BusinessPhone Operator Suite 5.0

Technical Guide





BusinessPhone Operator Suite 5.0 Technical Guide

EN/LZTBS 102 205/TG R3A

Copyright © 2003. Ericsson Enterprise AB. All rights reserved.

This document contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, or translated into another language, without prior written consent of Ericsson Enterprise AB, Stockholm, Sweden.

Windows is a trademark of Microsoft Corporation.

NOTICE

The information in this document is subject to change without notice.

ERICSSON MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Ericsson shall not be liable for errors contained herein nor for incidental or consequential damages in connection with the furnishing, performance or use of this material.

Ericsson Enterprise AB S-131 89 Stockholm, Sweden

Table of Contents

TABLE OF CONTENTS	3
KEY INFORMATION	
Dynamic Network Administration	13
Compatibility	14
D.N.A. Interworking	14
D.N.A. Server	15
What You Will Find In This Help Guide	15
Related Publications	
Using Help	
Printing Help.	
Glossary	
Now Eastures	10
APPLICATIONS	
Description of Applications	20
Limitations	20
BusinessPhone OWS and DMG:	21
Microsoft Data Engine (MSDE)	21
D.N.A. Directory Browser - Technical Aspects	22
OneBox Mailbox Integration	22
Integration of OneBox and D.N.A.	
OneBox Controls	23
Automatic Mailbox Creation/Deletion	
OneBox Database Synchronization	
OneBox Compatibility with Other Network Elements	24 24
Using Diversion Reasons	24 25
OneBox Intercept Capabilities	
Compatibility with Other Network Elements	26
BusinessLink	26
Server	26
Client	26
CCS / D.N.A. Application Suite Integration	27
CCA / D.N.A. Application Suite Integration	

Solidus eCare / D.N.A. Integration	
LDAP support in D.N.A	
Other Interfaces	
Directory Link	
D.N.A. CAAPI	
Change Log D.N.A. CTI	
Mobile Executive	
WAP Gateway	
Phone Setup	
R320s Phone setup for D.N.A. WAP	
Directory Browser	
SNMP Agent	
The Monitored Objects	
as_dmi.exe	
asami.exe	
NT SNMP	
Dmi2snmp	
Remote Data Monitor	
Visitor Registration	
RichWin	
EINSTALLATION	41
About Pre-Installation	
Pre-Installation Meeting	43
Addressing Important Issues	
Pre-installation Checklist	
PBX Hardware / Software Requirements	
PBX Software Requirements	
PBX Internal Settings	
PBX Command Settings	
Configuration Options	
PC Hardware Requirements	
Server	
Specific Requirements	
Client PC	
Additional Hardware Options	
	-

