
4	On the **Enter Archive Time** window, type the time at which you want the system to begin the archive activity.

Attention: The time that you enter must be within a 24 hour period.

Step	Action
5	Click **Schedule**.
6	Click **OK**.

--End--

Restoring an archive

Restore your database from any selected archive. The flat files are added to the database file.

To prepare to restore data, all archived audit records are loaded into the database from the archive location. A progress bar shows the progress of the restore. Do not close the Archive utility during this time. The delay is proportional to the number of archived audit records.

Prerequisites

- Start the archive utility. See Starting the archive utility (page 458).

Attention: If you modify the data generated from an archive, the data can become corrupt causing future restores to fail. For this reason, Nortel cannot support issues with the application arising from manual modification of the data generated by an archive.

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Nortel Contact Center**, **Multimedia Server**, **CCMM Administrator**.
2	Type your user ID and password.
3	Expand **Contact Center Multimedia**.
4	Expand **Database Administration**.
5	Double-click **Archive/Restore Utility**.
6	Click **Restore**.
7	In the **Restore** dialog box, click **Open**.
8	Browse to the folder from which you want to restore the archive. The **Restore Utility** restores all data from the folder that you choose.
9	Click **Restore**.

--End--

Recovering from a failed archive or restore

Restore from a failed archive or restore to recover your archived data. If you experience a problem with the database or Contact Center Multimedia server during an archive or restore, a message box indicates one of two things:

- a network issue prevents the client from reporting progress to the user but the archive and restore remains in progress
- a database or server crashed which prevents the process from completing successfully.

You can perform only one restore or archive at one time.

Procedure steps

Step	Action
1	If the database or server crashed, click **OK** on the message box to shut down the Archive utility. When the Archive utility closes, a message box indicated the number of outstanding contacts. The archive or restore automatically restarts.
2	Restart the Archive utility to complete the restoration or archive.

--End--

Platform Security

Windows allows you to install and configure security features that help you secure your server. The Security Configuration Wizard is part of Windows Server 2003 Service Pack 1.

Navigation

- Installing the Windows Server 2003 Security Configuration Wizard (page 467)
- Securing the Server (page 467)

Installing the Windows Server 2003 Security Configuration Wizard

Use the Security Configuration Wizard to determine the minimum functionality required for the role of the server, and disable functionality that you do not require. You can use the Security Configuration Wizard to perform the following activities:

- disable unneeded services
- block unused ports
- allow address or security restrictions for open ports
- prohibit IIS Web extensions
- reduce protocol exposure to server message block (SMB), LanMan, and Lightweight Directory Access Protocol (LDAP)
- define an audit policy based on your auditing objectives

Procedure steps

Step	Action
1	Log on to the server as Administrator.
2	On the Windows **Start** menu, choose **Control Panel, Add or Remove Programs**.
3	Click **Add/Remove Windows Components**.
4	Select the **Security Configuration Wizard** check box.
5	Click **Next**.
6	After the installation is complete, click **Finish**.

--End--

Securing the Server

Select minimum options when running the Security Configuration Wizard on your Contact Center application server. You can create a less restrictive policy by enabling other services and server roles depending on your requirements.

Prerequisites

- Ensure the Contact Center application server is running.

Procedure steps

Step	Action
1	On the **Start** menu, click **Run**.
2	Type **SCW**, and then click **OK**.
3	In the **Welcome** window, click **Next**.
4	In the **Configuration** window, select **Create a New Security Policy**, and then click **Next**.
5	Ensure the host name of the local server is correct, and then click **Next**.
6	After the processing of the security configuration database is finished, click **Next**.
7	In **Role-Based Service Configuration** window, click **Next**.
8	In the **Select Server Roles** window, select the **Web Server** check box, and then click **Next**.

Attention: Some of the following steps require specific selections according to your application. If this occurs, contact your administrator.

Step	Action
9	In the **Select Client Features** window, select the client features you want to enable according to your application server. As a minimum, Nortel recommends that you select the features already enabled according to the specified application server.
10	Click **Next**.
11	On the **Administration and Other Options** dialog box, select the server features that you want to enable. As a minimum, Nortel recommends that you select the features already enabled according to the specified application server.
12	Click **Next**.
13	Select the services you want to enable. You must enable the required services for each Contact Center application server to function correctly. Select services that you require such as antivirus software clients.
14	Click **Next**.
15	In the **Handling Unspecified Services** dialog box, select one the following options:

If	Then
You want to disable all services on the server that are not defined in the security policy.	Select **Disable the services**.
You want to avoid changing the startup mode of the services on the server that are not defined in the security policy.	Select **Do not change the startup mode of the services**.

16 Click **Next**.

17 In the **Confirm Service Changes** window, review the modified services when you apply this policy to your system.

18 Click **Next**.

19 In the **Network Security** window, click **Next**.

20 In the **Open Ports and Confirm Applications** window, select the ports to open.

21 To restrict which remote machines connect to the ports listed, in the **Open Ports and Confirm Applications** window, select the specific port.

22 Click **Advanced**, and then select the options that apply to your server.

23 Click **OK**.

24 Click **Next**.

25 In the **Confirm Port Configuration** window, review the Inbound Port Configuration, and click **Next**.

26 In the **Registry Settings** window, click **Next**.

27 In the **Require SMB Security Signatures** window, select the **All computers that connect to it satisfy the following minimum operation system requirements** check box.

28 Clear the **It has surplus processor capacity that can be used to sign file and print traffic** check box, and then click **Next**.

29 In the **Outbound Authentication Methods** window, select only the **Domain Accounts** box. Ensure that you clear the other check boxes, and then click **Next**.

30 In the **Outbound Authentication using Domain Accounts** window, select the **Windows NT 4.0 Service Pack 6a or later systems** check box.

31 Clear the **Clocks that are synchronized with the selected server's clock** check box, and click **Next**.

32 Review the Registry Settings Summary, and then click **Next**.

33 In the **Audit policy** window, click **Next**.

34 Review the Audit Policy Summary, and then click **Next**.

35 In the **Internet Information Services** window, click **Next**.

36 In the Audit Policy Section, select **Do not audit**.

37 In the **Select Web Service Extension for Dynamic Content** window, select the extensions that apply to your server.

38 Clear the **Prohibit all other Web service extensions not listed above** check box, and then click **Next**.

39 In the **Select the Virtual Directories to Retain** window, select the virtual directories you want to retain on the selected server, and then click **Next**.

40 In the **Prevent Anonymous Users from Accessing content Files** window, clear the **Deny anonymous users write access to content files** check box, and then click **Next**.

41 Review the IIS Security Settings Summary, and then click **Next**.

42 Save your security policy as an XML file to a location on your server.

43 Click **Next**.

44 In the **Apply Security Policy** window, click **Apply Now**, and then click **Next**.

The security policy is applied–the relevant services are disabled and the Windows firewall blocks relevant ports.

45 Click **Next**.

46 Click **Finish**.

--End--

Security Template

Nortel Contact Center 7.0 provides a set of predefined Windows Server 2003 Security Templates that you can deploy quickly to secure the Nortel Contact Center 7.0 suite of servers.

The following procedures allow you to activate and apply these templates.

Navigation

Activating the Nortel Contact Center security template

You can activate the Nortel Contact Center security template locally or as a group policy in an Active Directory that contains the Contact Center suite of application servers. You can deploy the Security Template either before or after you install the server software.

If you activate the Nortel Contact Center Security Template locally (on the server on which you installed Contact Center Multimedia/Outbound), you must select the applicable Security Template for the Nortel Contact Center application server and download the selected template from the Enterprise Solution PEP Library web site (www.nortel.com/espl) to the local disk drive. After you download the file, you can import and configure the Security Template using the Microsoft Security Configuration and Analysis utility.

If you want to activate the Nortel Contact Security Template on a coresident server, make sure that you download the coresident template.

If you are add Communication Control Toolkit to a previously stand-alone Contact Center Manager Server, you must rollback the original Contact Center 7.0 security template and reapply a new one for the coresident server.

Procedure steps

Step	Action
1	Log on to the server as Administrator.
2	In the Windows **Start** menu, click **Run**.
3	Type **mmc**, and then click **OK**.
4	In the **Console1** window, from the **File** menu, choose **Add/Remove Snapin**.
5	On the **Add/Remove Snap-in** dialog box, click **Add**.
6	Select **Security Configuration and Analysis,** and then click **Add**.
7	Click **OK**.
8	On the console, right-click **Security Configuration and Analysis.**
9	Click **Open Database**.
10	In the **File Name** box, enter a new database name. For example, type **CCM_Outbound_Security**.
11	Click **Open**.
12	Select **Contact Center Multimedia/Outbound Security Template.inf**, and then click **Open**.
13	On the console, right-click **Security Configuration and Analysis**, and then click **Analyze Computer Now**.

The **Perform Analysis** dialog box appears. The default location for the Security Template log is C:\Documents and Setttings\Administrator\My Documents\Security\Logs\. If you want to change the location in which the Security Template log is stored, do so now.

14 Click **OK**.

15 Right-click **Security Configuration and Analysis**, and then choose **Configure Computer Now**.

The **Configure System** dialog box appears. The default location for the configuration log file is C:\Documents and Setttings\Administrator\My Documents\Security\Logs\. If you want to change the location in which the Security Template log is stored, do so now.

16 Click **OK**.

17 Restart the server to activate the new security policy and configuration.

--End--

Applying the security template locally on the server

You can activate the Nortel Contact Center security template locally or as a group policy in an Active Directory that contains the Contact Center suite of application servers. You can deploy the security template either before or after you install the server software.

If you activate the Nortel Contact Center security template locally (on the server on which you installed Contact Center Multimedia/Outbound), you must select the applicable Security Template for the Nortel Contact Center application server and download the selected template from the Enterprise Solution PEP Library web site (www.nortel.com/espl) to the local disk drive. After you download the file, you can import and configure the Security Template using the Microsoft Security Configuration and Analysis utility.

Procedure steps

Step	Action
1	Log on to the server as Administrator.
2	In the Windows **Start** menu, click **Run**.
3	Type **mmc**, and then click **OK**.

4 In the **Console1** window, from the **File** menu, choose **Add/Remove Snapin**.

5 On the **Add/Remove Snap-in** dialog box, click **Add**.

6 Select **Security Configuration and Analysis,** and then click **Add**.

7 Click **OK**.

8 On the console, right-click **Security Configuration and Analysis.**

9 Click **Open Database**.

10 In the **File Name** box, enter a new database name. For example, type **Contact Center Multimedia/Outbound Security Template**.

11 Click **Open**.

12 Select **Contact Center Multimedia/Outbound Security Template.inf**, and then click **Open**.

13 On the console, right-click **Security Configuration and Analysis**, and then click **Analyze Computer Now**.

The **Perform Analysis** dialog box appears. The default location for the Security Template log is C:\Documents and Setttings\Administrator\My Documents\Security\Logs\. If you want to change the location in which the Security Template log is stored, do so now.

14 Click **OK**.

15 Right-click **Security Configuration and Analysis**, and then choose **Configure Computer Now**.

The **Configure System** dialog box appears. The default location for the configuration log file is C:\Documents and Setttings\Administrator\My Documents\Security\Logs\. If you want to change the location in which the Security Template log is stored, do so now.

16 Click **OK**.

17 Restart the server to activate the new security policy and configuration.

--End--

Applying the security template in a network domain

Apply the Nortel Contact Center security templates in a network domain environment by importing the template into a group policy object of an organizational unit (OU) of which the Contact Center 7.0 server is a member.

Prerequisites

- Download Group Policy Management Console (GPMC) from microsoft.com, and install it on the server.

Procedure steps

Step	Action
1	Open GPMC.
2	In the console tree, expand the domain or OU that you want to import to the Security Template.
3	Right-click the Group Policy object you want to edit, and then click **Edit**.
4	On the **Group Policy Object Editor** console tree, click **Computer Configuration**.
5	Click **Windows Settings**, and then right-click **Security Settings**.
6	Click **Import Policy**.
7	Select the Contact Center 7.0 Security Template that you want to import, and then click **Open**.

--End--

Microsoft Windows configuration and management

Perform the following procedures to configure settings in Microsoft Windows on your servers.

Navigation

Managing date and time features

Manage the date and time features in Microsoft Windows to avoid potential call processing outages.

Contact Center Manager Server does not support time changes backward beyond the current date. For example, do not change the time into the past beyond midnight.

Procedure steps

Step	Action
1	Log on to the server as administrator.
2	Click **Start**, **Control Panel**, and then **Date and Time**.
3	In the **Date and Time Properties** dialog box, click the **Time Zone** tab.
4	Clear the **Automatically adjust clock for daylight saving changes** check box.
5	Click the **Internet Time** tab.

Attention: If you click this tab and click OK without making changes, the Startup type for the Windows Time service is Automatic.

6	Clear the **Automatically synchronize with an Internet time server** check box.
7	Click **Apply** to save your changes.
8	Click **OK**.

--End--

Disabling the Windows time service

Disable the Windows Time service to stop it from running and attempting to synchronize the CCMS server time with a time source and to avoid potential call processing outages.

Contact Center Manager Server does not support time changes backward beyond the current date. For example, do not change the time into the past beyond midnight.

If the Contact Center Manager Server is in a SIP environment or is the Network Control Center server, you can skip this step.

Procedure steps

Step	Action
1	Click **Start**, **Administrative Tools**, **Services**.

2 In the **Services** window, in the right pane, double-click **Windows Time**.

3 In the **Windows Time Properties** dialog box, on the **General** tab, in the **Service Status** area, click **Stop**.

4 From the **Startup** type list, select **Disabled**.

5 Click **Apply** to save your changes.

6 Click **OK** to close the **Windows Time Properties dialog** box.

7 Close the Services window.

--End--

Verifying Service Updates

Verify that you have the most recent Services Updates for the Contact Center Manager Server software.

Prerequisites

- Look up the most recent patches and upgrades for your Contact Center Server at www.nortel.com.
- Review *Nortel Contact Center Upgrade and Patches* (NN44400-410) to understand how to install patches and service updates.

Procedure steps

Step	**Action**

1 Log on to the server on which you installed Contact Center Manager Server.

2 Click **Start, All Programs, Nortel, Contact Center, Common Utilities, Contact Center Patch Viewer**.

3 Click the **Manager Server** tab.

4 View the most recent **Update Name**.

5 Compare the most recent update name in the Patch Viewer with the most recent patch or upgrade listed on the Nortel Web site.

6 Click **Close**.

7 Install missing service updates and patches from the web site by performing the instructions in *Nortel Contact Center Upgrade and Patches* (NN44400-410).

--End--

Adding a server to a domain

Add your Contact Center Manager Server to an existing domain and perform other necessary tasks to ensure that your server works in a domain.

After you install Contact Center Manager Server, you can add your server as a member of an existing domain (stand-alone server only).

Prerequisites

- Install Contact Center Manager Server.
- Ensure that you have domain administrator's privileges, or ask the domain administrator to assign you a domain user account for remote access.
- Disable Windows Time Service (for Contact Center Manager Server is in a domain).

Procedure steps

Step	Action
1	Log on to the server on which you installed Contact Center Manager Server.
2	Right-click **My Computer**.
3	Select **Properties**.
4	In the **System Properties** dialog box, click the **Computer Name** tab.
5	Click **Change**.
6	In the **Computer Name Changes** dialog box, click **Domain**.
7	Type the domain name (you must provide the fully qualified domain name, which includes the prefix and suffix).
8	Click **OK**. A message appears indicating that the server now belongs to the domain that you specified.
9	Type a user name and password to add a machine to the domain.
10	Restart the server when you are prompted to do so.

--End--

Configuring the operating system for remote access in a domain

Configure remote access for your server in a domain to allow technical support to access the server.

Prerequisites

- Add your server to the domain.

Procedure steps

Step	Action
1	Log on to the server.
2	Click **Start**, **All Programs**, **Administrative Tools**, **Routing and Remote Access**.
3	Right-click the local server name, and then select **Configure and Enable Routing and Remote Access**.
4	Click **Next**.
5	Select **Remote Access (dial-up or VPN)**.
6	Click **Next**.
7	Click **Dial-up**.
8	Click **Next**.
9	Select the network connection that represents your Nortel server subnet.
10	Click **Next**.
11	Select **From a specified range of addresses**.
12	Click **Next**.
13	Click **New**.
14	Enter the range of IP addresses provided by your domain administrator.
15	Click **OK**.
16	Click **Next**.
17	Select **No**, **use Routing and Remote Access to authenticate requests**.
18	Click **Next**.
19	Click **Finish**.

--End--

Configuring the operating system for remote access in a workgroup

Configure remote access for your server in a workgroup to allow technical support to access the server.

Prerequisites

- Add your server to a workgroup.

Procedure steps

Step	Action
1	Log on to the server.
2	Click **Start, Control Panel, Network Connections, New Connection Wizard**.
3	In the **New Network Connection** window, click **Next**.
4	In the **Network Connection Type** window, select **Set up an advanced connection**.
5	Click **Next**.
6	In the **Advanced Connection Options** window, select **Accept incoming connections**.
7	Click **Next**.
8	In the **Incoming Virtual Private Connection** window, select **Do not allow virtual private connections**.
9	Click **Next**.
10	In the **User Permissions** window, select the **Administrator** check box.
11	If you work with the Contact Center Manager Server, select the check boxes beside **NGenDesign**, **NgenDist**, and **NGenSys**.
12	Click **Next**.
13	In the **Networking Software** window, select the **Internet Protocol (TCP/IP)**, **File and Printer Sharing for Microsoft Networks**, and **Network Load Balancing** check boxes.
14	Click **Next**.
15	In the **Incoming TCP/IP Properties** window, clear the check box beside **Allow callers to access my local area network**.

16	Select the **Specify TCP/IP** address option.
17	In the **From** and **To** boxes, specify a range of IP address in the same subnet as the Nortel server subnet IP address provided by your administrator.
18	Clear the check box beside **Allow calling computer to specify its own IP address**.
19	Click **OK**.
20	In the **Completing the New Connection** window, click **Finish**.

--End--

Installing Windows SNMP Service

Install Windows Simple Network Management Protocol (SNMP) agent to forward events to a Network Management System (NMS) on your network.

Procedure steps

Step	Action
1	Log on to the server as NGenSys.
2	Click **Start**, **Programs**, **Administrative Tools**, **Services**.
3	In the **Services** window, select the **SNMP Service**.
4	Click **Action**, **Properties**.
5	In the **SNMP Service Properties** window, click the **Traps** tab.
6	If no community name is defined, in the **Community name** box, type public.
7	Click **Add to list**.
8	Click **Add** to add the IP address of the NMS to which the server sends traps.
9	In the **SNMP Service Configuration** window, type the IP address of the NMS.
10	Click **Add**.
11	In the **SNMP Service Properties** window, click **OK**.
12	In the **Services** window, right-click the **SNMP Trap** Service, and select **Start**.
13	Close the **Services** window.
14	Click **Start**, **All Programs**, **Accessories**, **Windows Explorer**.

15 Browse to the folder **D:\Nortel\bin**, and double-click **SNMPFilterCnfg.exe**.

16 In the **Level of Filtering** box, select the event types to forward to the NMS.

17 Click **OK**.

--End--

Common server administration

Licensing administration

The License Manager (LM) controls the licensing of Contact Center. The License Manager provides central control and administration of application licensing for all of the elements of Contact Center.

You can choose Nodal Licensing mode for a single Contact Center installation or Corporate Licensing mode for a network of Contact Center installations.

You can also maintain a secondary License Manager, which takes over the licensing if the primary License Manager fails.

In the instance where the Contact Center Manager Server (CCMS) database is getting restored and the LM is co-resident on the same server, then that LM is not be available for the duration of the restore. That means that any Contact Center application CCT, CCMM, CCMA runs in the grace period while the database is getting restored. For corporate licensing, any other CCMS server in the network using that LM also runs in grace period.

This chapter describes the Nodal and Corporate Licensing modes, how to interpret your license file, how to install and configure the License Manager for your contact center, and the licensing grace period.

Navigation

- Resetting the grace period (page 486)
- Updating the license file (page 486)
- Changing from Nodal to Corporate licensing (page 487)
- Changing the license manager file on a Contact Center Manager Server (page 489)
- Refreshing your server (page 490)

Resetting the grace period

You can reset the grace period to 20 days at any time. When a communication error occurs, an event is fired to the Server Utility detailing that an error occurred, the time elapsed in the Grace Period, and a lock code that you must return to Nortel to reset the grace period.

If a communication error occurs between the Contact Center Manager Server and the License Manager, normal operation of the Contact Center Manager Server runs for the duration of the grace period.

If, at any stage, the grace period expires, Contact Center Manager Server shuts down and is locked. You cannot restart Contact Center Manager Server without resetting the grace period.

Prerequisites

- For Contact Center Manager Server, you must apply separate unlock codes for the CCMS Control Service and the ASM Service. Repeat step 1 to step 6.

Procedure steps

Step	Action
1	Log on to the server where the License Manager software is installed.
2	From the Event Viewer, make a copy of the lock code and send this code to Nortel Support.
3	Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Common Utilities**, **License Grace Period Reset Utility** to apply the new unlock code.
4	Enter the unlock code you received from Nortel Support.
5	Click **Apply**.
6	Click **Exit**.
7	Restart the Contact Center Manager Server application.

--End--

Updating the license file

Update the license file to upgrade Contact Center Manager Server.

Procedure steps

Step	Action
1	Click **Start, All Programs, Nortel, Contact Center, License Manager, Configuration**.
2	On the Configuration page, click **Browse**.
3	Navigate the file system and locate the new license file.
4	Click **Open**.
5	Click **Apply**.
6	Click **Yes** to restart the License Manager server.
7	Click **OK** to close the window.
8	Click **Exit**.

--End--

Changing from Nodal to Corporate licensing

Use Corporate Licensing to distribute licenses to multiple servers from a single license pool. You can configure one active License Manager in the server network and one standby License Manager in the server network.

Prerequisites

- Install License Manager on a Contact Center Manager Server or Network Control Center server.
- Use default ports 3998 to 4007 to pass through any firewall between nodes and the Corporate License Manager site.
- If your License Manager is installed on the same server as Contact Center Manager Server, shut down Contact Center Manager Server.
- Ensure that the primary License Manager and secondary License Manager can resolve the hostname of each other.
- Plan to restart the server at the end of this procedure.

Procedure steps

Step **Action**

1 On the **Start** menu, click **All Programs**, **Nortel, Contact Center**, **License Manager**, **Configuration**.

2 On the Configuration page, click **Browse**.

3 Navigate the file system and locate the new license file.

4 Click **Open**.

5 Click **Apply**.

6 Click **Yes** to restart the License Manager Server service.

7 Click **OK** to close the window.

8 Click **Exit**.

9 If you have a Secondary License Manager, perform the following steps. Otherwise, proceed to step 19.

10 Copy the new Corporate License file to the appropriate directory on the Contact Center Manager Server serving as the host for the secondary License Manager.

11 Shut down the Contact Center Manager Server services on the secondary License Manager server. If you do not, the Contact Center Manager Server services shut down due to a refresh error.

12 Click **Start**, **All Programs**, **Nortel, Contact Center**, **License Manager**, **Configuration**.

13 On the Configuration page, click **Browse**.

14 Navigate the file system and locate the new license file.

15 Click **Open**.

16 Click **Apply**.

17 Click **Yes** to restart the License Manager Server service.

18 Click **Exit** to close the window.

19 Click **Start**, **All Programs**, **Nortel, Contact Center**, **Manager Server**, **Server Configuration**.

The Initializing Server Setup Configuration Utility window appears. This window can remain open for up to 30 seconds.

20 If you have a co-resident License Manager, an information box may appear. If it does, click **Continue**.

21 Click **Licensing**.

22 Under **License Manager Package**, change the package to the corporate version. For example, if the current package is CCS300N, change it to CCS300C.

23 Under **License Server IP Address**, type the correct IP information for the Primary and Secondary License Manager IP address.

24 Click **Apply All**.

25 Click **Yes** to restart the server.

--End--

Changing the license manager file on a Contact Center Manager Server

Change the license manager file on a Contact Center Manager Server if you purchased additional options listed in the Contact Center Manager Server configuration.

Prerequisites

- Shut down the Contact Center Manager Server services on the appropriate server.
- Plan to restart the server at the end of this procedure.

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Nortel, Contact Center**, **License Manager**, **Shutdown**.
2	Click **Start, All Programs**, **Nortel, Contact Center**, **Manager Server**, **Server Configuration**.
3	Click **Licensing**.
4	Under **License Manager Package**, change the package to the corporate version. For example, if the current package is CCS200N, change it to CCS200C.
5	Under **License Server IP Address**, type the correct IP information for the Primary and Secondary License Manager IP address.
6	Click **Apply All**.
7	Click **Yes** to restart the server.

--End--

Refreshing your server

Refresh your server if a new license file is configured and accepted by Contact Center Manager Server, or you connect to a different License Manager server (that is, a new or standby License Manager server), or you have enabled Open Queue.

Prerequisites

- Log on as the Webadmin user to refresh the servers.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration.
2	On the launchpad, click **Configuration**.
3	On the **Server** menu, click **Refresh All Servers**.
4	Click **Yes**.

--End--

Contact Center server database maintenance

The Contact Center Manager Server, Communication Control Toolkit, and Contact Center Multimedia have a common backup and restore utility. Perform the procedures in this chapter to back up or restore one or more Contact Center Manager Server databases.

Contact Center maintains a maximum of seven backup folders in the backup location. The most recent backup file is in folder ..\backup_1\. The other backup folders, backup_2, backup_3, and so on, contain progressively older backup files. When a new backup (either manual or scheduled) is performed, all existing backup folders update to reflect the order of the backup taken. When the maximum number of backup folders is reached, the oldest backup is discarded and replaced with the second-oldest backup. All other backup files are adjusted to reflect the order they were performed.

Prerequisites to Contact Center server database maintenance

- Ensure that the Contact Center software is installed.

Navigation

Creating a backup location

Create a backup location on your network with the correct access permissions to ensure a designated location for the backup file.

If you use tapes for your backups, you need not create a backup destination.

Prerequisites

- Ensure that you have a user account with full permissions to access the location for the database backups.

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Database Utilities**, **Database Maintenance**.
2	In the **Database Maintenance** dialog box, in the left pane, expand Backups.
3	Click **Backup Locations**.
4	In the right pane, click **Create**.
5	From the **Drive Letter** list, select a drive letter.
6	In the **UNC Path** text box, type the location to which to backup the database.
7	In the **Username** box, type the user name used to log on to the server specified in the UNC Path box.
8	In the **Password** box, type the domain password.
9	Click **OK**.

--End--

Variable definitions

Variable	Value
Drive Letter	The drive letter representing the destination for the backup file. You can choose from the drive letters listed.
UNC Path	The Uniform Naming Convention (UNC) path, which is the IP Address and folder name of the server destination for the backup file. For example, the UNC path can be \\192.167.140.0\backup.

Variable	Value
Username	The user name, including server name and user name for the backup destination server. For example, the user name can be \\192.167.140.45\administrator.
Password	The password for the user that you configure for the backup location.

Performing an immediate backup of the database

Perform an immediate backup of the database to save the current data. You must perform this procedure after installation or when any significant change occurs in the database, so that you can easily restore the database.

You can back up one or more Contact Center databases at one time. The backup folder contains separate backup files for each database or folder you select.

Nortel recommends that you perform backups during low traffic periods. CCMS Services are not shut down during backups.

If your contact center is running with a standby server, ensure that you back up the primary server, not the standby server, to back up the most current data.

Prerequisites

- Create a backup location if you want to use a network location for your backup.
- Know which applications you are to back up.

Attention: If you back up a CCMM database without backing up the CCMS database, this might result in a mismatch in OAM data when you restore. Nortel recommends that you back up the CCMS database and the CCMM database at the same time.

Procedure steps

Step	Action
1	Click **Start, All Programs, Nortel, Contact Center, Database Utilities, Database Maintenance**.
2	In the **Database Maintenance** dialog box, in the left pane, click **Immediate Backup**.
3	In the **Media Type** section, select the **Tape Drive** or **Network Disk** option.
4	In the **Applications** section, select the check box beside each application to back up.
5	From the **Backup Location** list, select the network drive where you want to store the backup.
6	Click **OK**.
7	Click **Yes** to confirm your choices.
8	Use the **Progress information** field to monitor the progress of the backup.

9 Click **Exit** to close the Database Maintenance utility.

--End--

Variable definitions

Variable	Value
Applications	The Contact Center application databases that you can back up: • CCMS: Contact Center Manager Server database • CCT: Communication Control Toolkit database • CCMM: Contact Center Multimedia database • ADMIN: Configuration items for backup locations, redundancy paths and schedule information (not a database) If an application is not available, you cannot select it.
Backup Location	The destination for the network disk. The values are configured in the Backup Locations.
Media type	The type of media used for your backup file. You can use a network disk location or a tape drive. If you use a network disk location, you must configure a destination before you can back up the file.

Scheduling a backup of the database

Schedule a backup of the Contact Center Manager Server 7.0 database to save the data regularly. You must regularly back up the database to ensure you always have current information in case you need to restore the data.

Regularly scheduled backups overwrite the same file each time they occur. To keep more than one backup file, you must configure a separate network drive.

You can back up one or more databases at one time. The backup folder contains separate backup files for each database or folder you select. If you have two scheduled backups occurring at the same time, the backup with the larger timeframe occurs first. For example, if you have a weekly backup and a monthly backup scheduled at the same time, the monthly backup runs first.

If your contact center is running with a standby server, ensure that you back up the primary server, not the standby server, to back up the most current data.

Prerequisites

- Create a backup location.
- Know which applications you are to back up.

Attention: If you back up a CCMM database without backing up the CCMS database, this might result in a mismatch in OAM data when you restore. Nortel recommends that you schedule a back up of the CCMS database at the same time as the scheduled CCMM database backup.

Procedure steps

Step	Action
1	Click **Start, All Programs, Nortel, Contact Center, Database Utilities, Database Maintenance**.
2	In the **Database Maintenance** dialog box, in the left pane, click **Scheduled Backup**.
3	In the right pane, click **Create**.
4	Under **General Properties**, in the **Name** box, type a name for the scheduled backup.
5	From the **Media Type** list, select **Network Drive**.
6	In the **Start Date** box, type the date on which to begin scheduled backups. **OR**

Click the calendar icon and select a date on which to begin scheduled backups.

7 In the **Start Time** box, select the time to start the backup.

8 From the **Backup Location** list, select a drive to store the backup.

9 From the **Frequency** list, select the frequency of the backup.

10 Under **Applications**, select the check box beside the applications to back up.

11 Click **OK**.

12 Click **Exit** to close the Database Maintenance utility.

--End--

Variable definitions

Variable	Value
Applications	The Contact Center application databases that you can back up: • CCMS: Contact Center Manager Server database • CCT: Communication Control Toolkit database • CCMM: Contact Center Multimedia database • ADMIN: Configuration items for backup locations, redundancy paths and schedule information (not a database) If an application is not available, you cannot select it.
Backup Location	The destination for the network disk. The values are configured in the Backup Locations.
Frequency	The frequency of the backup. You can choose from daily, weekly, monthly, or run once.
Media type	The type of media used for your backup file. You can use a network disk location or a tape drive. If you use a network disk location, you must configure a destination before you can back up the file.
Name	Identifier for the scheduled backup. You can identify each backup with a unique name.

Recovering a scheduled backup

Recover a scheduled backup if an error occurs while the backup is running. A scheduled backup failure can occur for several reasons. For example, if the backup location is not available or if there is not enough space to save the backup file, the scheduled back up fails. If an error occurs, the scheduled backup stops and an event is created. View the event in the Windows Event Viewer.

Prerequisites

- Ensure that you view the event in Windows Event Viewer and address the reason why the scheduled backup failed.

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Database Utilities**, **Database Maintenance**.
2	In the **Database Maintenance** dialog box, in the left pane, click **Scheduled Backup**.
3	Click the name of the scheduled backup to recover.
4	Click **Recover**.
5	Click **OK**.

--End--

Restoring a backup

Restore a backup one database at a time to your servers to restore the database to the point at which the last backup occurred if you encounter a database error.

If you have a co-resident server, restore the databases in the order that the software was installed, Contact Center Manager Server, Communication Control Toolkit second, then Contact Center Multimedia database, then administration files.

Prerequisites

- Ensure that you know the location of the backup file.
- Ensure that you know which database to restore.

Attention: If you restore a CCMM database without restoring the CCMS database, this might result in a mismatch in OAM data. Nortel recommends that when you restore a CCMM database you also restore a corresponding CCMS database.

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Database Utilities**, **Database Maintenance**.
2	In the **Database Maintenance** dialog box, in the left pane, click **Restore**.
3	In the right pane, under **Media Type**, select the media type on which the backup is restored.
4	If the backup file is on the network drive, in the **Backup Location** list, select the backup location.
5	Under **Application**, select the database (CCT, CCMS, or CCMM) or administration (ADMIN) files to restore.
6	Under **Restore contents**, choose the contents to restore for the database.
7	Click **OK**.
8	Use the **Progress information** field to monitor the progress of the restore.
9	Click **Exit** to close the Database Maintenance utility.

--End--

Variable definitions

Variable	Value
Application	The database and applications of Contact Center that you can back up: • CCT: Communication Control Toolkit database • CCMS: Contact Center Manager Server database • CCMM: Contact Center Multimedia database • ADMIN: Configuration items for backup locations, redundancy paths and schedule information (not a database)
Backup Location	The destination for the network disk. The values are configured in the Backup Locations.
Restore contents	The type of content stored in the database. Data is the data in the database or application file. Code is the information for Web services on the Contact Center Multimedia database.
Media type	The type of media used for your backup file. You can use a network disk location or a tape drive. If you use a network disk location, you must configure a destination before you can back up the file.

Procedure job aid

When you restore a Contact Center Multimedia database, if you restore the database backup to a Multimedia server different from where the backup occurred, the e-mail attachments are restored to the original installation attachments folder (\Nortel\Contact Center\Email Attachments\).

After the restore, you must confirm that the Email Configuration settings in the CCMM administrator point to the correct attachments folder.

Migrating the database

Migrate the database from one server to another. You can also migrate a database from a previous release to the current release.

Prerequisites

- Ensure that your database from the previous release of Contact Center is converted to the Caché format. For more information, see *Nortel Contact Center Upgrade and Patches* (NN44400-410).
- Back up the old database.
- Know the drive on your server on which your database is installed.
- Create a backup location. See Creating a backup location (page 492).

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Database Utilities**, **Database Maintenance**.
2	In the **Database Maintenance** dialog box, in the left pane, click **Migration**.
3	In the right pane, select the **Application** from which you want to migrate.
4	In the **Migration Location** box, select the location for your current database backup.
5	Click **OK**.

--End--

Variable definitions

Variable	Value
Application	The possible applications from where you can select a database. For example, if you are on a Contact Center Manager Server 7.0, you can migrate a database from Symposium Call Center Server 5.0 or Contact Center Manager Server 6.0.
Migration Location	The location on the network for the database backup.

Procedure job aid

When you migrate a Contact Center Multimedia database, if you restore the database backup to a new Multimedia server, the e-mail attachments are restored to the original installation attachments folder (:\Nortel\Contact Center\Email Attachments\).

After the restore, you must confirm that the Email Configuration settings in the CCMM administrator point to the correct attachments folder.

Configuring Integrated Reporting

To access ICP-Contact Summary reports and Multimedia-Contact Summary reports, configure Integrated Reporting in Database Maintenance utility.

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Database Utilities**, **Database Maintenance**.
2	in the **Database Maintenance** window, in the left panel, expand **Main Menu** folder.
3	Click **Integrated Reporting Server**.
4	In the right panel, click **Create**.
5	From the **Media** type, select **ICP**.
6	In the **Name** box, type <server name>.
7	In the **Username** box, type the username to log on to the server in the name box.
8	In the **Password** box, type the domain password.
9	Click **OK**.
10	In the right panel, click **Create**.
11	From the type list, select **Multimedia**.
12	Repeat step to step.
13	To close the **Database Maintenance** utility, click **Exit**.

--End--

Variable definitions

Variable	Value
<server name>	The display name that depends on the server type: ICP or Multimedia.

Contact Center server redundancy

A new database technology, Caché from Intersystems, is introduced to both Contact Center Manager Server and Communication Control Toolkit in Contact Center 7.0. Contact Center Multimedia already uses the Caché database. The Caché database is a single data replication technology that is used on the servers: Caché Shadowing. Replication of data in Contact Center 7.0 is peer to peer, removing the need for a separate server resources.

The redundancy mechanism reduces down time and extra hardware by providing a warm standby copy of all of the data in the databases.

The warm standby can be used if a monitored service stops, the active server shuts down, or there is a hardware failure.

Prerequisites to Contact Center Server redundancy

- Install the primary server. For more information, see *Nortel Contact Center Installation* (NN44400-311).
- Install the redundancy or standby server with the same configuration of drive letters and software, site name as the corresponding primary server for Contact Center Manager Server, Communication Control Toolkit, or Contact Center Multimedia. For more information, see *Nortel Contact Center Installation* (NN44400-311).

Navigation

- Configuring resiliency and redundancy for Multimedia (page 513)
- Changing the active Contact Center Multimedia server (page 515)

Configuring managed IP addresses

Configure the managed IP addresses for connections that each of the Contact Center Manager Server and Communication Control Toolkit server use to ensure that a seamless transition occurs between the active and standby servers.

Use managed IP addresses for campus redundancy. With a managed IP address, both the active and standby servers use the same IP address, thus other applications that require calls to the IP address or server name (such as Contact Center Manager Administration needs the Contact Center Manager Server name), require no extra configuration in the contact center system.

In geographic redundancy, where the servers are not necessary near one another, you do not configure a managed IP address for the servers. Instead, the resiliency and redundancy is configured to complete a full site-by-site switchover. If Communication Control Toolkit goes down, then the whole site switches over to the configured standby server configuration for the entire contact center suite.

Procedure steps

Step **Action**

1 Log on to the server where Contact Center Manager Server, Communication Control Toolkit, or Contact Center Multimedia is installed.

2 Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Database Utilities**, **Resiliency and Replication**.

3 In the left pane of the **Resiliency & Replication** window, expand **Configuration**.

4 Click **Server Mode**.

5 Under **Server Mode Configuration**, select **Standby**.

6 Confirm the IP addresses for the **Managed IP**, **Active Server details**, the **Standby Server details** and the **Trusted IP**, if applicable.

7 Click **OK**.

--End--

Variable definitions

Variable	Value
Select Mode	The mode of the server: • Active: The server that currently handles contacts. • Standby: The server that backs up operations if the server fails.
Switchover	The length of time configured for server inactivity before the change to the Standby server for handing contacts.
Managed IP	The IP address that is used for both the Active and Standby servers for campus resiliency.
Active Server details	The IP address for the server initially configured in Active mode.
Standby Server details	The IP address for the server initially configured in Standby mode.
Trusted IP address	The IP address of a trusted server that is not likely to go down so that both Active and Standby servers have something to ping regularly to verify the network connection.

Configuring the standby server

Configure the standby server for each Contact Center Manager Servers and Communication Control Toolkit server to ensure that the Caché database can determine which server is in standby mode. The other server is automatically in active mode.

Procedure steps

Step **Action**

1 Log on to the server where Contact Center Manager Server, Communication Control Toolkit, or Contact Center Multimedia is installed.

2 Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Database Utilities**, **Resiliency and Replication**.