	1 D.N.A. Server:	45
	2 D.N.A. Clients:	
	3 Internet Tools:	40 46
	5 BusinessPhone	
	6 Simplified Chinese language support	
	SQL Server	47
	Internet Tools	47
Su	upported D.N.A. Server / Client Configurations	47
На	ard Disk Requirements	48
	Recommendation	48
Se	erver Disk Space Requirements	48
	Notes	
	D.N.A. Server	
	SQL Server Data Volume Estimates	
Cli	ient Disk Space Requirements	50
So	oftware Licensing	50
На	ardware Connections	51
	Connection Between Server PC and Client PC	51
	Connection Between PABX and BusinessPhone Operator Suite	51
WINDC	OWS AND SQL INSTALLATION	
ΝТ	C 4 0 Server	51
NT	Γ 4.0 Server	51
NT NT	Γ 4.0 Server Γ 4.0 Workstation	51
NT NT	Γ 4.0 Server Γ 4.0 Workstation Check Hardware before You Start Installing Windows NT from a Logal CD DOM Drive	51
NT NT	Γ 4.0 Server Γ 4.0 Workstation Check Hardware before You Start Installing Windows NT from a Local CD-ROM Drive Installing Windows NT from a Network Drive	51 54
NT NT	Γ 4.0 Server Γ 4.0 Workstation Check Hardware before You Start Installing Windows NT from a Local CD-ROM Drive Installing Windows NT from a Network Drive Date and Time Properties	51
NT NT	Γ 4.0 Server Γ 4.0 Workstation Check Hardware before You Start Installing Windows NT from a Local CD-ROM Drive Installing Windows NT from a Network Drive Date and Time Properties Display Properties	51 54
NT NT	Γ 4.0 Server Γ 4.0 Workstation Check Hardware before You Start Installing Windows NT from a Local CD-ROM Drive Installing Windows NT from a Network Drive Date and Time Properties Display Properties Copying Files and Restarting	
NT NT	T 4.0 Server T 4.0 Workstation Check Hardware before You Start Installing Windows NT from a Local CD-ROM Drive Installing Windows NT from a Network Drive Date and Time Properties Display Properties Copying Files and Restarting Regional Settings Properties	51
NT NT	T 4.0 Server T 4.0 Workstation Check Hardware before You Start Installing Windows NT from a Local CD-ROM Drive Installing Windows NT from a Network Drive Date and Time Properties Display Properties Copying Files and Restarting. Regional Settings Properties System Performance Settings	51 54 54 54 54 55 55 55 56 56 56 56 56
NT NT	T 4.0 Server T 4.0 Workstation Check Hardware before You Start Installing Windows NT from a Local CD-ROM Drive Installing Windows NT from a Network Drive Date and Time Properties Display Properties Copying Files and Restarting Regional Settings Properties System Performance Settings System Startup/Shutdown Settings	51 54 54 54 54 54 54 55 55 55 56 56 56 56 56 56
NT	T 4.0 Server T 4.0 Workstation Check Hardware before You Start Installing Windows NT from a Local CD-ROM Drive Installing Windows NT from a Network Drive Date and Time Properties Display Properties Copying Files and Restarting Regional Settings Properties System Performance Settings System Startup/Shutdown Settings Install NT Service Packs	51
NT NT	T 4.0 Server T 4.0 Workstation Check Hardware before You Start Installing Windows NT from a Local CD-ROM Drive Installing Windows NT from a Network Drive Date and Time Properties Display Properties Copying Files and Restarting Regional Settings Properties System Performance Settings System Startup/Shutdown Settings Install NT Service Packs Install Microsoft Excel Report and Verify Setur Success	51 54 54 54 55 55 56 56 56 56 56 56 56 56 56 56 56 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57
NT	T 4.0 Server T 4.0 Workstation Check Hardware before You Start Installing Windows NT from a Local CD-ROM Drive Installing Windows NT from a Network Drive Date and Time Properties Display Properties Copying Files and Restarting Regional Settings Properties System Performance Settings System Startup/Shutdown Settings Install NT Service Packs Install Microsoft Excel Reboot and Verify Setup Success	51
NT NT	T 4.0 Server T 4.0 Workstation Check Hardware before You Start Installing Windows NT from a Local CD-ROM Drive Installing Windows NT from a Network Drive Date and Time Properties Display Properties Copying Files and Restarting Regional Settings Properties System Performance Settings System Startup/Shutdown Settings Install NT Service Packs Install Microsoft Excel Reboot and Verify Setup Success Install Microsoft Excel Reboot and Verify Setup Success	51 54 54 55 55 55 56 56 56 56 56 56 56 56 56 56 56 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57
NT NT	T 4.0 Server T 4.0 Workstation Check Hardware before You Start Installing Windows NT from a Local CD-ROM Drive Installing Windows NT from a Network Drive Date and Time Properties Display Properties Copying Files and Restarting Regional Settings Properties System Performance Settings System Startup/Shutdown Settings Install NT Service Packs Install Microsoft Excel Reboot and Verify Setup Success indows 2000 Upgrade Installing Windows 2000 from a Local CD-ROM Drive Installing Windows 2000 from a Network Drive	51 54 54 54 54 55 55 56 56 56 56 56 56 56 56 56 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57
NT NT Wi	T 4.0 Server T 4.0 Workstation Check Hardware before You Start Installing Windows NT from a Local CD-ROM Drive Installing Windows NT from a Network Drive Date and Time Properties Display Properties Copying Files and Restarting Regional Settings Properties System Performance Settings System Startup/Shutdown Settings Install NT Service Packs Install Microsoft Excel Reboot and Verify Setup Success indows 2000 Upgrade Installing Windows 2000 from a Local CD-ROM Drive Installing Windows 2000 from a Network Drive SQL Server 7.0	51 54 54 54 55 55 56 56 56 56 56 56 56 56 56 56 56 56 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57
NT NT Wi	T 4.0 Server F 4.0 Workstation Check Hardware before You Start Installing Windows NT from a Local CD-ROM Drive Installing Windows NT from a Network Drive Date and Time Properties Display Properties Copying Files and Restarting. Regional Settings Properties System Performance Settings System Startup/Shutdown Settings Install Microsoft Excel Reboot and Verify Setup Success Installing Windows 2000 from a Local CD-ROM Drive Installing Windows 2000 from a Network Drive	51 54 54 54 55 55 56 56 56 56 56 56 56 56 56 56 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57
NT NT Wi SC	T 4.0 Server T 4.0 Workstation Check Hardware before You Start Installing Windows NT from a Local CD-ROM Drive Installing Windows NT from a Network Drive Date and Time Properties. Display Properties Copying Files and Restarting Regional Settings Properties System Performance Settings System Startup/Shutdown Settings Install NT Service Packs. Install Microsoft Excel Reboot and Verify Setup Success indows 2000 Upgrade Installing Windows 2000 from a Local CD-ROM Drive Installing Windows 2000 from a Network Drive Security Memory	51 54 54 54 55 55 56 56 56 56 56 56 56 56 56 56 56 56 56 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 57 58 58 58
NT NT Wi SC	F 4.0 Server Check Hardware before You Start Installing Windows NT from a Local CD-ROM Drive Installing Windows NT from a Network Drive Date and Time Properties Display Properties Copying Files and Restarting Regional Settings Properties System Performance Settings System Startup/Shutdown Settings Install Microsoft Excel Reboot and Verify Setup Success indows 2000 Upgrade Installing Windows 2000 from a Local CD-ROM Drive Installing Windows 2000 from a Network Drive QL Server 7.0 Security Memory	51 54 54 54 55 55 55 56 56 56 56 56 56 56