3 In the left pane of the **Resiliency & Replication** window, expand **Configuration**.

4 Click **Server Mode**.

5 Under **Server Mode Configuration**, select **Standby**.

6 To configure a maximum time before the switchover occurs, select the **Switchover** check box, and select a time interval.

7 Click **OK**.

--End--

Variable definitions

Variable	Value
Select Mode	The mode of the server: • Active: The server currently used to handle contacts. • Standby: The server used for back up operation if the server fails.
Switchover	The length of time configured for server inactivity before the change to the Standby server for handing contacts.
Managed IP	The IP address that is used for both the Active and Standby servers for campus resiliency.
Active Server details	The IP address for the server initially configured in Active mode.
Standby Server details	The IP address for the server initially configured in Standby mode.
Trusted IP address	The IP address of a trusted server that is not likely to go down so that both Active and Standby servers have a server to check to verify the network connection.

Configuring the notification of automatic switchovers

Configure the notification tool to inform your system administrator or other designated personnel about the automatic switchover if you configured an automatic switchover in your Standby server configuration.

Prerequisites

- Configure the standby server with automatic switchover. See Configuring managed IP addresses (page 504).
- If you use SNMP clients for notification, you must install the Windows SNMP service before you installed the Caché software. See Installing Windows SNMP Service (page 482).

Procedure steps

Step	Action
1	Log on to the server where Contact Center Manager Server, Communication Control Toolkit, or Contact Center Multimedia is installed.
2	Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Database Utilities**, **Resiliency and Replication**.
3	In the left pane of the **Resiliency & Replication** window, expand **Configuration**.
4	Click **Notifications**.
5	Under **Notification Level**, select an option for the notification.
6	If you choose e-mail, in the **Hours** box, specify the number of hours to elapse between e-mail message notifications.
7	Configure the **Notification Configuration** section to specify your SMTP server name, From Address, and To Address as applicable for your notification level.
8	Click **Verify** to check the logon details for the server.
9	Click **OK**.

--End--

Variable definitions

Variable	Value
Notification Level	The notification format that your administrator receives if the automatic switchover from the Active to Standby server occurs: • Logging: Add an entry to the log file. • SNMP: Use Simple Network Management Protocol to notify configured SNMP clients with the correct MIB files. The MIB file is installed in Nortel/Contact Center/Common Components/ Caché. • WSDL: Not supported for this release. • E-mail: Send an e-mail to the configured personnel.

Configuring manual switchovers

Configure a manual switchover from the Active server to the Standby server if you plan to take the primary server off line for an upgrade, repair, or other maintenance reason. You can manually start the standby server to operate in the primary mode.

Prerequisites

- Configure the standby server for the Contact Center server (CCT, CCMS, or CCMM) you want to manually switchover. See Configuring managed IP addresses (page 504).

Procedure steps

Step	Action
1	Log on to the current primary server with Contact Center Manager Server, Communication Control Toolkit, or Contact Center Multimedia.
2	Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Database Utilities**, **Resiliency and Replication**.
3	In the left pane of the **Resiliency & Replication** window, expand **Tasks**.
4	Double-click **CC Applications**.
5	In the first box, select the server to switchover.
6	Under **Enabled**, select **Yes**.

7	Under Switchover, select **Enabled**.
8	Click **Start**.

--End--

Configuring service monitoring

Configure service monitoring to perform an automatic switchover if a monitored service on the Contact Center Manager Server, the Communication Control Toolkit fails.

Each Contact Center server has different services that are monitored.

Prerequisites

- Configure the standby server for each Contact Center server (CCT, CCMS) on which you want to configure automatic switchover. See Configuring managed IP addresses (page 504).

Procedure steps

Step	Action
1	Log on to the server for which you want to configure the automatic switchover for services that fail.
2	Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Database Utilities**, **Resiliency and Replication**.
3	In the left pane of the **Resiliency & Replication** window, expand **Tasks**.
4	Double-click **CC Configuration**.
5	For each service, select the **Monitor** check box to monitor the service.
6	For each service, select the **Restart** check box to attempt to restart the service.
7	For each service, in the **Start Wait Time** column, type the number of seconds to wait before a service restarts.
8	For each service, in the **Stop Wait Time column**, type the number of seconds to wait before a service stops.
9	For each service, in the **Restart Limit** column, type the maximum number of attempts to restart the service before switchover.
10	For each service, in the **Restart Threshold** column, type the time (in seconds) to reset the Restart Limit after the threshold is passed.

--End--

Procedure job aid

The following table shows the services that are monitored for activity. If the services do not restart, a switchover to the standby server is performed after the configured number of seconds.

Server name	Services monitored
Contact Center Manager Server	OAM_Service TSM_Service ASM_Service TFE_Service
Communication Control Toolkit server	Caché Service NCCT SMON NCCT Logging Service ACD Proxy Telephony NCCT Data Access Layer NCCT TAPI Connector NCCT Server NCCT OI Service
Contact Center Multimedia server	Manual switchover only.
Start Wait Time	The number of seconds to wait before restarting a service.
Stop Wait Time	The length of time the service is stopped before it starts a switchover. So if OAM is set to 60 seconds, then OAM must be down for 60 consecutive seconds before it restarts. It also restarts all dependent services.

Configuring automatic switchovers

Configure automatic switchovers to switch the active server in Contact Center Manager Server or Communication Control Toolkit if the active server shuts down, or there is a hardware failure. You can configure the automatic switchover on either the active or standby server.

Prerequisites

- Configure the standby server for each Contact Center server (CCT, CCMS) on which you want to configure automatic switchover. See Configuring managed IP addresses (page 504).

Procedure steps

Step	Action
1	Log on to the server for which you want to configure the automatic switchover for services that fail.
2	Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Database Utilities**, **Resiliency and Replication**.
3	In the left pane of the **Resiliency & Replication** window, expand **Tasks**.
4	Click **Server Mode**.
5	Select the **Switchover** check box.
6	Configure the number and unit of time until the automatic switchover.
7	Click **OK**.

--End--

Monitoring switchover information

Monitor the switchover information to determine why the automatic or manual switchover occurred.

Also use the monitoring to determine if the current configuration is appropriate to run for a length of time, or if you must switch the active and standby servers back to their original role.

Procedure steps

Step	Action
1	Log on to the server for which you want to review the switchover status.
2	Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Database Utilities**, **Resiliency and Replication**.
3	In the left pane of the **Resiliency & Replication** window, expand **Tasks**.
4	Select **System Control**.
5	Review the content of information in the **System Control** panel to determine why the switchover occurred.
6	In the **Control** box, select the status of the Resiliency configuration.
7	Click **Start**.

--End--

Variable definitions

Variable	Value
Control	Choose to maintain the current active server configuration, or switch back to the original configuration (switchback).

Procedure job aid

The configuration for the automatic switchover is cancelled when one automatic switchover completes. You must re-enable the automatic switchover. See Configuring automatic switchovers (page 511).

Reviewing shadowing

Review the server status to confirm that the shadowing is occurring between the servers.

Procedure steps

Step	Action
1	Log on to the server for which you want to review the switchover status.

2 Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Database Utilities**, **Resiliency and Replication**.

3 In the left pane of the **Resiliency & Replication** window, expand **Configuration**.

4 Select **System**.

5 In the **System Configuration** panel, locate the shadowing entries.

6 Confirm the last record of shadowing is within the last minute of the current time.

7 Click **OK**.

--End--

Configuring resiliency and redundancy for Multimedia

Configure the Resiliency and Redundancy in Contact Center Multimedia. You must perform the steps manually when the active server fails.

Prerequisites

- Install CCMM software on the active server. See *Nortel Contact Center Installation* (NN44400-311).
- Know how to back up the Contact Center Multimedia database. See Performing an immediate backup of the database (page 494).
- Know how to restore the Contact Center Multimedia database. See Restoring a backup (page 498).
- Know how to configure the Resiliency and Replication settings.
- Install CCMM software on the standby server. See *Nortel Contact Center Installation* (NN44400-311).

Procedure steps

Step **Action**

1 Log on to the active or primary Contact Center Multimedia server.

2 Choose **Start**, **All Programs**, **Nortel**, **Contact Center**, **Multimedia Server**, **CCMM Administration**.

3 Expand **Contact Center Multimedia**, **General Administration**.

4 Click **Server Settings**.

5 Ensure the **Contact Center Multimedia Server** is configured with the name of the active server, and the **Contact Center Multimedia Standby** is configured with the name of the current standby server.

6 Choose **Start**, **All Programs**, **Nortel**, **Contact Center**, **Database Utilities**, **Database Maintenance**.

7 Use the Database Maintenance utility to backup the CCMM database.

8 Choose **Start**, **All Programs**, **Nortel**, **Contact Center**, **Database Utilities**, **Resiliency & Replication**.

9 Under **Configuration**, click **Server Mode**.

10 Select the **Active** server mode.

11 Log on to the Contact Center Multimedia standby server.

12 On the Contact Center Multimedia standby server, using the Database Maintenance application, restore the CCMM database backup.

13 In the CCMM Administration application, expand **Database Administration**.

14 Double-click **Server Demotion**.

15 Click **Begin**.

16 Confirm server names (active and standby) and attachment locations on the standby server.

17 On the standby server, choose **Start**, **All Programs**, **Nortel**, **Contact Center**, **Database Utilities**, **Resiliency & Replication**.

18 Under **Configuration**, click **Server Mode**.

19 Select the **Standby** server mode.

20 Log on to the Contact Center Multimedia active server.

21 Choose **Start**, **All Programs**, **Nortel**, **Contact Center**, **Database Utilities**, **Resiliency & Replication**.

22 **Under Tasks, click System Control**.

23 Beside **Control**, select **Shadowing**.

24 Click **Start**.

--End--

Changing the active Contact Center Multimedia server

Change the active Contact Center Multimedia server if the primary server fails for some reason, such as a hardware failure, or network failure. You must manually switch the active server for Contact Center Multimedia.

Prerequisites

- Disconnect the active server from your network.
- Know how to add a Contact Center Multimedia server to the Contact Center Manager Administration application. See *Nortel Contact Center Manager Administration – Client Administration* (NN44400-611).
- Know how to configure the external Web server name in the Contact Center Multimedia Administrator. See Assigning development Web server name (page 397).
- Know how to ensure the CCMM services are running. See Starting individual services (page 517).

Procedure steps

Step	Action
1	In the CCMM Administration application, expand **Database Administration**.
2	Double-click **Server Demotion**.
3	Click **Begin**.
4	Confirm server names (active and standby) and attachment locations on the standby server.
5	Using CCMA, associate the new reporting server.
6	If you have an external Web server, configure the Web server to point to the new active server.
7	Start the CCAD application.
8	Confirm that the CCMM services are running.
9	Using the Resiliency & Replication application, click manual switchover to start shadowing from the new active server.

--End--

Common procedures

This chapter describe the common procedures that you perform to administer your Contact Center software.

Navigation

Starting or stopping Contact Center applications

Use the System Control and Monitor Utility to start and stop all of the applications in Contact Center.

Prerequisites

Attention: When you start the System Control and Monitor Utility on a CCMA server, there is a delay before RptAdmin shows as started. This is expected behavior and the RptAdmin status will correct itself within a short time.

Procedure steps

Step	Action
1	Log on to the server on which the Contact Center applications to start or stop are installed.

2	Click **Start**, **All Programs**, **Nortel**, **Contact Center**, **Common Utilities**, **System Control and Monitor Utility**.
3	Click the **Contact Center** tab.
4	Select the check box for each applications to start or stop on the current server.
5	To start the selected applications, click **Start Contact Center**. **OR** To stop the selected applications, click Stop Contact Center.

--End--

Stopping individual services

During some procedures, you must stop one or more Windows services to manipulate a feature or function.

Prerequisites

- Know which server you are working on.
- Know which service or services you must stop.

Procedure steps

Step	Action
1	Click **Start**, **Administrative Tools**, **Services**.
2	In the **Services** window, right-click the name of the service and click **Stop**.

--End--

Starting individual services

During some procedures, you must start one or more Windows services to manipulate a feature or function.

Prerequisites

- Know which server you are working on.
- Know which service or services you must start.

Procedure steps

Step	Action
1	Click **Start**, **Administrative Tools**, **Services**.
2	In the **Services** window, right-click the name of the service and click **Start**.

--End--

Disabling services

During some procedures, you must disable one or more Windows services to manipulate a feature or function.

Prerequisites

- Know which server you are working on.
- Know which service or services you must disable.

Procedure steps

Step	Action
1	Click **Start**, **Administrative Tools**, **Services**.
2	In the Services window, right-click the name of the service.
3	Click **Properties**.
4	From the Startup type list, choose **Disabled**.
5	Click **OK**.
6	Restart the computer.

--End--

Enabling services

During some procedures, you must enable one or more Windows services to manipulate a feature or function.

Prerequisites

- Know which server which you are working on.
- Know which service or services you must enable.

Procedure steps

Step	Action
1	Click **Start**, **Administrative Tools**, **Services**.
2	In the Services window, right-click the name of the service.
3	Click **Properties**.
4	From the Startup type list, choose **Automatic**.
5	Click **OK**.
6	Restart the computer.

--End--

Adding a server to a domain

Add your Contact Center Manager Server to an existing domain and perform other necessary tasks to ensure that your server works in a domain.

After you install Contact Center Manager Server, you can add your server as a member of an existing domain (stand-alone server only).

Prerequisites

- Install Contact Center Manager Server.
- Ensure that you have domain administrator privileges, or ask the domain administrator to assign you a domain user account for remote access.
- Disable Windows Time Service (for Contact Center Manager Server is in a domain).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Server.
2	Right-click **My Computer**.
3	Select **Properties**.
4	In the **System Properties** dialog box, click the **Computer Name** tab.
5	Click **Change**.
6	In the **Computer Name Changes** dialog box, click the **Domain** option.
7	Type the domain name (you must provide the fully qualified domain name, which includes the prefix and suffix).
8	Click **OK**. *A message appears indicating that the server now belongs to the domain that you specified.*
9	Type your administrator user name and password.
10	Restart the server when you are prompted to do so.

--End--

Server name or IP address change

To change the server name or an IP address of a server already running in your contact center, you must perform the procedures in this chapter to ensure that your servers in the Contact Center suite are updated with the correct information.

Prerequisites for changing server names or IP addresses

- Understand if your network administrator is using a Domain Name Service in your network or if you need to update the HOSTS files on each server when you perform a name or IP address change.
- Know the old server name or IP address for your server and the new server name or IP address for your server.
- Ensure that your server name meets the requirements for the Contact Center server.

Navigation

CCMS server name change

Change the name of the Contact Center Manager Server (CCMS) and update the properties of the CCMS server on all of the other servers in the Contact Center Suite. The new name of the server must meet the specifications of the server names in the Contact Center suite.

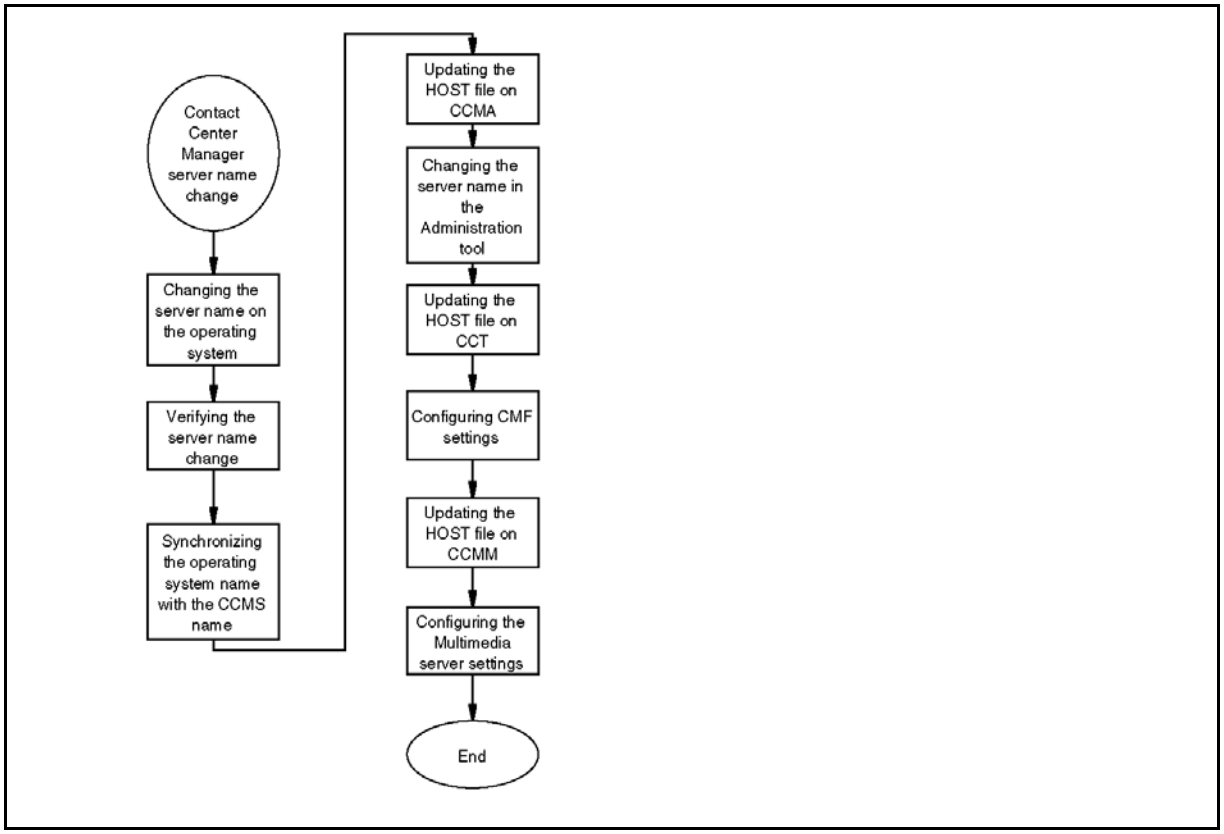
Prerequisites for CCMS server name change

- Ensure that the new server name is unique among both the domain and the other servers on the domain.
- Ensure that the new server name is 6 to 15 characters where the first character is alphabetical.
- Ensure that the new server name contains no underscores (_), hyphens (-), spaces ( ), or punctuation.

CCMS server name change procedures

This task flow shows you the sequence of procedures you perform to change the name of the CCMS server. To link to any tasks, click on CCMS server name change navigation (page 523).

CCMS server name change procedures


Contact Center Manager server name change
Changing the server name on the operating system
Verifying the server name change
Synchronizing the operating system name with the CCMS name
Updating the HOST file on CCMA
Changing the server name in the Administration tool
Updating the HOST file on CCT
Configuring CMF settings
Updating the HOST file on CCMM
Configuring the Multimedia server settings
End

CCMS server name change navigation

- Changing the server name on the operating system (page 523)
- Verifying the server name change (page 524)
- Synchronizing the operating system name with the CCMS name (page 524)
- Updating the HOST file (page 525) on CCMA
- Changing the server name in the Administration tool (page 526)
- Updating the HOST file (page 525) on CCT
- Configuring the Contact Management Framework settings (page 527)
- Updating the HOST file (page 525) on CCMM
- Configuring the Multimedia server settings (page 527)

Changing the server name on the operating system

Change the server name on the Contact Center Manager Server operating system to reflect the new server name.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Server as administrator.
2	On the Contact Center Manager Server, choose **Start**, **Control Panel**, **System**.
3	Click the **Computer Name** tab.
4	Click **Change**.
5	Type the new server name.
6	Click **OK**.
7	Click **Yes** to restart the server.
8	If you use a Domain Name Service, contact your local network prime to update the DNS with the new server name.

--End--

Verifying the server name change

Verify that the Domain Name Service server or network has the correct server name.

Prerequisites

- Change the server name on the operating system. See Changing the server name on the operating system (page 523).

Procedure steps

Step	Action
1	Click **Start**, **Run**.
2	Type **cmd**.
3	Click **OK**.
4	In a Command line window, type **ping <*server name*>**.
5	Verify that the IP address matches the IP address of the server with the new name.

--End--

Variable definitions

Variable	Value
server name	The new name of the server.

Synchronizing the operating system name with the CCMS name

Synchronize the operating system name with the Contact Center Manager Server name to ensure that the Contact Center suite uses the new server name.

Prerequisites

- Verify the server name change. See Verifying the server name change (page 524).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Server as administrator.
2	Close the System Control and Monitor Utility if it is running.
3	Choose **Start**, **All Programs**, **Nortel**, **Contact Center**, **Manager Server**, **Computer Name Synchronisation Utility**.
4	Click **OK**. *If the names do not match, you are prompted to synchronize the names.*
5	After the Contact Center Manager Server services shut down and the synchronize process is complete, click **OK**.
6	On the Synchronization Utility box, click **OK**.
7	Restart the server.

--End--

Updating the HOST file

If you have no DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer name to ensure that all servers can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your server.

Attention: Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows Server 2003.

Procedure steps

Step	Action
1	Log on to the server.
2	Browse to the HOSTS file in the Windows Server 2003 installation directory, C:\Windows\system32\drivers\etc.

3	Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4	Update the file to reflect the new server name of the Contact Center Manager Server.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Changing the server name in the Administration tool

Change the Contact Center Manager Server name in the Administration tool to ensure that the connections in Contact Center Manager Administration connect to the correct server.

Prerequisites

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server name or that you updated the HOSTS file on the Contact Center Manager Administration server with the new Contact Center Manager Server name. See Updating the HOST file (page 525).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Log on to the Contact Center Manager Administration application as an administrator with all access permissions.
3	Double-click **Configuration**.
4	In the left pane, right-click the Contact Center Manager Server name to change.
5	Click **Edit Properties**.
6	Type the new server name, and click **Submit**.

--End--

Configuring the Contact Management Framework settings

Update the Contact Management Framework component in Communication Control Toolkit with the new Contact Center Manager Server name to ensure that the contacts are routed correctly.

Prerequisites

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server name and that you updated the HOSTS file on the Communication Control Toolkit server with the new Contact Center Manager Server name. See Updating the HOST file (page 525).
- Know how to restart the CCT server.

Procedure steps

Step	Action
1	Log on to the Communication Control Toolkit server.
2	Choose **Start**, **All Programs**, **Nortel**, **Contact Center**, **Communication Control Toolkit**, **CCT Console**.
3	Expand **NCCT Admin**.
4	In the left pane, click **CCT Server**.
5	In the right pane, double-click **CCT Server**.
6	Click the **CMF Configuration** tab.
7	In the **CCMS Server Name** box, type the new name of the Contact Center Manager Server.
8	Click **Apply** to save the Contact Management Framework settings.
9	Click **OK** to close the window.
10	Restart the CCT server.

--End--

Configuring the Multimedia server settings

Configure the Multimedia server settings to ensure that the Multimedia database can find the contacts and has the correct name of the Contact Center Manager Server.

Prerequisites

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server name and that you updated the HOSTS file on the Contact Center Multimedia server with the new Contact Center Manager Server name. See Updating the HOST file (page 525).

Procede steps

Step	Action
1	Log on to the Contact Center Multimedia server.
2	Choose **Start**, **All Programs**, **Nortel**, **Contact Center**, **Multimedia Server**, **CCMM Administrator**.
3	Log on to the Contact Center Multimedia Administrator application using an administration user ID and password.
4	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
5	Expand **General Administration**.
6	Double-click **Server Settings**.
7	Select **Contact Center Manager Server**.
8	Click **Edit**.
9	In the **Server Name** box, change the name of the Contact Center Manager Server.
10	Click **Save**.
11	When the warning appears describing potential errors for changing this server, click **OK**.
12	If the License Manager server is installed on the same server as Contact Center Manager Server, in the **Server Settings** window, click **Contact Center License Server**.
13	Click **Edit**.
14	In the **Server Name** box, type the new name of the Contact Center License Manager server.
15	If you have a backup Contact Center License Manager server, type the name in the **Backup Server** box.
16	Click **Save**.
17	When the warning appears, click **OK**.
18	Restart the Multimedia server.

--End--

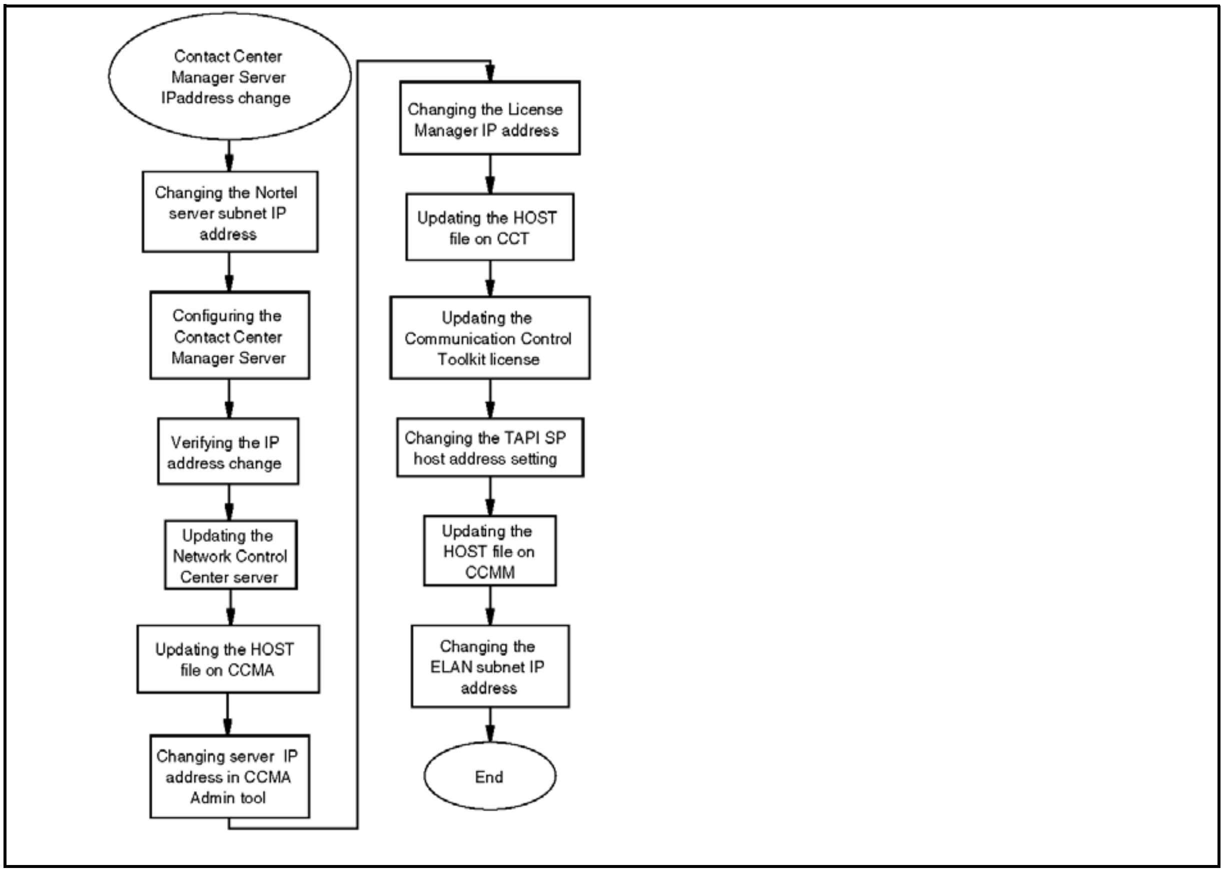
CCMS server IP address change

This section describes the steps you must perform to change the IP address of the Contact Center Manager Server.

CCMS server IP address change procedures

This task flow shows you the sequence of procedures you perform to change the IP address of the Contact Center Manager Server. To link to any tasks, click on CCMS server IP address change navigation (page 529).

CCMS server IP address change procedures


Contact Center Manager Server IPaddress change
Changing the Nortel server subnet IP address
Configuring the Contact Center Manager Server
Verifying the IP address change
Updating the Network Control Center server
Updating the HOST file on CCMA
Changing server IP address in CCMA Admin tool
Changing the License Manager IP address
Updating the HOST file on CCT
Updating the Communication Control Toolkit license
Changing the TAPI SP host address setting
Updating the HOST file on CCMM
Changing the ELAN subnet IP address
End

CCMS server IP address change navigation

- Changing the Nortel server subnet IP address (page 530)
- Configuring the Contact Center Manager Server (page 531)
- Verifying the IP address change (page 531)
- Updating the Network Control Center server (page 532)
- Updating the HOSTS file (page 533) on CCMA
- Updating the server IP address in CCMA (page 534)

- Changing the License Manager IP address (page 534)
- Updating the HOSTS file (page 533) on CCT
- Updating the Communication Control Toolkit license (page 535)
- Updating the HOSTS file (page 533) on CCMM
- Changing the ELAN subnet IP address (page 536)

Changing the Nortel server subnet IP address

Change the Nortel server subnet IP address where the server IP address is recorded.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Server.
2	Choose **Start**, **All Programs**, **Nortel**, **Contact Center**, **Common Utilities**, **System Control and Monitor Utility**.
3	On the **System Control and Monitor Utility** window, click **Shutdown Contact Center**.
4	Choose **Start**, **Control Panel**.
5	Right-click **Network Connections**.
6	Right-click the LAN connection of the Nortel server subnet network interface card, and then click **Properties**.
7	Select **Internet Protocol (TCP/IP)**, and then click **Properties**.
8	Type the new IP address, and then click **OK**.
9	In the **Properties** window, click **Close**.

--End--

Configuring the Contact Center Manager Server

Ensure that the Contact Center Manager Server software has a record of the new IP address for the server to ensure communications between the Contact Center servers continues.

Prerequisites

- Change the Nortel server subnet IP address. See Changing the Nortel server subnet IP address (page 530).

Procedure steps

Step	Action
1	On the Contact Center Manager Server, choose **Start**, **All Programs**, **Nortel, Contact Center**, **Manager Server**, **Server Configuration**.
2	Click **Local Settings**.
3	Under **Nortel Server Subnet**, in the **IP Address** box, type the new Nortel server subnet IP address.
4	If the License Manager server is installed with Contact Center Manager Server, in the **Server Configuration** utility, click **License Manager**.
5	Under **License Server IP Address**, type the new Contact Center Manager IP address.
6	Click **Apply All**.
7	Click **Yes** to restart the server.

--End--

Verifying the IP address change

Verify that the Domain Name Service server or network has the correct server IP address.

Prerequisites

- Configure the Contact Center Manager Server software with the new IP address. See Configuring the Contact Center Manager Server (page 531).

Procedure steps

Step	Action
1	Click **Start**, **Run**.
2	Type **cmd**.
3	Click **OK**.
4	In a Command line window, type **ping <*server name*>**.
5	Verify that the IP address matches the new IP address of the server.

--End--

Variable definitions

Variable	Value
server name	The name of the Contact Center Manager Server.

Updating the Network Control Center server

Update the Network Control Center server if you have a network of Contact Center Manager Servers connected to a Network Control Center server to ensure the Network Control Center server can identify the Contact Center Manager Server.

Prerequisites

- Ensure that you have a network of Contact Center Manager Servers.
- Verify that the IP address changed. See Verifying the IP address change (page 531).

Procedure steps

Step	Action
1	On the Network Control Center server, choose **Start**, **All Programs**, **Nortel, Contact Center**, **Manager Server**, **Network Configuration**.
2	Click the **Site Table** tab.
3	On the **Site Table** tab, select the site name.
4	Click **Edit**.

5	In the **CLAN IP Address** box, type the new IP address.
6	Click **OK**.
7	On the **Nbconfig** dialog box, click **Verify**.
8	On the **Nbconfig** dialog box, click **OK**.
9	Verify that the correct IP address appears on the **Site Table** tab.
10	Click **OK**.

--End--

Updating the HOSTS file

If you have no DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer IP address to ensure that all servers can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your server.

Attention: Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows Server 2003.

Procedure steps

Step	Action
1	Log on to the server.
2	Browse to the HOSTS file in the Windows Server 2003 installation directory, C:\Windows\system32\drivers\etc.
3	Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4	Update the file to reflect the new IP address of the Contact Center Manager Server.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Updating the server IP address in CCMA

Update the server IP address to ensure that the Contact Center Manager Server Administration software has a record of the new IP address for the Contact Center Manager Server to ensure communications between the software is maintained.

Prerequisites

- Change the server IP address. See Changing the Nortel server subnet IP address (page 530).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Log on to the Contact Center Manager Administration application as an administrator with all access permissions.
3	Double-click **Configuration**.
4	In the left pane, right-click the Contact Center Manager Server name to change.
5	Click **Edit Properties**.
6	Type the new server IP address, and click **Submit**.

--End--

Changing the License Manager IP address

If the License Manager server is installed on the same server as Contact Center Manager Server, modify the primary or secondary License Manager server IP address to ensure the entire Contact Center suite servers communicate the licensing information correctly.

Prerequisites

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server IP address, or you updated the HOSTS file on the Contact Center Manager Administration server with the new Contact Center Manager Server IP address. See Updating the HOSTS file (page 533).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Choose **Start**, **All Programs**, **Nortel, Contact Center**, **Manager Administration**, **Configuration**.
3	In the left pane, click **LM Service Configuration**.
4	In the right pane, click the **LM Service Configuration** icon.
5	In the **Primary License Manager Server's IP Address** box, type the new IP address.
6	Click **OK** to submit the information.
7	On the **Configuration Setup Completed** dialog box, click **OK**.
8	Click **Yes** to restart the License Manager service.
9	Click **OK**.
10	On the **File** menu, click **Exit**.

--End--

Updating the Communication Control Toolkit license

If the License Manager server is co-resident with the Contact Center Manager Server, use the following procedure to configure the License Manager IP address for the Communication Control Toolkit server.

Prerequisites

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server IP address, or you updated the HOSTS file on the Communication Control Toolkit server with the new Contact Center Manager Server IP address. See Updating the HOSTS file (page 533).

Procedure steps

Step	Action
1	Log on to the Communication Control Toolkit server.
2	Choose **Start**, **All Programs**, **Nortel**, **Contact Center**, **Communication Control Toolkit**, **CCT Console**.
3	Expand **NCCT Admin**.
4	In the left pane, click **CCT Server**.
5	In the right pane, double-click **CCT Server**.
6	Click the **Licensing** tab.
7	Under **Primary License Manager Server**, in the **IP Address** box, type the new IP address.
8	On the **File** menu, click **Exit**.

--End--

Changing the ELAN subnet IP address

Change the ELAN subnet IP address to ensure that all servers on the network use the correct IP address for the Contact Center Manager Server.

Prerequisites

- Change the Nortel server subnet IP address. See Changing the Nortel server subnet IP address (page 530).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Server.
2	Choose **Start**, **All Programs**, **Nortel**, **Contact Center**, **Common Utilities**, **System Control and Monitor Utility**.
3	On the **System Control & Monitor Utility** window, click **Shutdown Contact Center**.
4	On the Contact Center Manager Server, choose **Start**, **All Programs**, **Nortel, Contact Center**, **Manager Server**, **Server Configuration**.
5	Click the **Local Settings**.

6 Under ELAN Subnet, In the **IP Address** box, type the new ELAN subnet IP address.

7 Click **Apply All**.

8 Click **Yes** to restart the server.

--End--

Co-resident server name change

Change the name of the Co-resident server where Contact Center Manager Server and Contact Center Manager Administration are installed on the same server and update the properties of all other servers in the Contact Center Suite. The new name of the server must meet the specifications of the server names in the Contact Center suite.

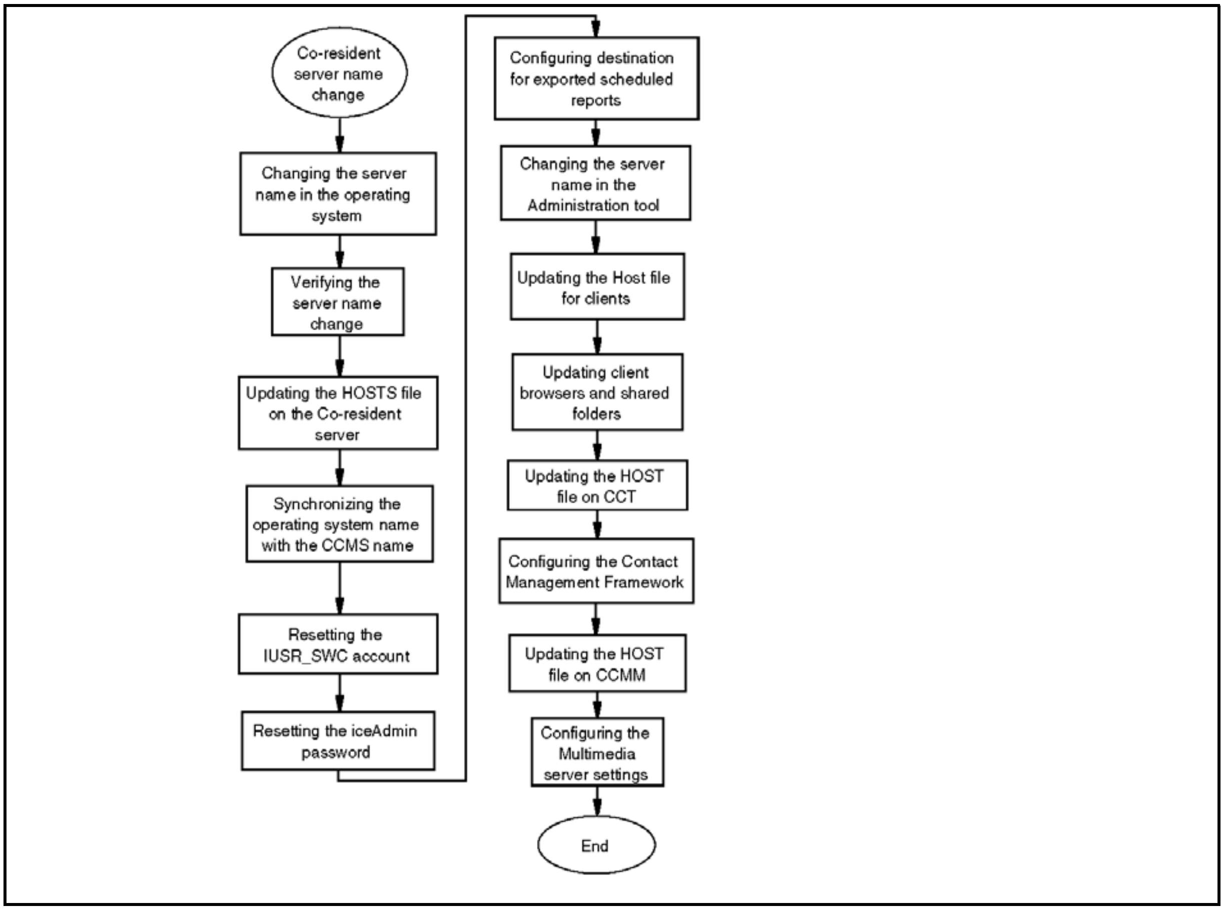
Prerequisites for Co-resident server name change

- Ensure that the new server name is unique among both the domain and the other servers on the domain.
- Ensure that the new server name is from 6 to 15 characters and that the first character is alphabetical.
- Ensure that the new server name contains no underscores (_), hyphens (-), spaces ( ), or punctuation.

Co-resident server name change procedures

This task flow shows you the sequence of procedures you perform to change the name of the co-resident server. To link to any tasks, click on Co-resident server name change navigation (page 539).