New Installation	60
Unattended SQL Server Installation	61
SNMP Master Agent	63
Windows NT	63
Windows 2000	
D.N.A. INSTALLATION	65
About Installation	65
Hardware Connections	
Software Installation	65
Installation Checklists	65
Using the Checklists	65
For More Information	65
Submit Your Comments	65
Pre-installation Checklist	65
Installation Profile	
Installation Component Verification	
Installation Product Identification	
Application Suite Installation	67
Installation Features	
Pre-Configured System	
> See also Configuration BusinessPhone File Parameters below	
DSEI Names and Phyleges	
GICI Configurations	88
Data Synchronization	
User-defined Fields for Directory Manager	68
Configuration BusinessPhone File Parameters	
Upgrading To Operator Suite 5.0	70
Server Installation	
Auto-Run Installation	
Taskbar Installation	
New Server Installation	72
Server Installation Wizard	73
Installation Options	75
Add Components	
Resize Database	
Client Installation	
Auto-Run Installation	76
Taskbar Installation	77
New Client Installation	
Client Installation Wizard	
Client Installation Options	
Silent Installation	79
Modifying the Setup (dnasuite.ini) File	79
Installation Procedure	80

	Using the Setup Command	80
Мо	bile Executive	81
	Installing with Auto-Run	81
	Installation Options	82
	Post Installation Setup	82
	Windows NT	82
	Windows 2000	82
Dire	ectory Browser - Installation and Configuration of Directory Browser	83
Out	look Integration	86
Lot	us Notes Integration	88
	COMPUTER or USER ID User Defined Fields	
	Lotus Notes Integration Templates	89
	User Help	89
SETTIN	GS AND CONFIGURATIN AFTER INSTALLATION	89
Dire	actory Setup for Network Installations	
Bac	sic Configuration for the Server	90
Dat		
	Administrative I ools	
	D.N.A Server Configuration	92 02
	Directory Configuration	92 02
		92
Set	tings for Operator Workstation	93
	Busy Lamp Field	93
	Feature Settings	93
	Night Switching	
	Number	
	Malicious	
	URL	
	Common Queue Number (Operator)	
	NT Netopod Procedure	
	NT Notepau Procedure	94 04
•		
Set	tings for the Directory Manager	94
PERFO	RMANCE	
Per	formance Enhancements	95
RD	S Performance	95
	LDB Integrity Check Feature (RDS 2.x)	
	Reduce I/O Completion Ports in Large Systems (RDS2.1)	
	Enable/Disable Incremental LDB Updates from DMG	96
	Configure RDS to Use Fewer SQL Connections	96
INSTAL	LATION PROBLEMS	
1.0	Files	~7
LOG	ן רוופס	

Technical Guide

	Server Installation Logs Client Installation Logs	97 97
Εv	/ent Log Messages	97
D.N.A.	SERVER	105
Fa	cilities and Services	105
Ac	dministrative Tools	106
Cł	nanging Users, Servers, and Passwords	108
Re	egistry	109
	Registry Settings	109
	Operator Workstation Registry Settings	109
	Server Identification	109
	LDS Servers	109
Ма	aintenance	110
	SQL Database	110
	Database Upsizing	110
	Tasks	110
	I ransaction Log	
	Ine CleanDB Routine	110
	Ovwin log File	110
Sr	nort Message Service	111
	Limitations	111
Lo	ocal Database Compression	111
MAINT		112
Ar	chival Backup	112
	Temporary Workspace	112
Da	atabase Utility	112
	Options	113
	Capacity and Limitations	113
TROU	BLESHOOTING	113
Те	echnical Support	113
	Before Contacting Technical Support	114
Re	eporting Your Problem	114
	Problem Description	114
	PBX	114
	Operating System Information (mark all that apply)	115
	Network Protocol (mark all that apply)	115
	PC	
	D.N.A. Applications	115

Event Viewer	115
Error Messages	
Error Messages for SNMP Agent	118
Directory Manager	121
Operator Workstation	123
Mobile Executive	124
Outlook Integration	125
Corrected Features	125
APPLICATION DATA	126
Report Generation	126
Directory Manager Database Organization	127
Extension Manager Database Organization	133
Operator Workstation Data	146
Directory Assistance Databases	146
Operator Workstation Configuration	
How Settings Files are Created	146
Permissions for Changing User and Directory Settings	146
Where to Find Settings Files	146
Operator Console Settings	146
DIRECTORY STRUCTURES	
D.N.A. Directory Structures	147
Directory Manager (Server)	147
Administrative Tools (Server)	148
Operator Workstation (Server)	150
Directory Manager (Client)	150
Administrative Tools (Client)	151
Operator Workstation (Client)	151
FREQUENTLY ASKED QUESTIONS	152
Directory Manager	152
D.N.A. Server	
Operator Workstation	152
Operator Workstation	
Operator workstation LAN	
Remote Data Server	156

Serial Communications Server	157
D.N.A. Application Suite	157
Registry	158
SQL Server	158
ClockSync	159
SNMP	159
CONFIGURATION	159
Customers	159
Service Provider Customer Groups	
Configuring Type I Customers	
Configuring Type II Customers	160
D.N.A. Server	160
Serial Communication Server	162
Web Site Security	162
Windows NT	162
Windows 2000	
NCOP-OWS	
Definitions	
Service Provider Customer Groups	
Configuring Type I customers	
Configuring Type II customers	
Configuring the NCOD OWS	1/4
Configuring the SCS	177
Performance	
	179
E-mail Integration	179
Operator Workstation E-mail Requirements	179
Loading the MAPI library	179
Performing a Null Logon	180
VSI AND TSS	180
Voice System Interface	180
Setting Un Communications and Configuration Parameters	180
The VSI Protocol	180
Capacities and Limitations	
Time System Interface	182
Interface	182
Logical Interface	182
Protocols	182
Finnish Character Coding	182
Message Format	
FLEXIM Protocol	
Messages sent from FLEXIM to D.N.A. Time System Interface	