Co-resident server name change procedures


Co-resident server name change
Changing the server name in the operating system
Verifying the server name change
Updating the HOSTS file on the Co-resident server
Synchronizing the operating system name with the CCMS name
Resetting the IUSR_SWC account
Resetting the iceAdmin password
Configuring destination for exported scheduled reports
Changing the server name in the Administration tool
Updating the Host file for clients
Updating client browsers and shared folders
Updating the HOST file on CCT
Configuring the Contact Management Framework
Updating the HOST file on CCMM
Configuring the Multimedia server settings
End

Co-resident server name change navigation

- Changing the server name in the operating system (page 540)
- Verifying the server name change (page 540)
- Updating the HOST file (page 541) on the co-resident server
- Synchronizing the operating system name with the CCMS name (page 542)
- Resetting the IUSR_SWC account (page 543)
- Resetting the iceAdmin password (page 544)
- Configuring destination for exported scheduled reports (page 546)
- Changing the server name in the Administration tool (page 547)
- Updating the HOST file for clients (page 547)
- Updating client browsers and shared folders (page 545)
- Updating the HOST file (page 541) on CCT
- Configuring the Contact Management Framework (page 548)

- Updating the HOST file (page 541) on CCMM
- Configuring the Multimedia server settings (page 549)

Changing the server name in the operating system

Change the server name on the Contact Center Manager Server operating system to reflect the new name of the server.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Server as administrator.
2	On the Contact Center Manager Server, choose **Start**, **Control Panel**, **System**.
3	Click the **Computer Name** tab.
4	Click **Change**.
5	Type the new server name.
6	Click **OK**.
7	Click **Yes** to restart the server.
8	If you are using a Domain Name Service, contact your local network prime to update the DNS with the new server name.

--End--

Verifying the server name change

Verify that the Domain Name Service server or network has the correct server name.

Prerequisites

- Ensure that you use a Domain Name Service server in your network.

Procedure steps

Step	Action
1	Click **Start**, **Run**.
2	Type **cmd**.
3	Click **OK**.
4	In a Command line window, type **ping <*server name*>**.
5	Verify that the IP address matches the IP address of the server with the new name.

--End--

Variable definitions

Variable	Value
server name	The new name of the server.

Updating the HOST file

If you have no DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer name to ensure that all servers can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your server.

Attention: Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows Server 2003.

Procedure steps

Step	Action
1	Log on to the server.
2	Browse to the HOSTS file in the Windows Server 2003 installation directory, C:\Windows\system32\drivers\etc.

3	Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4	Update the file to reflect the new server name of the Contact Center Manager Server.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Synchronizing the operating system name with the CCMS name

Synchronize the operating system name with the Contact Center Manager Server name to ensure that the Contact Center suite uses the new server name.

Prerequisites

- Verify that the server name change. See Verifying the server name change (page 540).

Procedure steps

Step	**Action**
1	Log on to the Contact Center Manager Server as administrator.
2	Close the System Control and Monitor Utility if it is running.
3	Choose **Start**, **All Programs**, **Nortel**, **Contact Center**, **Manager Server**, **Computer Name Synchronisation Utility**.
4	Click **OK**. *If the names do not match, you are prompted to synchronize the names.*
5	After the Contact Center Manager Server services shut down and the synchronize process is complete, click **OK**.
6	On the Synchronization Utility box, click **OK**.
7	Restart the server.

--End--

Resetting the IUSR_SWC account

Reset the IUSR_SWC account to reflect the new server name to ensure that users log on to the correct Contact Center Manager Server and Contact Center Manager Administration server.

Prerequisites

- Verify that the server name changed. See Verifying the server name change (page 540).
- Obtain the user ID and password for the IUSR_SWC account from your network administrator.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Choose **Start**, **All Programs**, **Administrative Tools**, **Internet Information Services (IIS) Manager**.
3	In the **Internet Information Services (IIS) Manager** window, expand **<Computer_Name> (local computer)**.
4	Expand the **Web Sites** folder.
5	Right-click **Default Web Site**, and then select **Properties**.
6	In the **Default Web Site Properties** dialog box, click the **Directory Security** tab.
7	In the **Directory Security** tab, under **Authentication and access control**, click **Edit**.
8	In the **Authentication Methods** dialog box, click **Browse**.
9	In the **Select User** dialog box, click **Advanced**.
10	Click **Find Now**.
11	From the list of user accounts, select the IUSR_SWC account, and then click **OK**.
12	Click **OK**.
13	In the **Password** box, type the password you used for this account when you initially configured it.
14	Click **OK**.
15	Type the password again, and then click **OK**.
16	Click **OK** to save your changes.

--End--

Variable definitions

Variable	Value
Computer Name	The name of the computer you must configure for the IIS protocol.

Resetting the iceAdmin password

Reset the iceAdmin password to access the contents of the Administration database.

Prerequisites

- Obtain the domain account name and password from your network administrator.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	On the **Start** menu, click **All Programs**, **Nortel, Contact Center**, **Manager Administration**, **Configuration**.
3	In the left pane, click **Nortel**.
4	In the **Nortel Applications Configuration** window, click **IceAdmin Password Change**.
5	In the **Old Password** box, type the old password.
6	In the **New Passwor**d box, type the new password for the iceAdmin user account.
7	In the **Confirm Password** box, type the password again. *If your Contact Center Manager Administration server is a member of an active domain, the Domain Account option is enabled in the iceAdmin Password Change window.*
8	To export scheduled reports to a domain network PC, click **Domain Account**.
9	From the **Select Domain Name** list, select the name of the domain to add.
10	In the **Enter Domain Account** box, type the domain account.
11	In the **Enter Domain Account Password** box, type the domain account password.

12 In the **Confirm Domain Account Password** box, type the domain account password again.

13 Click **OK**.

14 Click **OK**.

--End--

Updating client browsers and shared folders

Update the client browsers and shared folders to reference the new Contact Center Manager Administration server name in the browser.

Prerequisites

- Ensure that you export scheduled reports in your Contact Center.
- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server name or that you updated the HOSTS file on the clients with the new Contact Center Manager Server name. See Updating the HOST file for clients (page 547).

Procedure steps

Step **Action**

1 Log on to the Contact Center Manager Administration server.

2 Log on to the Contact Center Manager Administration application as an administrator with all access permissions.

3 Double-click **Historical Reporting**.

4 In the **Historical Reporting** main window, on the system tree, click the server under which you want to modify the reports.

5 For each report associated with the new server, right-click the report name.

6 In the **Report Properties** window, click the **Output Options** heading to expand the section.

7 Select the **Output to file** check box.

8 In the **Output path** box, update the path of the report to reflect the new name of the Contact Center Manager Administration server.

9 Click **Save Report**.

10 Click **Activate**.

11 Close the report.

12 Repeat steps 4 to 10 for each report.

--End--

Variable definitions

Variable	Value
Output path	The path of the file in which the historical reports are stored. The path format is \\[computer name]\[shared folder name]\[file name].

Configuring destination for exported scheduled reports

Configure the destination for exported scheduled reports if you export scheduled reports to a domain network computer.

Prerequisites

- Plan to export scheduled reports to a computer on your domain network.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Click **Start**, **All Programs**, **Nortel, Contact Center**, **Manager administration**, **Configuration**.
3	In the left pane, click **Nortel**.
4	Click **IceAdmin Password Change**.
5	In the **IceAdmin Password Change** dialog box, click **Domain Account**.
6	From the **Select Domain Name** list, select the name of the domain to add.
7	In the **Enter Domain Account** box, type the domain account.
8	In the **Enter Domain Account Password** box, type the domain account password.
9	In the **Confirm Domain Account Password** box, type the domain account password.
10	Click **OK**.
11	Click **OK**.

--End--

Changing the server name in the Administration tool

Change the Contact Center Manager Server name in the Administration tool to ensure that the connections in Contact Center Manager Administration are to the correct server.

Prerequisites

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server name and that you updated the HOSTS file on the Contact Center Manager Administration server with the new Contact Center Manager Server name. See Updating the HOST file (page 525).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Log on to the Contact Center Manager Administration application as an administrator with all access permissions.
3	Double-click **Configuration**.
4	In the left pane, right-click the Contact Center Manager Server name to change.
5	Click **Edit Properties**.
6	Type the new server name, and click **Submit**.

--End--

Updating the HOST file for clients

If you have no DNS server, you must manually update the HOSTS file on each client in your contact center with the new computer name to ensure that all clients can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your client.

Attention: Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows.

Procedure steps

Step	Action
1	Log on to the client PC.
2	Browse to the HOSTS file in the Windows installation directory, C:\Windows\system32\drivers\etc.
3	Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4	Update the file to reflect the new server name of the Contact Center Manager Server.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Configuring the Contact Management Framework

Update the Contact Management Framework component in Communication Control Toolkit with the new Contact Center Manager Server name to ensure that the contacts are routed correctly.

Prerequisites

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server name or that you updated the HOSTS file on the Communication Control Toolkit server with the new Contact Center Manager Server name. See Updating the HOST file (page 525).
- Know how to restart the CCT server.

Procedure steps

Step	Action
1	Log on to the Communication Control Toolkit server.
2	On the Start menu, choose **All Programs**, **Nortel**, **Contact Center, Communication Control Toolkit**, **CCT Console**.
3	In the left pane, expand **NCCT Admin**.
4	In the left pane, click **CCT Server**.
5	In the right pane, double-click **CCT Server**.
6	In the **CCT Server Properties** box, click the **CMF Configuration** tab.
7	In the **CCMS Server Name** box, type the new name of the Contact Center Manager Server.
8	Click **Apply** to save the Contact Management Framework settings.
9	Click **OK** to close the window.
10	Restart the CCT server.

--End--

Configuring the Multimedia server settings

Configure the Multimedia server settings to ensure that the Multimedia database can find the contacts and has the correct name of the Contact Center Manager Server.

Prerequisites

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server name or that you updated the HOSTS file on the Contact Center Multimedia server with the new Contact Center Manager Server name. See Updating the HOST file (page 525).

Procedure steps

Step	Action
1	Log on to the Contact Center Multimedia server.
2	Choose **Start**, **All Programs**, **Nortel**, **Contact Center**, **Multimedia Server**, **CCMM Administrator**.

3 Log on to the Contact Center Multimedia Administrator application using an administration user ID and password.

4 In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.

5 Expand **General Administration**.

6 Double-click **Server Settings**.

7 Select **Contact Center Manager Server**.

8 Click **Edit**.

9 In the **Server Name** box, change the name of the Contact Center Manager Server.

10 Click **Save**.

11 When the warning appears describing potential errors for changing this server, click **OK**.

12 If the License Manager server is installed on the same server as Contact Center Manager Server, in the **Server Settings** window, click **Contact Center License Server**.

13 Click **Edit**.

14 In the **Server Name** box, type the new name of the Contact Center License Manager server.

15 If you have a backup Contact Center License Manager server, type the name in the **Backup Server** box.

16 Click **Save**.

17 When the warning message appears, click **OK**.

18 Restart the Multimedia server.

--End--

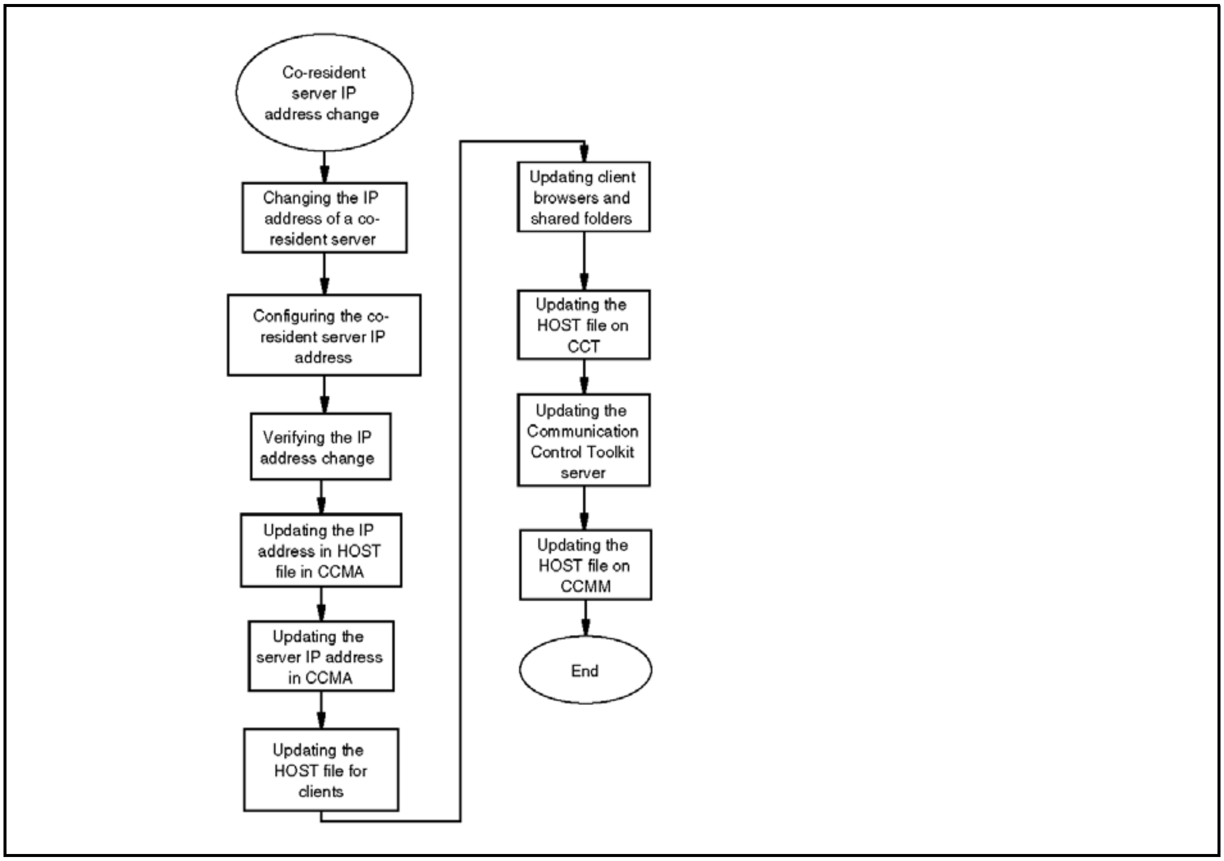
Co-resident server IP address change

Change the IP address of the Co-resident server where Contact Center Manager Server and Contact Center Manager Administration are installed on the same server and update the properties of all of the other servers in the Contact Center Suite.

Co-resident server IP address change procedures

This task flow shows you the sequence of procedures you perform to change the IP address of the co-resident server. To link to any tasks, click on Co-resident server IP address change navigation (page 551).

Co-resident server IP address change procedures


Co-resident server IP address change
Changing the IP address of a co-resident server
Configuring the co-resident server IP address
Verifying the IP address change
Updating the IP address in HOST file in CCMA
Updating the server IP address in CCMA
Updating the HOST file for clients
Updating client browsers and shared folders
Updating the HOST file on CCT
Updating the Communication Control Toolkit server
Updating the HOST file on CCMM
End

Co-resident server IP address change navigation

- Changing the Nortel server subnet IP address of the co-resident server (page 552)
- Configuring the co-resident server IP address (page 553)
- Verifying the server IP address change (page 553)
- Updating the Network Control Center server (page 554)

- Updating the HOST file (page 555) on CCMA
- Updating the server IP address in CCMA (page 556)
- Updating the HOST file for clients (page 556)
- Updating client browsers and shared folders (page 557)
- Updating the HOST file (page 555) on CCT
- Updating the Communication Control Toolkit license (page 559)
- Updating the HOST file (page 555) on CCMM

Changing the Nortel server subnet IP address of the co-resident server

Update the server IP address to ensure that the co-resident server address is updated so that all Contact Center servers have a record of the new IP address for the server to ensure communications between the software is maintained.

Procedure steps

Step	Action
1	Log on to the co-resident server.
2	Choose **Start**, **All Programs**, **Nortel**, **Contact Center**, **Common Utilities**, **System Control and Monitor Utility**.
3	On the **System Control & Monitor Utility** window, click **Shutdown Contact Center**.
4	Choose **Start**, **Control Panel**.
5	Right-click **Network Connections**.
6	Right-click the LAN connection of the Nortel server subnet network interface card, and then click **Properties**.
7	Select **Internet Protocol (TCP/IP)**, and then click **Properties**.
8	Type the new IP address, and then click **OK**.
9	In the **Properties** window, click **Close**.
10	Click **OK**.
11	Click **Yes** to restart the server.

--End--

Configuring the co-resident server IP address

Update the server IP address to ensure that the co-resident server address is updated so that all Contact Center servers have a record of the new IP address for the server to ensure communications between the software is maintained.

Procedure steps

Step	Action
1	Log on to the co-resident server.
2	Choose **Start**, **All Programs**, **Nortel**, **Contact Center**, **Manager Server**, **Server Configuration**.
3	Click the Local Settings tab.
4	Under **Nortel Server Subnet IP** address, type the new Nortel server subnet IP address.
5	If the License Manager server is installed with Contact Center Manager Server, click the **License Manager** tab.
6	Ensure that the Primary License Manager IP Address is the same as the new Contact Center Manager Server IP Address.
7	Click **OK**.

--End--

Verifying the server IP address change

Verify that the Domain Name Service server or network has the correct server IP address.

Prerequisites

- Configure the Contact Center Manager Server software with the new IP address. See Configuring the Contact Center Manager Server (page 531).

Procedure steps

Step	Action
1	Click **Start**, **Run**.

2 Type **cmd**.

3 Click **OK**.

4 In a Command line window, type **ping <*server name*>**.

5 Verify that the IP address matches the new IP address of the server.

--End--

Variable definitions

Variable	Value
server name	The name of the Contact Center Manager Server.

Updating the Network Control Center server

Update the Network Control Center server if you have a network of Contact Center Manager Servers connected to a Network Control Center server to ensure the Network Control Center server can identify the Contact Center Manager Server.

Prerequisites

- Ensure that you have a network of Contact Center Manager Servers.
- Verify that the IP address is changed. See Verifying the IP address change (page 531).

Procedure steps

Step	Action
1	On the Network Control Center server, choose **Start**, **All Programs**, **Nortel**, **Contact Center**, **Manager Server**, **Network Configuration**.
2	Click the **Site Table** tab.
3	On the **Site Table** tab, select the site name.
4	Click **Edit**.
5	In the **CLAN IP Address** box, type the new IP address.
6	Click **OK**.
7	On the **Nbconfig** dialog box, click **Verify**.
8	On the **Nbconfig** dialog box, click **OK**.

9	Verify that the correct IP address appears on the **Site Table** tab.
10	Click **OK**.

--End--

Updating the HOST file

If you have no DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer IP address to ensure that all servers can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your server.

Attention: Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows Server 2003.

Procedure steps

Step	Action
1	Log on to the server.
2	Browse to the HOSTS file in the Windows Server 2003 installation directory, C:\Windows\system32\drivers\etc.
3	Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4	Update the file to reflect the new IP address of the Contact Center Manager Server.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Updating the server IP address in CCMA

Update the server IP address to ensure that the Contact Center Manager Server Administration software has a record of the new IP address for the server to ensure communications between the software is maintained.

Prerequisites

- Change the server IP address. See Changing the Nortel server subnet IP address of the co-resident server (page 552).

Procedure steps

Step	Action
1	On the co-resident server, log on to the Contact Center Manager Administration application as a user with administrative permissions.
2	Click **Configuration**.
3	Right-click the name of the Contact Center Manager Server.
4	Change the IP address for the server.
5	Click **OK**.
6	Click **Yes** to restart the server.

--End--

Updating the HOST file for clients

If you have no DNS server, you must manually update the HOSTS file on each client in your contact center with the new computer name to ensure that all clients can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your client.

Attention: Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows.

Procedure steps

Step	Action
1	Log on to the client.
2	Browse to the HOSTS file in the Windows installation directory, C:\Windows\system32\drivers\etc.
3	Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4	Update the file to reflect the new server name of the Contact Center Manager Server.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Updating client browsers and shared folders

Update the client browsers and shared folders to reference the new Contact Center Manager Administration server name in the browser.