Messages sent from D.N.A. Time System Interface to FLEXIM	.187
L ogin/logout message	189
Messages sent from General Time Monitoring System to Time System Interface	.190
CTR Protocol	.191
Messages sent from the CTR Time Monitoring System to D.N.A.	.192
Messages sent from Time System Interface to CTR Time Monitoring System	.193
ESMI Protocol	.194
Messages sent from ESMI Time System To D.N.A. Time System Interface	.194
Messages sent from D.N.A. Time System Interface to ESMI Time System	.195
TIMECON Protocol	.196
Stamping Message	.196
Return Time	.196
Clock Message	196
Exchange Interface	197
	.197
N/P/Voice System to VSI Messages	107
	. 197
IVR/Voice System from VSI Messages	.199
TIME SYSTEM INTERFACE	201
Compatibility with Other Network Elements	.201
BUSINESSPHONE .CFG EXAMPLE	202
InfoFile Procedure	.205
STAND-ALONE INSTALLATION - SINGLE NODE	206
NETWORK INSTALLATION - SINGLE NODE	206
NETWORK INSTALLATION - SINLGE NODE / SERVER AND CLIENT COMBINED	206
NETWORK INSTALLATION SINGLE NODE / TELEPHONY SERVER	208
NETWORK INSTALLATION - MULTI NODE / CORPORATE NETWORK	209
Obtaining on E mail Address	
Obtaining an E-mail Address	
E-mail Related D.N.A. System Administration	
Directory Configuration	
RDS Configuration	
System Maintenance	
Troubleshooting	
Troubleshooting Operator Workstation E-mail with Performance Monitor 211	
Troubleshooting Operator Workstation E-mail with Remote Data Monitor 212	
REMOTE DATA SERVER	213
SECURITY DATA SERVER	213
	•
SYSTEM CLOCK SYNCHRONIZATION	213

TO GENERATE REPORTS USING ACCESS	
TO LOG OFF	213
TO LOGON	

Key Information

Dynamic Network Administration

The new operator solution for BusinessPhone (BusinessPhone Operator Suite) is based on MD110 Operator Workstation which is part of the D.N.A. (Dynamic Network Administration) concept. BusinessPhone Operator Workstation has been adapted to work as CTI-client towards BusinessPhone and enhanced by some special features for BusinessPhone segment.

The BusinessPhone Operator Suite software products are a comprehensive set of graphical PC-based tools that support all aspects of BusinessPhone Operator functions, including:

- Operator call management
- Directory management
- High-level telecommunications networking
- Server based directory, advanced directory functionality
- Advanced message handling (E-mail)
- Free seating
- Enhanced information messaging (BusinessPhone information system)
- Customisable user environment
- Busy Lamp Field
- Interaction with other BusinessPhone 3rd party CTI applications (e.g. BusinessPhone Call Centre Assistant)

BusinessPhone Operator Suite is developed to run under the Microsoft Windows NT Server/2000 Server (the client and the stand alone installation can be installed also on NT4 professional/ Win 2000 professional and XP Professional) operating system and to work towards the PBX via the BusinessPhone BusinessLink (3rd party CTI: TSAPI Link for Windows).

The complete BusinessPhone solution consists of following parts, bundled to one special BusinessPhone package:

BusinessPhone Operator Workstation (OWS)

Operator Workstation (OWS) is a BusinessPhone Operator Suite administrative tool for operator call management of BusinessPhone 250 and BusinessPhone 50 PBX telephone traffic.

The Operator Workstation application introduces efficient graphical point-and-click controls and fully integrated on-screen Directory Assistance. These basic functions are complemented by a powerful Busy Lamp Field that provides an instant overview and associated operator functions for any any individual part of the exchange managed by individual operators.

• Directory Manager (DMG) for BusinessPhone

Directory Manager (DMG) provides a graphical user interface plus tools for the administration of the directory database. It is a prerequisite application for OWS and can be run on the same PC as OWS

if required.

D.N.A Server

The Management Repository Server (MRS) module is the heart of the whole solution. It serves as common data storage medium and communications interface for Operator Workstation and Directory Manager.

Compatibility

This release of the D.N.A. Application Suite is compatible with:

- Microsoft Windows NT Workstation Version 4.0, Windows 2000 Professional and Windows XP Professional (stand alone and Client)
- Microsoft Windows NT Workstation Version 4.0 and Windows 2000 Professional
- Ericsson BusinessPhone Communication System
- Microsoft SQL Server 2000
- Microsoft SQL Server 2000 Desktop Engine
- Microsoft SQL Server 7.0
- Microsoft MSDE
- Microsoft Internet Information Server 4.0 and 5.0
- Microsoft Excel 97 or Excel 2000 or Excel XP
- BusinessPhone BusinessLink
- Microsoft Internet Explorer 4.x or higher

D.N.A. Interworking

D.N.A. is compatible with a broad family of Ericsson Computer Telephony Integration network and telephony products. This section explains the interworking of different CTI products with a focus on the D.N.A. Application Suite. The interworking products are:

- D.N.A. Application Suite
- CCS
- CCA
- BackStage
- LDAP Data Sources*
- Solidus eCare*
- OneBox 1.1 and newer*
- Time Systems*

* not used for BusinessPhone

The relevant network elements are

• MD110

• Business Phone

The following matrix shows current interworking between different network elements and the CTI applications:

	One Box	D.N.A. Server /DMG/OWS	App Link	BusinessLink	CCA	CCS	Solidus eCare
MD110	+	+	+	-	+	+	+
Business Phone	+	+	+*1	+	+	+	-

- + = full interworking
- * = restricted interworking
- = no interworking

D.N.A. Server

The D.N.A. Server lets you administrate the D.N.A. Application Suite users. It also contains different utilities to set up the connection with BPX Nodes. The central component of a D.N.A. Installation is the Remote Data Server (RDS). RDS maintains network database synchronization between all PBX nodes, the D.N.A. SQL Server, and D.N.A. Local Databases. Some of the most important database support functions are:

- Message Diversion Synchronization with the PBX.
- Message Waiting Synchronization that updates the Voice System Interface configuration utility.
- Application-to-Application Interactive Updates.
- Security and Licensing Support.
- D.N.A. Distributed Database Synchronization.
- Photo Storage and Retrieval for Operator Workstation and Directory Manager.
- Configuration File Storage and Retrieval for Operator Workstation and OCX.
- Administrative Task Scheduling.
- A tool to set up the Voice System Interface.
- A tool to specify the replication between multiple D.N.A. Servers.

What You Will Find In This Help Guide

This guide is written for technicians responsible for installing and maintaining Ericsson's Dynamic Network Administration (D.N.A.) applications. The D.N.A. Application Suite is a family of PC-based telephony applications for management and control of BusinessPhone PBX operations. This guide includes the following help books.

Applications - Provides a basic description of the applications.

Pre Installation - Describes the main types of installations, PC hardware requirements, software which must be installed on the PC, and requirements for the PBX.

Installation - Describes first-time installation of the D.N.A. applications, including hardware connections between the PBX and PC, and installation of the application software on the PC.

D.N.A. Server - The security and support platform for the Dynamic Network Administration (D.N.A.) applications.

Maintenance - Describes tasks that should be performed periodically to ensure proper operation of your applications.

Troubleshooting - Describes how to resolve problems that may occur.

Application Data - Report generation, data organization, and populating directory assistance databases.

Disk Space - Helps you determine how much hard disk space is needed on PCs used for D.N.A. applications.

Technical Support - Hardware specifications and problem reporting.

PBX Configuration - Tables of commands.

Installation Checklist - Checklists for D.N.A. server and client workstation installation.

Related Publications

In addition to the "Technical Guide", getting started guides are available for the following products.

- Operator Workstation
- Directory Manager
- Mobile Executive

Conventions Used in This Guide

The D.N.A. server PC may be part of a larger network that uses another computer as a server for that network. Throughout this help guide, however, "server" refers to the PC set up as the server for the D.N.A. application suite, and "network" refers to the Windows NT LAN that is hosting the D.N.A. server PC.

Using Help

Click the **Contents** tab to scroll through a table of contents for the Help file. Click the **Index** tab to search for topics by using an index of Help subjects. Click the **Search** tab to use a full-text search for specific words or phrases.

Tips for using Help

When viewing Help, you can maximize the window or resize it if you want. Click **Help Topics** to show or hide the Navigation Pane. Click **Print** to print the current topic. Click **>>** to go to the next topic in the browse sequence. Click **<<** to go to the previous topic in the browse sequence. The **Options** menu provides additional display controls.

Printing Help

Click the **Print** button to print the current topic. To print the entire help file you need to have Microsoft Word or Word Viewer installed on the PC. Word Viewer is a free download from Microsoft's web site.

To print the entire help file

- 1 Right-click on the *TechGuideHelp.doc* file in the *MRS\HELP* directory under *DNA_C* or *DNA_S*.
- 2 Click **Print** on the pop-up menu.

Glossary

Refer to the descriptions in this section for help with understanding terms used in this guide.

Backup Domain Controller (BDC) - A Windows NT/2000 configuration option.

Call Origin Group - A group number defined for an operator that serves a unique call type, such as internal calls, public trunk calls, tie lines, and DID lines. An operator can be assigned to several different call origin groups.

Client - A PC in a network installation that is connected to a server PC and accesses data on the server when running applications. In a D.N.A. network installation, the SQL database and the **D.N.A. Server** reside on a server PC, and one or more client PCs run applications that access the data on the server. For a stand-alone installation, the server and the client are the same PC.