Prerequisites

- Ensure that you export scheduled reports in your Contact Center.
- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server name and that you updated the HOSTS file on the clients with the new Contact Center Manager Server name. See Updating the HOST file for clients (page 556).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Log on to the Contact Center Manager Administration application as an administrator with all access permissions.
3	Double-click **Historical Reporting**.
4	In the **Historical Reporting** main window, on the system tree, click the server under which you want to modify the reports.

5 For each report associated with the new server, right-click the report name.

6 In the **Report Properties** window, click the **Output Options** heading to expand the section.

7 Select the **Output to file** check box.

8 In the **Output path** box, update the path of the report to reflect the new name of the Contact Center Manager Administration server.

9 Click **Save Report**.

10 Click **Activate**.

11 Close the report.

12 Repeat steps 4 to 11 for each report.

--End--

Variable definitions

Variable	Value
Output path	The path of the file in which the historical reports are stored. The path format is \\[computer name]\[shared folder name]\[file name].

Changing the License Manager IP address

If the License Manager server is installed on the same server as Contact Center Manager Server, modify the primary or secondary License Manager server IP address to ensure the entire Contact Center suite servers communicate the licensing information correctly.

Prerequisites

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server IP address or that you updated the HOSTS file on the Contact Center Manager Administration server with the new Contact Center Manager Server IP address. See Updating the HOST file (page 555).

Procedure steps

Step **Action**

1 Log on to the Contact Center Manager Administration server.

2 From the **Start** menu, click **All Programs**, **Nortel, Contact Center**, **Manager Administration**, **Configuration**.

3 In the right pane, click the **LM Service Configuration** icon.

4 In the **Primary License Manager Server's IP Address** box, type the new IP address.

5 Click **OK**.

6 On the **Configuration Setup Completed** dialog box, click **OK**.

7 Click **Yes** to restart the License Manager service.

8 Click **OK**.

9 On the **File** menu, click **Exit**.

--End--

Updating the Communication Control Toolkit license

If the License Manager server is co-resides with the Contact Center Manager Server, configure the License Manager IP address for the Communication Control Toolkit server.

Prerequisites

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server IP address or that you updated the HOSTS file on the Communication Control Toolkit server with the new Contact Center Manager Server IP address. See Updating the HOST file (page 555).

Procedure steps

Step **Action**

1 Log on to the Communication Control Toolkit server.

2 From the **Start** menu, click **All Programs**, **Nortel**, **Contact Center, Communication Control Toolkit**, **CCT Console**.

3 Expand **NCCT Admin**.

4 In the left pane, click **CCT Server**.

5 In the right pane, double-click **CCT Server**.

6 Click the **Licensing** tab.

7 Under **Primary License Manager Server**, in the **IP Address** box, type the new IP address.

8 On the **File** menu, click **Exit**.

--End--

CCMA server name change

Change the name of the Contact Center Manager Administration and update the properties of all of the other servers in the Contact Center Suite. The new name of the server must meet the specifications of the server names in the Contact Center suite.

If the CCMA server is in a domain, and has Active Directory Mode Application (ADAM) replication configured, perform the name change with the server in the domain.

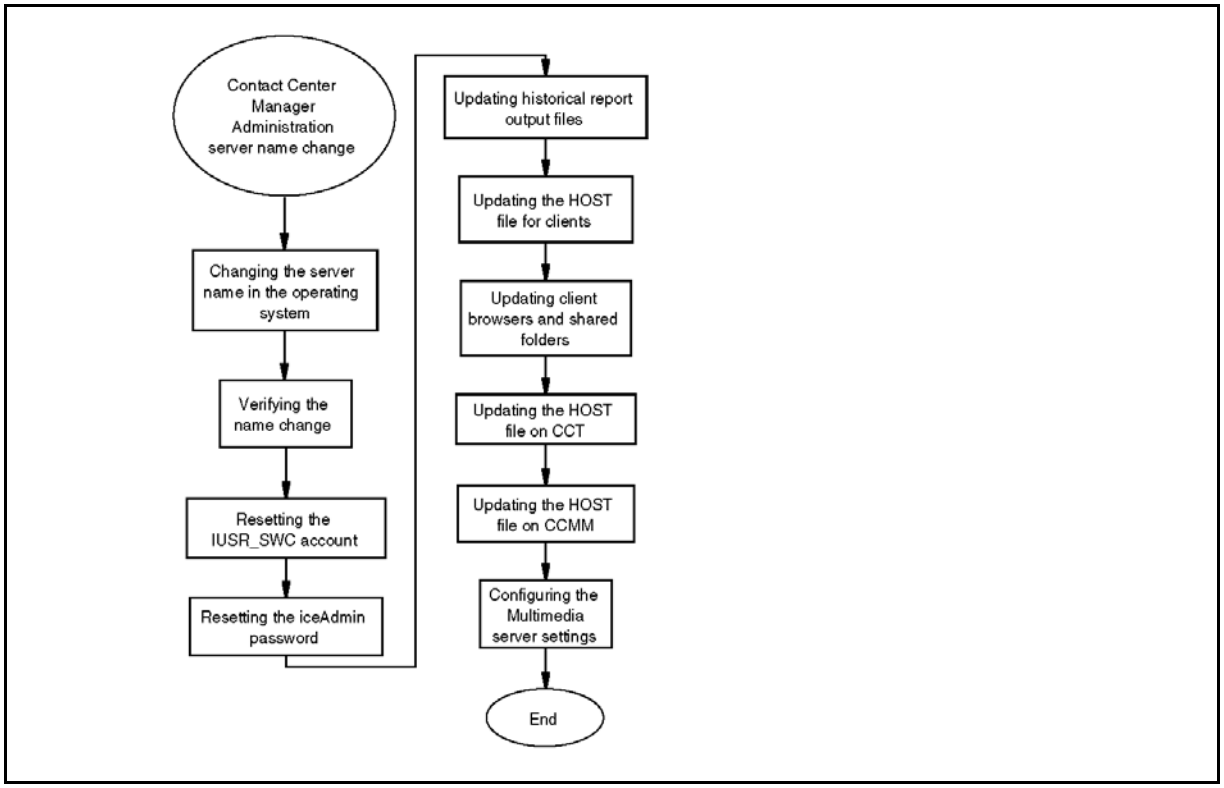
Prerequisites for CCMA server name change

- The name cannot be the same as any other computer or domain name in the network.
- The name must contain 6 to 15 characters (A through Z, 0 through 9).
- The first character of the name must be alphabetical.
- No other characters are allowed. For example, the name cannot include underscores (_).

CCMA server name change procedures

This task flow shows you the sequence of procedures you perform to change the name of the Contact Center Manager Administration server. To link to any tasks, click on CCMA server name change navigation (page 562).

CCMA server name change procedures


Contact Center Manager Administration server name change
Changing the server name in the operating system
Verifying the name change
Resetting the IUSR_SWC account
Resetting the iceAdmin password
Updating historical report output files
Updating the HOST file for clients
Updating client browsers and shared folders
Updating the HOST file on CCT
Updating the HOST file on CCMM
Configuring the Multimedia server settings
End

CCMA server name change navigation

- Changing the server name in the operating system (page 563)
- Verifying the server name change (page 563)
- Resetting the IUSR_SWC account (page 564)
- Resetting the iceAdmin password (page 565)
- Updating historical report output files (page 566)
- Updating the HOST file for clients (page 567)
- Updating client browsers and shared folders (page 568)
- Updating the HOST file (page 569) on CCT
- Updating the HOST file (page 569) on CCMM
- Configuring the Multimedia server settings (page 570)

Changing the server name in the operating system

Change the name of the Contact Center Manager Administration server in the operating system to indicate the name of the server.

Procedure steps

Step **Action**

1 On the Contact Center Manager Administration server, select **Start**, **Control Panel**, and then click **System**.

2 Click the **Computer Name** tab.

3 Click **Change**.

4 In the **Computer Name Changes** dialog box, in the **Computer Name** box, type the new server name.

5 Click **OK**.

6 When you receive a prompt to restart the server, click **Yes**.

--End--

Verifying the server name change

Verify that the Domain Name Service server or network has the correct server name.

Prerequisites

- Ensure that you use a Domain Name Service server in your network.

Procedure steps

Step **Action**

1 Click **Start**, **Run**.

2 Type **cmd**.

3 Click **OK**.

4 In a Command line window, type **ping <*server name*>**.

5 Verify that the IP address matches the IP address of the server with the new name.

--End--

Variable definitions

Variable	Value
server name	The new name of the server.

Resetting the IUSR_SWC account

Reset the IUSR_SWC account to reflect the new server name to ensure that users log on to the correct Contact Center Manager Server and Contact Center Manager Administration server.

Prerequisites

- Verify that the server name is changed. See Verifying the server name change (page 563).
- Obtain the user ID and password for the IUSR_SWC account from your network administrator.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Choose **Start**, **All Programs**, **Administrative Tools**, **Internet Information Services (IIS) Manager**.
3	In the **Internet Information Services (IIS) Manager** window, expand **<Computer_Name> (local computer)**.
4	Expand the **Web Sites** folder.
5	Right-click **Default Web Site**, and then select **Properties**.
6	In the **Default Web Site Properties** dialog box, click the **Directory Security** tab.
7	In the **Directory Security** tab, under **Authentication and access control**, click **Edit**.
8	In the **Authentication Methods** dialog box, click **Browse**.
9	In the **Select User** dialog box, click **Advanced**.
10	Click **Find Now**.

11 From the list of user accounts, select the IUSR_SWC account, and then click **OK**.

12 Click **OK**.

13 In the **Password** box, type the password you used for this account when you initially configured it.

14 Click **OK**.

15 Type the password again, and then click **OK**.

16 Click **OK** to save your changes.

--End--

Variable definitions

Variable	Value
Computer Name	The name of the computer you must configure for the IIS protocol.

Resetting the iceAdmin password

Reset the iceAdmin password to access the contents of the Administration database.

Prerequisites

- Obtain the domain account name and password from your network administrator.

Procedure steps

Step **Action**

1 Log on to the Contact Center Manager Administration server.

2 On the **Start** menu, click **All Programs**, **Nortel, Contact Center**, **Manager Administration**, **Configuration**.

3 In the left pane, click **Nortel**.

4 In the **Nortel Applications Configuration** window, click **IceAdmin Password Change**.

5 In the **Old Password** box, type the old password.

6 In the **New Passwor**d box, reenter the old password for the iceAdmin user account.

7 In the **Confirm Password** box, type the password again.

If your Contact Center Manager Administration server is a member of an active domain, the Domain Account option is enabled on the iceAdmin Password Change window.

8 To export scheduled reports to a domain network PC, click **Domain Account**.

9 From the **Select Domain Name** list, select the name of the domain to add.

10 In the **Enter Domain Account** box, type the domain account.

11 In the **Enter Domain Account Password** box, type the domain account password.

12 In the **Confirm Domain Account Password** box, type the domain account password again.

13 Click **OK**.

14 Click **OK**.

--End--

Updating historical report output files

Configure the destination for exported scheduled reports if you export scheduled reports to a domain network computer.

Prerequisites

- Plan to export scheduled reports to a computer on your domain network.

Procedure steps

Step **Action**

1 Log on to the Contact Center Manager Administration server.

2 Click **Start**, **All Programs**, **Nortel, Contact Center**, **Manager administration**, **Configuration**.

3 In the left pane, click **Nortel**.

4 Click **IceAdmin Password Change**.

5 In the **IceAdmin Password Change** dialog box, click **Domain Account**.

6	From the **Select Domain Name** list, select the name of the domain to add.
7	In the **Enter Domain Account** box, type the domain account.
8	In the **Enter Domain Account Password** box, type the domain account password.
9	In the **Confirm Domain Account Password** box, type the domain account password.
10	Click **OK**.
11	Click **OK**.

--End--

Updating the HOST file for clients

If you have no DNS server, you must manually update the HOSTS file on each client in your contact center with the new computer name to ensure that all clients can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your client.

Attention: Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows.

Procedure steps

Step	Action
1	Log on to the client PC.
2	Browse to the HOSTS file in the Windows installation directory, C:\Windows\system32\drivers\etc.
3	Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4	Update the file to reflect the new server name of the Contact Center Manager Server.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Updating client browsers and shared folders

Update the client browsers and shared folders to reference the new Contact Center Manager Administration server name in the browser.

Prerequisites

- Ensure that you export scheduled reports in your Contact Center.
- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server name or that you updated the HOSTS file on the clients with the new Contact Center Manager Server name. See Updating the HOST file for clients (page 567).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Log on to the Contact Center Manager Administration application as an administrator with full access permissions.
3	Double-click **Historical Reporting**.
4	In the **Historical Reporting** main window, on the system tree, click the server under which you want to modify the reports.
5	For each report associated with the new server, right-click the report name.
6	In the **Report Properties** window, click the **Output Options** heading to expand the section.
7	Select the **Output to file** check box.
8	In the **Output path** box, update the path of the report to reflect the new name of the Contact Center Manager Administration server.
9	Click **Save Report**.
10	Click **Activate**.
11	Close the report.
12	Repeat steps 4 to 11 for each report.

--End--

Variable definitions

Variable	Value
Output path	The path of the file where the historical reports are stored. The path format is \\[computer name]\[shared folder name]\[file name].

Updating the HOST file

If you have no DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer name to ensure that all servers can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your server.

Attention: Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows Server 2003.

Procedure steps

Step	Action
1	Log on to the server.
2	Browse to the HOSTS file in the Windows Server 2003 installation directory, C:\Windows\system32\drivers\etc.
3	Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4	Update the file to reflect the new server name of the Contact Center Manager Server.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Configuring the Multimedia server settings

Configure the Multimedia server settings to ensure that the Multimedia database knows where to find contacts and has the correct name of the Contact Center Manager Server.

Prerequisites

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server name or that you updated the HOSTS file on the Contact Center Multimedia server with the new Contact Center Manager Server name. See Updating the HOST file (page 569).

Procedure steps

Step	Action
1	Log on to the Contact Center Multimedia server.
2	Choose **Start**, **All Programs**, **Nortel**, **Contact Center**, **Multimedia Server**, **CCMM Administrator**.
3	Log on to the Contact Center Multimedia Administrator application using an administration user ID and password.
4	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
5	Expand **General Administration**.
6	Double-click **Server Settings**.
7	Select **Contact Center Manager Server**.
8	Click **Edit**.
9	In the **Server Name** box, change the name of the Contact Center Manager Server.
10	Click **Save**.
11	When the warning appears describing potential errors for changing this server, click **OK**.
12	If the License Manager server is installed on the same server as Contact Center Manager Server, in the **Server Settings** window, click **Contact Center License Server**.
13	Click **Edit**.
14	In the **Server Name** box, type the new name of the Contact Center License Manager server.
15	If you have a backup Contact Center License Manager server, type the name in the **Backup Server** box.
16	Click **Save**.

17 When the warning appears describing potential errors for changing this server, click **OK**.

18 Restart the Multimedia server.

--End--

CCMA server IP address change

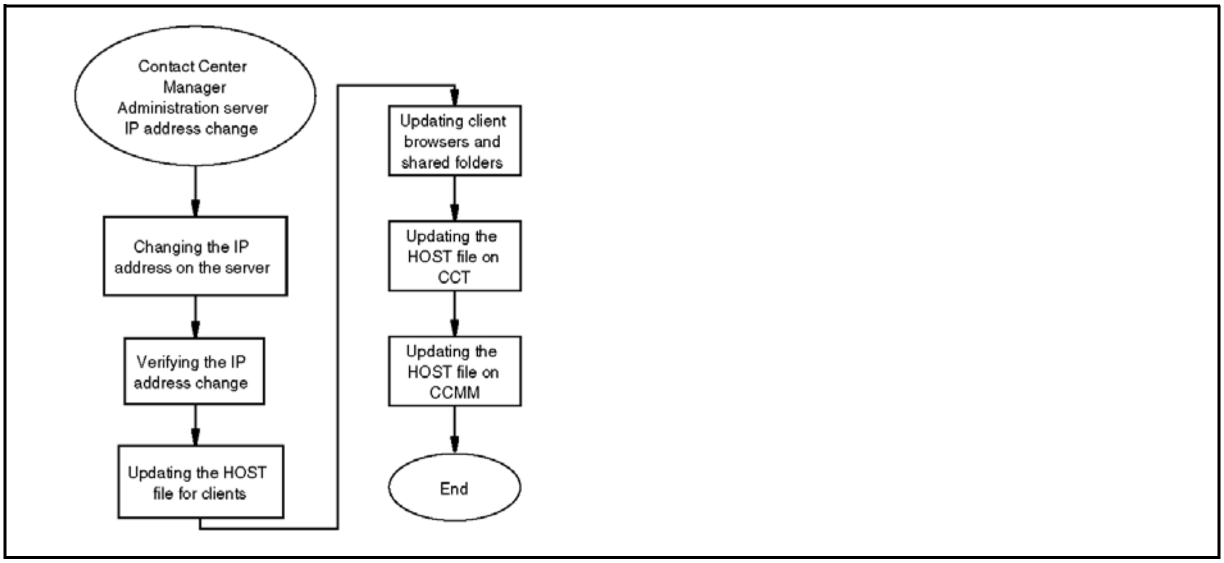
Change the IP address of the Contact Center Manager Administration server and update the properties of all other servers in the Contact Center Suite.

If the CCMA server is in a domain, and has ADAM replication configured, perform the IP address change with the server in the domain.

CCMA server IP address change procedures

This task flow shows you the sequence of procedures you perform to change the Contact Center Manager Administration server IP address. To link to any tasks, click on CCMA server IP address change navigation (page 572).

CCMA server IP address change procedures


Contact Center Manager Administration server IP address change
Changing the IP address on the server
Verifying the IP address change
Updating the HOST file for clients
Updating client browsers and shared folders
Updating the HOST file on CCT
Updating the HOST file on CCMM
End

CCMA server IP address change navigation

- Changing the server IP address on the server (page 573)
- Verifying the server IP address change (page 573)
- Updating the HOST file for clients (page 574)
- Updating client browsers and shared folders (page 575)
- Updating the HOST file (page 576) on the Communication Control Toolkit server
- Updating the HOST file (page 576) on the Contact Center Multimedia server

Changing the server IP address on the server

Update the server IP address to ensure that the Contact Center Manager Server Administration software has a record of the new IP address for the server to ensure communications between the software is maintained.

Procedure steps

Step	Action
1	Choose **Start**, **All Programs**, **Nortel, Contact Center**, **Manager Server**, **Server Configuration**.
2	Click the **Local Settings** tab.
3	Under **Nortel Server Subnet**, type the new Nortel server subnet IP address.
4	If the License Manager server is installed with Contact Center Manager Server, click the **License Manager** tab.
5	Ensure that the Primary License Manager IP Address is the same as the new Contact Center Manager Server IP Address.
6	Click **OK**.
7	Click **Yes** to restart the server.

--End--

Verifying the server IP address change

Verify that the Domain Name Service server or network has the correct server IP address.

Prerequisites

- Configure the Contact Center Manager Administration software with the new IP address. See Verifying the server IP address change (page 573).

Procedure steps

Step	Action
1	Click **Start**, **Run**.
2	Type **cmd**.
3	Click **OK**.

4 In a Command line window, type **ping <*server name*>**.

5 Verify that the IP address matches the new IP address of the server.

--End--

Variable definitions

Variable	Value
server name	The name of the Contact Center Manager Server.

Updating the HOST file for clients

If you have no DNS server, you must manually update the HOSTS file on each client in your contact center with the new computer name to ensure that all clients can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your client.

Attention: Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows.

Procedure steps

Step **Action**

1 Log on to the client PC.

2 Browse to the HOSTS file in the Windows installation directory, C:\Windows\system32\drivers\etc.

3 Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.

4 Update the file to reflect the new server name of the Contact Center Manager Server.

5 On the **File** menu, click **Save**.

6 Close all windows.

--End--

Updating client browsers and shared folders

Update the client browsers and shared folders to reference the new Contact Center Manager Administration server name in the browser.

Prerequisites

- Ensure that you export scheduled reports in your Contact Center.
- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server name or that you updated the HOSTS file on the clients with the new Contact Center Manager Server name. See Updating the HOST file for clients (page 556).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Log on to the Contact Center Manager Administration application as an administrator with all access permissions.
3	Double-click **Historical Reporting**.
4	In the **Historical Reporting** main window, on the system tree, click the server under which you want to modify the reports.
5	For each report associated with the new server, right-click the report name.
6	In the **Report Properties** window, click the **Output Options** heading to expand the section.
7	Select the **Output to file** check box.
8	In the **Output path** box, update the path of the report to reflect the new name of the Contact Center Manager Administration server.
9	Click **Save Report**.
10	Click **Activate**.
11	Close the report.
12	Repeat steps 4 to 11 for each report.

--End--

Variable definitions

Variable	Value
Output path	The path of the file where the historical reports are stored. The path format is \\[computer name]\[shared folder name]\[file name].

Updating the HOST file

If you have no DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer IP address to ensure that all servers can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your server.

Attention: Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows Server 2003.

Procedure steps

Step	Action
1	Log on to the server.
2	Browse to the HOSTS file in the Windows Server 2003 installation directory, C:\Windows\system32\drivers\etc.
3	Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4	Update the file to reflect the new IP address of the Contact Center Manager Server.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

CCT server name change

Change the name of the Communication Control Toolkit server and update the properties of all other servers in the Contact Center Suite. The new name of the server must meet the specifications of the server names in the Contact Center suite.

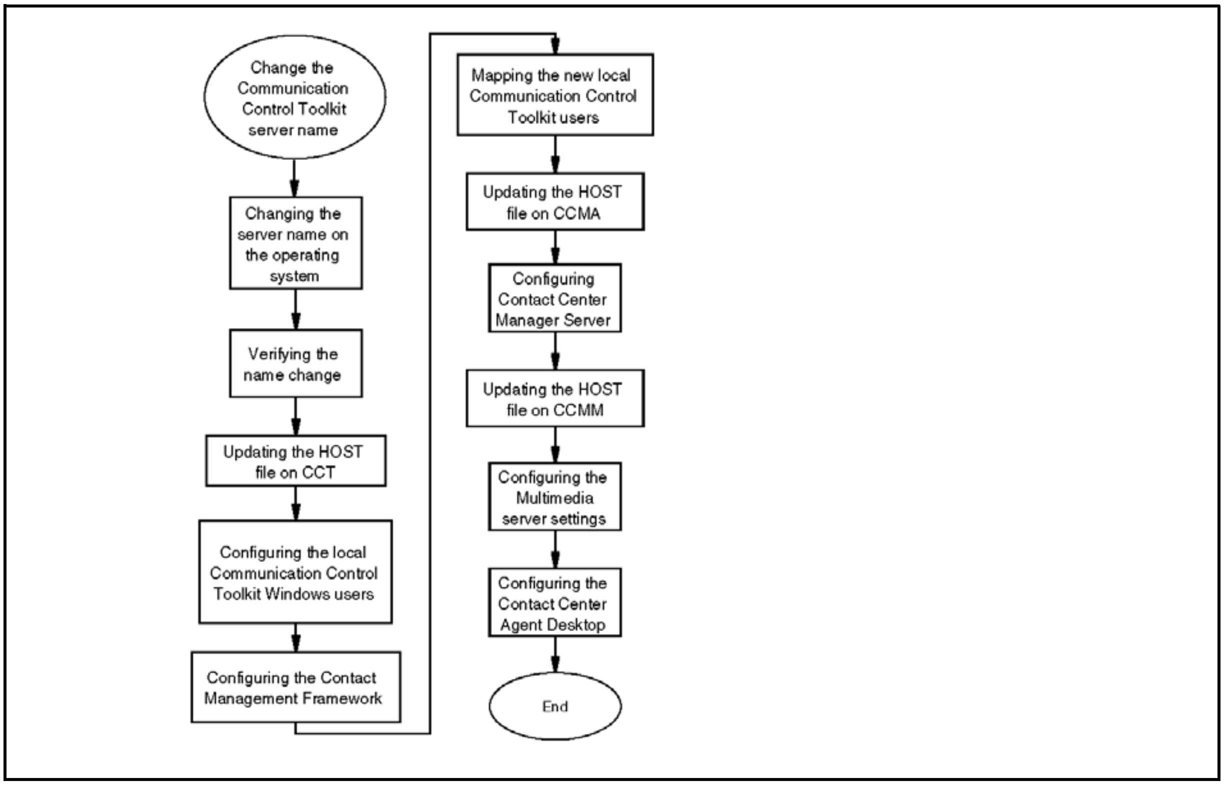
Prerequisites for CCT server name change

- Ensure that the new server name is unique among both the domain and the other servers on the domain.
- Ensure that the new server name is from 6 10 15 characters where the first character is alphabetical.
- Ensure that the new server name contains no underscores (_), hyphens (-), spaces ( ), or punctuation.

CCT server name change procedures

This task flow shows you the sequence of procedures you perform to change the name of the Communication Control Toolkit server. To link to any tasks, click on CCT server name change navigation (page 578).

CCT server name change procedures


Change the Communication Control Toolkit server name
Changing the server name on the operating system
Verifying the name change
Updating the HOST file on CCT
Configuring the local Communication Control Toolkit Windows users
Configuring the Contact Management Framework
Mapping the new local Communication Control Toolkit users
Updating the HOST file on CCMA
Configuring Contact Center Manager Server
Updating the HOST file on CCMM
Configuring the Multimedia server settings
Configuring the Contact Center Agent Desktop
End

CCT server name change navigation

- Changing the server name on the operating system (page 578)
- Verifying the server name change (page 579)
- Updating the HOST file (page 579) on CCT
- Changing the local Communication Control Toolkit Windows users (page 580)
- Configuring the Contact Management Framework (page 581)
- Mapping the new local Communication Control Toolkit users (page 582)
- Updating the HOST file (page 579) on CCMA
- Configuring Contact Center Manager Server (page 583)
- Updating the HOST file (page 579) on CCMM
- Configuring the Multimedia server settings (page 584)
- Configuring the Contact Center Agent Desktop (page 585)

Changing the server name on the operating system

Change the Communication Control Toolkit server name on the operating system to ensure that the server has the correct name and other servers in Contact Center can locate it.

Prerequisites

- Know how to restart the Communication Control Toolkit server.

Procedure steps

Step	Action
1	On the Communication Control Toolkit Server, select **Start**, **Control Panel**, **System**.
2	Click the **Computer Name** tab.
3	Click **Change**.
4	Enter the new server name.
5	Click **OK**.
6	Click **Yes** to restart the server.

--End--

Verifying the server name change

Verify that the Domain Name Service server or network has the correct server name.

Prerequisites

- Ensure that you use a Domain Name Service server in your network.

Procedure steps

Step	Action
1	Click **Start**, **Run**.
2	Type **cmd**.
3	Click **OK**.
4	In a Command line window, type **ping <*server name*>**.
5	Verify that the IP address matches the IP address of the server with the new name.

--End--

Variable definitions

Variable	Value
server name	The new name of the server.

Updating the HOST file

If you have no DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer name to ensure that all servers can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your server.

Attention: Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows Server 2003.

Procedure steps

Step	Action
1	Log on to the server.
2	Browse to the HOSTS file in the Windows Server 2003 installation directory, C:\Windows\system32\drivers\etc.
3	Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4	Update the file to reflect the new server name of the Contact Center Manager Server.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Changing the local Communication Control Toolkit Windows users

Change the local Communication Control Toolkit Windows users to use the new name of the Communication Control Toolkit server.

For example, if the Communication Control Toolkit server uses the user IDs OldName\User1 and OldName\User2, you must reconfigure these local users to use the new name of the Communication Control Toolkit server.

Nortel recommends that you rename the existing users, rather than create new users. Rename the existing users to keep the appropriate resource mappings of the old user name.

Prerequisites

- Change the name of the Communication Control Toolkit server in the operating system. See Changing the server name on the operating system (page 578).

Procedure steps

Step	Action
1	On the **Start** menu, right-click **My Computer**.
2	Click **Manage**.
3	In the **Computer Management** window, expand the **Local Users and Groups**.
4	Click **Users**.
5	Select each user in the users list.
6	In the **User name** box, replace the old server name with the new server name.
7	Click **OK**.

--End--

Configuring the Contact Management Framework

Update the Contact Management Framework component in Communication Control Toolkit with the new Communication Control Toolkit server name.

Prerequisites

- Change the name of the Communication Control Toolkit server in the operating system. See Changing the server name on the operating system (page 578).

Procedure steps

Step	Action
1	Log on to the Communication Control Toolkit server.
2	On the **Start** menu, choose **All Programs**, **Nortel**, **Contact Center, Communication Control Toolkit, CCT Console**.
3	Expand **NCCT Admin**.

4	In the left pane, click **CCT Server**.
5	In the right pane, double-click **CCT Server**.
6	In the **CCT Server Properties** dialog box, click the **CMF Configuration** tab.
7	In the **CCT Server Name** box, type the new name of the Communication Control Toolkit server.
8	In the **CCMS Server Name** box, confirm the name of the Contact Center Manager Server.
9	Click **Apply** to save the Contact Management Framework settings.
10	Click **OK** to close the window.

--End--

Mapping the new local Communication Control Toolkit users

Ensure that the new local Communication Control Toolkit users map to the appropriate addresses, terminals, and groups.

Prerequisites

- Update the users on the Communication Control Toolkit server. See Changing the local Communication Control Toolkit Windows users (page 580).

Procedure steps

Step	Action
1	Log on to the Communication Control Toolkit server.
2	On the **Start** menu, choose **All Programs**, **Nortel**, **Contact Center, Communication Control Toolkit**, **CCT Console**.
3	On the right side of the Console window, expand **NCCT Admin**.
4	Expand **Users**.
5	Double-click the user to configure.
6	Click the **User Group Maps** tab.
7	From the **Available User Groups** list, select the appropriate user groups.
8	Click **Add**.
9	Click the **Terminal Maps** tab.

10 From the **Available Terminals and Terminal Groups** list, select the appropriate terminals and terminal groups for this user.

11 Click **Add**.

12 To automatically allow mapping of address, select the **Automatically map/ unmap related addresses** check box.

13 Click the **Address Maps** tab.

14 From the **Available Addresses and Address Groups** list, select the appropriate terminals and terminal groups for this user.

15 Click **Add**.

16 Click **OK**

--End--

Configuring Contact Center Manager Server

Configure the Contact Center Manager Server software with the name of the new Communication Control Toolkit to ensure that Contact Center Manager works correctly.

Prerequisites

- Change the name of the Communication Control Toolkit server in the operating system. See Changing the server name on the operating system (page 578)

Procedure steps

Step **Action**

1 On the Contact Center Manager Server, select **Nortel, Contact Center**, **Manager Server**, **Server Configuration**.

2 Click the **CCT Server** tab.

3 In the **CCT Host Name** box, type the new name of the Communication Control Toolkit server.

4 Click **Apply**.

--End--

Configuring the Multimedia server settings

Configure the Multimedia server settings to ensure that the Multimedia database can find the contacts and has the correct name of the Contact Center Manager Server.

Prerequisites

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server name or that you updated the HOSTS file on the Contact Center Multimedia server with the new Contact Center Manager Server name. See Updating the HOST file (page 579).

Procedure steps

Step	Action
1	Log on to the Contact Center Multimedia server.
2	Choose **Start**, **All Programs**, **Nortel**, **Contact Center**, **Multimedia Server**, **CCMM Administrator**.
3	Log on to the Contact Center Multimedia Administrator application using an administration user ID and password.
4	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
5	Expand **General Administration**.
6	Double-click **Server Settings**.
7	Select **Contact Center Manager Server**.
8	Click **Edit**.
9	In the **Server Name** box, change the name of the Contact Center Manager Server.
10	Click **Save**.
11	When the warning appears describing potential errors for changing this server, click **OK**.
12	If the License Manager server is installed on the same server as Contact Center Manager Server, in the **Server Settings** window, click **Contact Center License Server**.
13	Click **Edit**.
14	In the **Server Name** box, type the new name of the Contact Center License Manager server.
15	If you have a backup Contact Center License Manager server, type the name in the **Backup Server** box.
16	Click **Save**.

17 When the warning appears describing potential errors for changing this server, click **OK**.

18 Restart the Multimedia server.

--End--

Configuring the Contact Center Agent Desktop

Configure the Contact Center Agent Desktop if you use the Contact Center Agent Desktop with the Communication Control Toolkit to allow agents to monitor calls and make calls using the telephony toolbar.

Prerequisites

- Ensure that agents use the Contact Center Agent Desktop.
- Change the name of the Communication Control Toolkit server in the operating system. See Changing the server name on the operating system (page 578).

Procedure steps

Step **Action**

1 Log on to the Communication Control Toolkit server.

2 In Windows Explorer, navigate to Nortel\Contact Center Multimedia\Agent Desktop.

3 Open the CCADAppSettings.xml file in Notepad.

4 Locate the CCTSERVER key in the CCADAppSettings.xml file.

5 Change the name of the server key to the new Communication Control Toolkit server name.

6 Save the file.

--End--

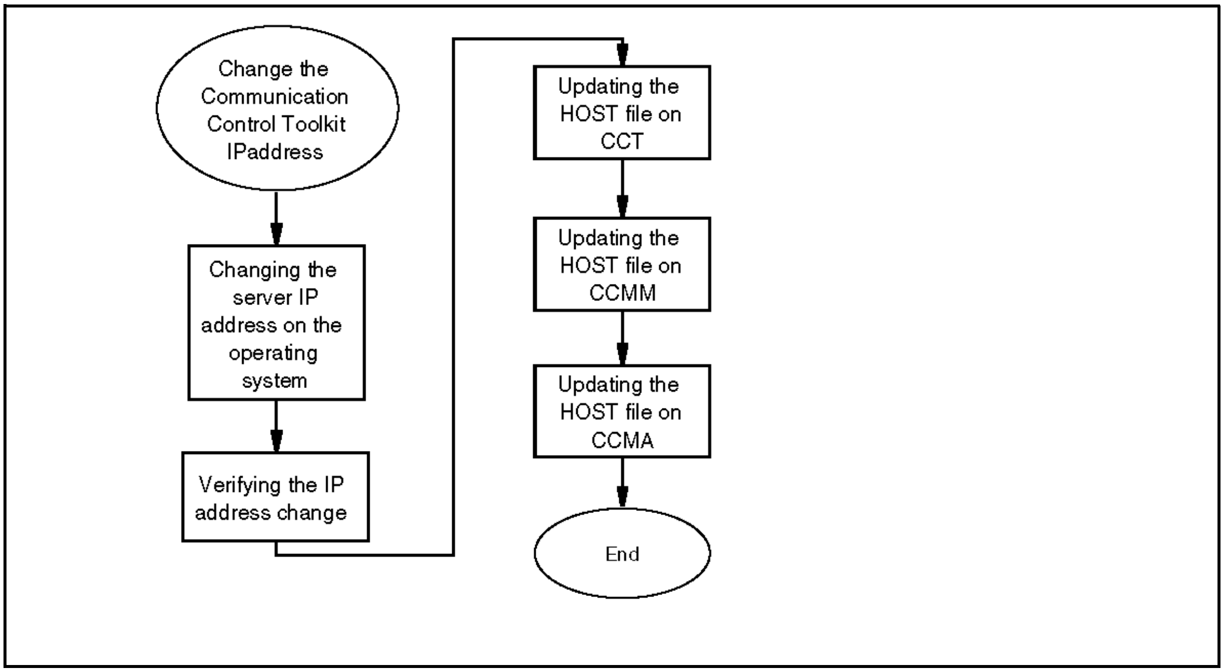
CCT server IP address change

Change the IP address of the Communication Control Toolkit server and update the properties of all other servers in the Contact Center Suite.

CCT server IP address change procedures

This task flow shows you the sequence of procedures you perform to change the IP address of the Communication Control Toolkit server. To link to any tasks, click on CCT server IP address change navigation (page 586).

CCT server IP address change procedures


Change the Communication Control Toolkit IPaddress
Changing the server IP address on the operating system
Verifying the IP address change
Updating the HOST file on CCT
Updating the HOST file on CCMM
Updating the HOST file on CCMA
End

CCT server IP address change navigation

- Changing the server IP address on the operating system (page 587)
- Verifying the server IP address change (page 587)
- Updating the HOST file (page 588) on CCT.
- Updating the HOST file (page 588) on CCMM.
- Updating the HOST file (page 588) on CCMA.

Changing the server IP address on the operating system

Change the Communication Control Toolkit server IP Address on the operating system to ensure that the server has the correct information and other servers in Contact Center can locate it.

Prerequisites

- Know how to restart the Communication Control Toolkit services.

Procedure steps

Step	Action
1	On the Communication Control Toolkit Server, stop the services.
2	From the **Start** menu, choose **Control Panel**.
3	Right-click **Network Connections**.
4	Right-click the LAN connection, and then click **Properties**.
5	Select **Internet Protocol (TCP/IP)**, and then click **Properties**.
6	In the **IP Address** box, type the new IP address.
7	Click **OK**.
8	On the **Properties** window, click **Close**.
9	Restart the services.

--End--

Verifying the server IP address change

Verify that the Domain Name Service server or network has the correct server IP address.

Prerequisites

- Configure the Contact Center Manager Server software with the new IP address. See Configuring the Contact Center Manager Server (page 531).

Procedure steps

Step	Action
1	Click **Start**, **Run**.

2 Type **cmd**.

3 Click **OK**.

4 In a Command line window, type **ping <*server name*>**.

5 Verify that the IP address matches the new IP address of the server.

--End--

Variable definitions

Variable	Value
server name	The name of the Contact Center Manager Server.

Updating the HOST file

If you have no DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer IP address to ensure that all servers can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your server.

Attention: Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows Server 2003.

Procedure steps

Step **Action**

1 Log on to the server.

2 Browse to the HOSTS file in the Windows Server 2003 installation directory, C:\Windows\system32\drivers\etc.

3 Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.

4 Update the file to reflect the new IP address of the Contact Center Manager Server.

5 On the **File** menu, click **Save**.

6 Close all windows.

--End--

CCMM server name change

Change the name of the Contact Center Multimedia server and update the properties of all other servers in the Contact Center Suite. The new name of the server must meet the specifications of the server names in the Contact Center suite.

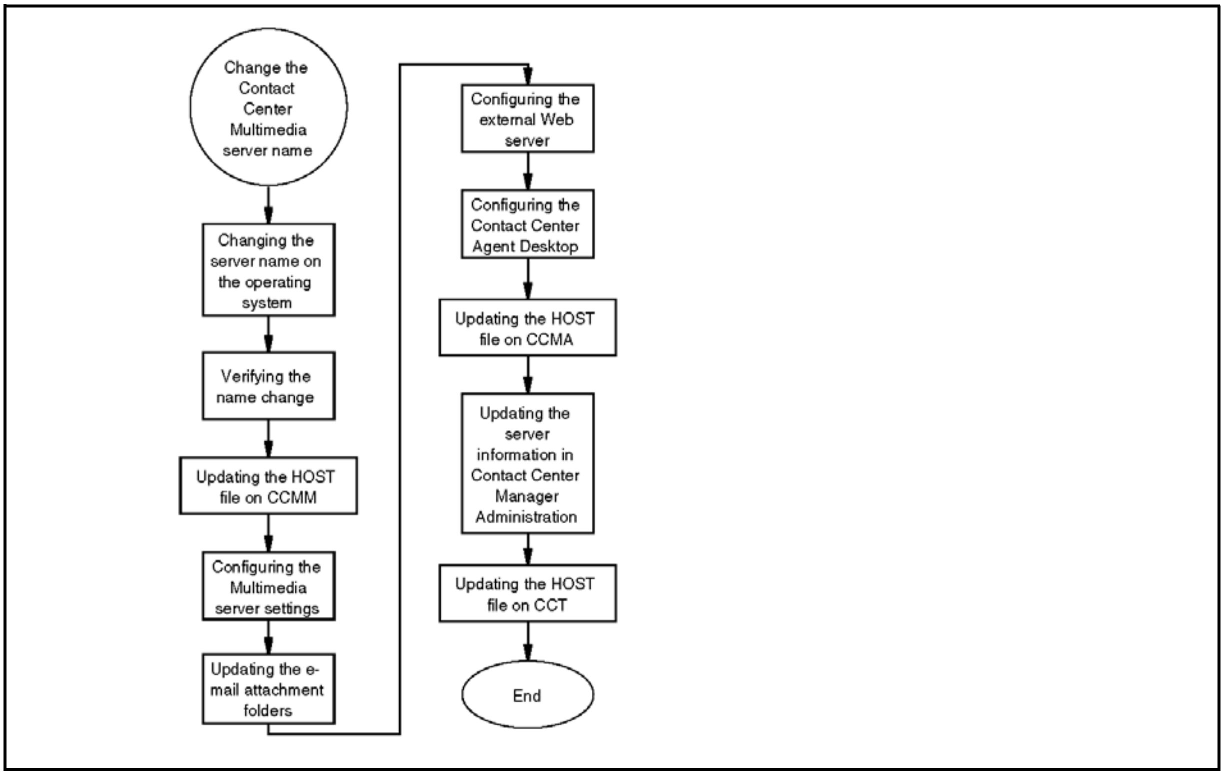
Prerequisites for CCMM server name change

- Ensure that the new server name is unique among both the domain and the other servers on the domain.
- Ensure that the new server name is from 6 to 15 characters in which the first character is alphabetical.
- Ensure that the new server name contains no underscores (_), hyphens (-), spaces ( ), or punctuation.

CCMM server name change procedures

This task flow shows you the sequence of procedures you perform to change the name of the Contact Center Multimedia server. To link to any tasks, click on CCMM server name change navigation (page 590).

CCMM server name change procedures


Change the Contact Center Multimedia server name
Changing the server name on the operating system
Verifying the name change
Updating the HOST file on CCMM
Configuring the Multimedia server settings
Updating the e-mail attachment folders
Configuring the external Web server
Configuring the Contact Center Agent Desktop
Updating the HOST file on CCMA
Updating the server information in Contact Center Manager Administration
Updating the HOST file on CCT
End

CCMM server name change navigation

- Changing the server name on the operating system (page 591)

- Verifying the server name change (page 592)
- Updating the HOST file (page 592) on CCMM
- Configuring the Multimedia server settings (page 593)
- Updating the e-mail attachment folders (page 595)
- Configuring the external Web server (page 595)
- Configuring the Contact Center Agent Desktop (page 597)
- Updating the HOST file (page 592) on CCMA
- Updating the server information in Contact Center Manager Administration (page 598)
- Updating the HOST file (page 592) on CCT

Changing the server name on the operating system

Change the Contact Center Multimedia server name on the operating system so that the server software recognizes the new name in the Contact Center.

Procedure steps

Step	Action
1	Log on to the Contact Center Multimedia server.
2	On the **Start** menu, choose **Control Panel**, **System**.
3	Click the **Computer Name** tab.
4	Click **Change**.
5	Enter the new server name.
6	Click **OK**.
7	Click **Yes** to restart the server.

--End--

Verifying the server name change

Verify that the Domain Name Service server or network has the correct server name.

Prerequisites

- Ensure that you use a Domain Name Service server in your network.

Procedure steps

Step	Action
1	Click **Start**, **Run**.
2	Type **cmd**.
3	Click **OK**.
4	In a Command line window, type **ping <*server name*>**.
5	Verify that the IP address matches the IP address of the server with the new name.

--End--

Variable definitions

Variable	Value
server name	The new name of the server.

Updating the HOST file

If you have no DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer name to ensure that all servers can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your server.

Attention: Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows Server 2003.

Procedure steps

Step	Action
1	Log on to the server.
2	Browse to the HOSTS file in the Windows Server 2003 installation directory, C:\Windows\system32\drivers\etc.
3	Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4	Update the file to reflect the new server name of the Contact Center Manager Server.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Configuring the Multimedia server settings

Configure the Contact Center Multimedia server name in the Multimedia Administrator application and ensure that the folders are labelled correctly to access the multimedia database.

Prerequisites

- Change the name of the Contact Center Multimedia server. See Changing the server name on the operating system (page 591).

Procedure steps

Step	Action
1	Log on to the Contact Center Multimedia server.
2	Choose **Start**, **All Programs**, **Nortel**, **Contact Center**, **Multimedia Server**, **CCMM Administrator**.
3	Log on to the Contact Center Multimedia Administrator using an administrator ID and password.
4	In the Contact Center Multimedia Administrator window, expand **Contact Center Multimedia**.
5	Expand **General Administration**.
6	Double-click **Server Settings**.

7 On the Server Settings dialog box, select **Contact Center Multimedia Server**.

8 Click **Edit**.

9 In the **Server Name** box, type the name of the Contact Center Multimedia server.

10 In the **Server Port** box, change the port number of the server as required. The default server port is 1972.

11 To change the MCMC event port number, type the new number in the **MCMC Event Port** box. The default MCMC event port number is 7999.

12 Click **Save**.

13 A warning appears describing potential errors for changing this server. Click **OK** to accept.

14 Click **Close** to close the Server Settings dialog box.

15 On the Contact Center Multimedia server, navigate to the path D:\Avaya\Contact Center\Multimedia Server\Agent Desktop\CCADAppSettings.xml.

16 On the appropriate line of the text file, replace the name of the old Contact Center Multimedia server with the new Contact Center Multimedia server.

17 On the Contact Center Multimedia server, navigate to the path D:\Avaya\Contact Center\Multimedia Server\Outbound Client\OCMTappsetting.xml.

18 On the appropriate line of the text file, replace the name of the old Contact Center Multimedia server with the new Contact Center Multimedia server.

19 On the Contact Center Multimedia server, navigate to the path D:\Avaya\Contact Center\Multimedia Server\Common utilities\db.properties.

20 On the appropriate line of the text file, replace the name of the old Contact Center Multimedia server with the new Contact Center Multimedia server.

21 On the **Start** menu, choose **All Programs**, **Nortel Contact Center**, **Multimedia Server**, **CCMM Services Control**.

22 On the CCMM Service Control dialog box, click **Stop All.**

23 Click **Start All**.

24 Click **Exit** to close the CCMM Service Control window.

--End--

Updating the e-mail attachment folders

Update the e-mail attachment folders for Contact Center Multimedia. If you are licensed for e-mail messages in your contact center, you must update the e-mail attachment folders.

Prerequisites

- Ensure that you have the e-mail feature installed and enabled using the License Manager.

Procedure steps

Step	Action
1	In the Multimedia Administrator, expand **Contact Center Multimedia**.
2	Expand **Email Administration**.
3	Double-click **Email Configuration**.
4	Click **Save**.
5	Close the Contact Center Multimedia Administrator.
6	On the **Start** menu, click **All Programs**, **Nortel Contact Center**, **Multimedia Server**, **CCMM Services Control**.
7	On the CCMM Service Control dialog box, click **Stop All**.
8	Click **Start All**.
9	Click **Exit** to close the CCMM Service Control window.

--End--

Configuring the external Web server

Configure the external Web server to update the files with the new server name if you have an external Web server in your contact center. You must update for .jsp files with Apache Tomcat. If you use a different servlet engine (for example, JRun or WebLogic) or a different technology (ASP.NET), you must use the standard procedures for your environment.

Prerequisites

- Know the custom interface folder names and paths for the web.xml and .jsp files for the sample customer Web installation.

Procedure steps

Step	Action
1	Log on to your external Web server.
2	On the **Start** menu, choose **All Programs**, **Administrative Tools**, **Services**.
3	Right-click **Apache Tomcat** service, and click **Stop**.
4	Close the services window.
5	On the external Web server, navigate to ..\webapps\CI_Sample_Website\WEB-INF.
6	Open the web.xml file in Notepad or another text editor.
7	Locate the text string <param-name>CCMM_HOSTNAME</paramname>.
8	In the <param-name> line, replace the old server name with the name of the new server.
9	Save and close the file.
10	On the external Web server, navigate to ..\webapps\WebComms\WEB-INF.
11	Open the web.xml file in Notepad or another text editor.
12	Locate the text string <param-name>CCMM_HOSTNAME</paramname>.
13	In the <param-name> line, replace the old server name with the new server name.
14	Save and close the file.
15	Delete all files in the following folders: • ..Program Files\Apache Software Foundation\Tomcat 5.5\Catalina\localhost\CI_Sample_Website\org\apache\jsp • ..Program Files\Apache Software Foundation\Tomcat 5.5\Catalina\localhost\WebComms\org\apache\jsp
16	On the **Start** menu, choose **All Programs**, **Administrative Tools**, **Services**.
17	Right-click **Apache Tomcat** service, and click **Start**.
18	Close the services window.

--End--

Variable definitions

Variable	Value
CCMM_HOSTNAME	The name of the Contact Center Multimedia server.

Configuring the Contact Center Agent Desktop

Configure the Contact Center Agent Desktop to allow agents to monitor calls and make calls using the telephony toolbar.

Prerequisites

- Ensure that agents use the Contact Center Agent Desktop.
- Change the name of the Contact Center Multimedia server in the operating system. See Changing the server name on the operating system (page 591).

Procedure steps

Step	Action
1	Log on to the Agent desktop.
2	Change the URL that agents use to access the Contact Center Agent Desktop to reflect the new server name.

--End--

Variable definitions

Variable	Value
URL	The Uniform Resource Locator (URL) agents use to access the Contact Center Agent Desktop. The format of the URL is http://<servername>/agentdesktop/ccad.exe.

Updating the server information in Contact Center Manager Administration

Update the Contact Center Multimedia server name in the Contact Center Manager Administration. You can configure more than one Contact Center Multimedia server in Contact Center Manager Administration, but only one Contact Center Multimedia server is active at a time.

Prerequisites

- Change the name of the Contact Center Multimedia server. Changing the server name on the operating system (page 591).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	In a Web browser, start the Contact Center Manager Administration browser.
3	Click **Configuration**.
4	From the **Server** menu, select **Add Server**.
5	On the **Contact Center Manager server Properties** window, in the **Server Name** box, type the name of the Contact Center Multimedia server. *The system automatically completes the IP address and display name.*
6	In the **Login ID** box, type the logon ID for the reporting user name for the server.
7	In the **Password** box, type the password for the reporting user name for the server.
8	From the **Type** list, select **CCMM**.
9	Click **Submit**.
10	In the left pane, select the Contact Center Manager Server with which you want to associate the Contact Center Multimedia server.
11	Right-click the Contact Center Manager Server, and then click **Edit Properties**.
12	Under **Associated Reporting Server**, select the check box next to the current active Contact Center Multimedia server name.
13	Click **Submit**.
14	On the Launchpad menu, click **Logout**.

--End--

Variable definitions

Variables	Value
<CCMA_ServerName>	The name of the server where Contact Center Manager Administration is installed.
Login ID	The name used to generate multimedia reports. The default logon ID for the Contact Center Multimedia server is mmReport.
Password	The password used for the ID used to generate multimedia reports. The default user password is mmRep.

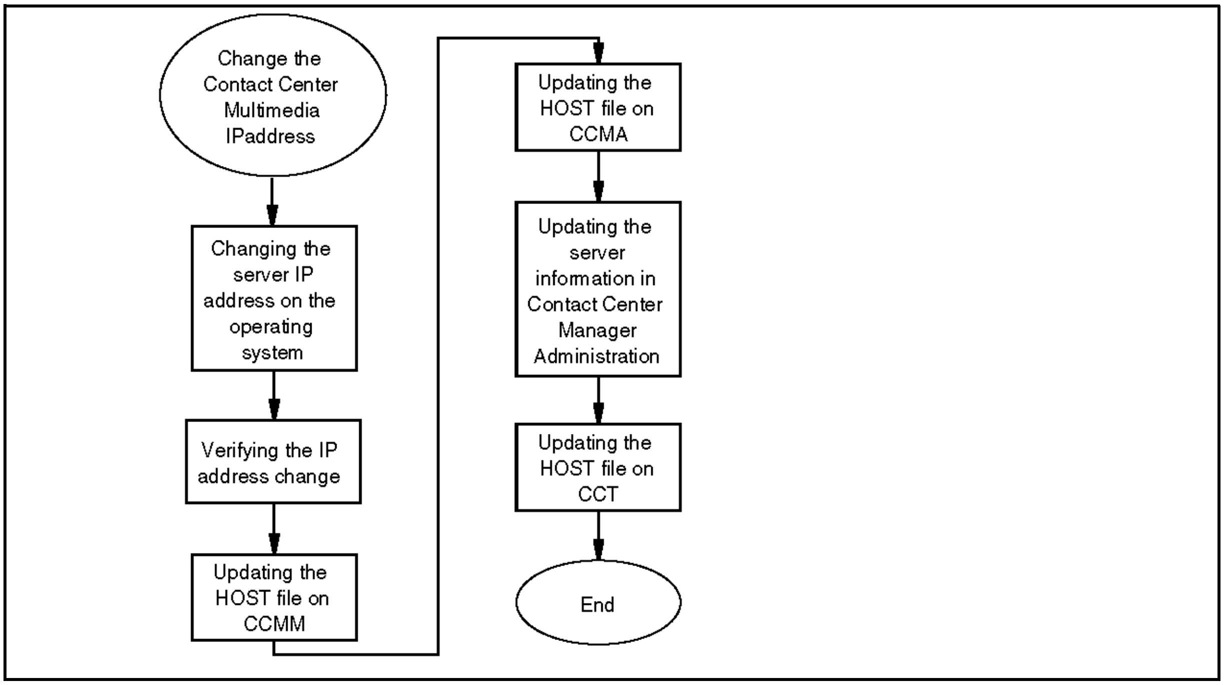
CCMM server IP address change

Change the IP address of the Contact Center Multimedia server and update the properties of all of the other servers in the Contact Center Suite.

CCMM server IP address change procedures

This task flow shows you the sequence of procedures you perform to change the IP address of the Contact Center Multimedia server. To link to any tasks, click on CCMM server IP address change navigation (page 600).

CCMM server IP address change procedures


Change the Contact Center Multimedia IPaddress
Changing the server IP address on the operating system
Verifying the IP address change
Updating the HOST file on CCMM
Updating the HOST file on CCMA
Updating the server information in Contact Center Manager Administration
Updating the HOST file on CCT
End

CCMM server IP address change navigation

- Changing the IP address on the operating system (page 601)
- Verifying the server IP address change (page 601)
- Updating the HOST file (page 602) on CCMM
- Changing the IP address on the operating system (page 601)
- Updating the HOST file (page 602) on CCMA
- Updating the server information in Contact Center Manager Administration (page 603)
- Updating the HOST file (page 602) on CCT

Changing the IP address on the operating system

Change the Contact Center Multimedia server IP address on the operating system to ensure that the server has the correct information and other servers in Contact Center can locate it.

Prerequisites

- Know how to stop and restart the Contact Center Multimedia services.

Procedure steps

Step	Action
1	Log on to the Contact Center Multimedia server.
2	Stop all of the multimedia services.
3	From the **Start** menu, choose **Control Panel**.
4	Right-click **Network Connections**.
5	Right-click the LAN connection, and then click **Properties**.
6	Select **Internet Protocol (TCP/IP)**, and then click **Properties**.
7	In the **IP Address** box, type the new IP address.
8	Click **OK**.
9	On the **Properties** window, click **Close**.
10	Restart the multimedia services.

--End--

Verifying the server IP address change

Verify that the Domain Name Service server or network has the correct server IP address.

Procedure steps

Step	Action
1	Click **Start**, **Run**.
2	Type **cmd**.
3	Click **OK**.

4	In a Command line window, type **ping <*server name*>**.
5	Verify that the IP address matches the new IP address of the server.

--End--

Variable definitions

Variable	Value
server name	The name of the Contact Center Manager Server.

Updating the HOST file

If you have no DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer IP address to ensure that all servers can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your server.

Attention: Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows Server 2003.

Procedure steps

Step	Action
1	Log on to the server.
2	Browse to the HOSTS file in the Windows Server 2003 installation directory, C:\Windows\system32\drivers\etc.
3	Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4	Update the file to reflect the new IP address of the Contact Center Manager Server.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Updating the server information in Contact Center Manager Administration

Update the Contact Center Multimedia server name in the Contact Center Manager Administration. You can configure more than one Contact Center Multimedia server in Contact Center Manager Administration, but only one Contact Center Multimedia server is active at a time.

Prerequisites

- Change the name of the Contact Center Multimedia server. Changing the IP address on the operating system (page 601).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Log on to the Contact Center Manager Administration application as a user with administrative permissions.
3	Click **Configuration**.
4	From the **Server** menu, select **Add Server**.
5	On the **Contact Center Manager server Properties** window, in the **Server Name** box, type the name of the Contact Center Multimedia server. *The system automatically completes the IP address and display name.*
6	In the **Login ID** box, type the logon ID for the reporting user name for the server.
7	In the **Password** box, type the password for the reporting user name for the server.
8	From the **Type** list, select **CCMM**.
9	Click **Submit**.
10	In the left pane, select the Contact Center Manager Server with which you want to associate the Contact Center Multimedia server.
11	Right-click the Contact Center Manager Server, and then click **Edit Properties**.
12	Under **Associated Reporting Server**, select the check box next to the current active Contact Center Multimedia server name.

13 Click **Submit**.

14 On the Launchpad menu, click **Logout**.

--End--

Variable definitions

Variables	Value
<CCMA_ServerName>	The name of the server where Contact Center Manager Administration is installed.
Login ID	The name used to generate multimedia reports. The default logon ID for the Contact Center Multimedia server is mmReport.
Password	The password used for the ID used to generate multimedia reports. The default user password is mmRep.

Appendix

Default login values

For security purposes, you can log on to the different Contact Center applications with the default login values listed in the following table. Refer to the list to acquire the default usernames and passwords.

Application	Default user ID	Default Password	Notes
Manager Server–Commissioning	NGenDist OR NGenSys	<user defined>	
Server Administration–Server Utility	sysadmin	nortel	
Manager Administration Commissioning–ICEAdmin user ID	<user sets up their own account>	<user sets up their own account>	
Manager Administration Commissioning–ADAM user ID	webadmin	webadmin	
Manager Administration–with no Security Framework	webadmin	webadmin	
Administration user for UCM Commissioning–with Security Framework	admin	<configured by user>	
Manager Administration–Commissioning	sysadmin	__ccmm! (underscore, underscore, c, c, m, m, !)	

Application	Default user ID	Default Password	Notes
Virtual directories for IIS–Commissioning	<servername>\CCMMOPSUSER	_mm6NtRed!	
CCT clients	Windows user configured in CCT client		Failed authentication attempts are not logged in the NCCT Security Log because Windows only invokes the CCT service after successfully authenticating the client credentials.
Process Monitor–Common Utilities		__nortel (underscore, underscore, n, o, r, t, e, l)	
Trace Control Utility–Common Utilities		__nortel (underscore, underscore, n, o, r, t, e, l)	

Nortel Contact Center

Server Administration

Publication: NN44400-610
Document status: Standard
Document issue: 01.10
Document date: 27 August 2010
Product release: Release 7.0
Job function: Administration
Type: NTP
Language type: English

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

To provide feedback or report a problem with this document, go to www.nortel.com/documentfeedback.

www.nortel.com