COM Port - An RS-232C serial communication interface on a PC that allows direct connection to another PC or an BusinessPhone CPU-D with a cable or indirect connection using a modem, or via Networkcard from PC to the BusinessPhone IPU with Vcom (Virtual com).

Computer Supported Telephony Application (CSTA) - Supports Computer Telephony Integration (CTI) between the Distributed Network Architecture (D.N.A.) environment and the BusinessPhone PBX.

Directory Manager (DMG) - A D.N.A. application that allows administrative personnel to manage subscriber directory entries. Includes capabilities for adding, modifying, and deleting subscriber directory records.

D.N.A. Applications - The set of software applications that run on PC clients and are used in combination with one or more BusinessPhone' to manage telecommunications operations.

D.N.A. Server - D.N.A. platform services and utilities that reside on the server and act as the intermediary between all D.N.A. applications and databases.

Extension Manager (EMG) - A D.N.A. application for managing MD110 telephone data and extensions. Includes capabilities for administration of telephone and data extensions, messaging, and other PBX elements.

General Information Communications Interface (GICI) - The logical interface for the ICU or NIU board in the MD110. Note: GICI is not used for the BusinessPhone. BusinessPhone uses BusinessLink instead of GICI.

Graphical User Interface (GUI) - The user interface presented by D.N.A. applications and management utilities.

Hardware Compatibility List (HCL) - A list of hardware tested and verified to work with Windows operating system. The list is available at .

IPU - BusinessPhone IP Telephony solutions are based on the IP Unit (IPU), which is a plug-in board that makes Voice-over- IP (VoIP) an affordable, integrated and – above all – useful tool for small to medium sized enterprises. It enables existing BusinessPhone systems to offer IP-based, as well as traditional telephony.

Integrated Digital Network Exchange (IDNX) - For ISDN networks, the IDNX uses routing access information to enhance PBX performance. This unit helps achieve efficient bandwidth utilization, high network reliability and availability, and control over the usage of network resources.

Integrated Services Digital Network (ISDN) - ISDN uses a 64 kbit/s channel for transmitting digitally coded speech and data. This digital medium is normally used for circuit-switched connections, packet-switched connections, and semi-permanent connections. The complete digital interface (2B+D) consists of two B-channels for speech/data and one D-channel for signaling.

Lightweight Directory Access Protocol Service (LDAP) - Directory lookup and modification services for LDAP clients accessing Directory Manager databases.

Local Area Network (LAN) - A computer network based on one or more centralized server PCs and one or more locally or remotely connected client PCs.

BusinessPhone Communication System – The Ericsson PBX for small to medium sized companies.

NT/2000 File System (NTFS) - The Windows NT/2000 file system.

Operator Workstation (OWS) - A D.N.A. application that enables operators to manage PBX telephone traffic through subscriber databases.

Performance Data Manager (PDM) - See Performance Manager.

Performance Manager (PMG) - not available in the BusinessPhone package.

Primary Domain Controller (PDC) - A Windows NT/2000 configuration option.

Private Branch Exchange (PBX) - Telephone switching system that supports a private community of subscribers, typically a business environment. Usually managed from a central operator console, PABXs interconnect internal subscribers to one another, and to other subscribers in the public network. Also known as *Private Business Exchange* and Private *Automated Business Exchange (PABX)*.

Remote Data Server (RDS) - D.N.A. Server Utility that allows you to configure the Remote Data Server for D.N.A. database and application support roles, including network database synchronization between PBX nodes, the D.N.A. SQL Server, and D.N.A. Local Databases (LDBs).

Serial Communications Server (SCS) - D.N.A. Server Utility that allows you to manage direct, Telnet, SCS, and third party serial communications port settings.

Server - The central PC for a D.N.A. network installation. In a network installation, the SQL database and the **D.N.A. Server** software reside on a server. One or more client PCs may run D.N.A. applications that access the data on the server. The server acts as a database "referee," providing data security, centralized file access, management services, and controlling ID master files and external subscriber directories. For a stand-alone installation, the server and the client is the same physical PC.

Stand-alone - An installation of D.N.A. applications on a single PC instead of a network of PCs. In a network installation, the SQL database and the **D.N.A. Server** reside on a server PC, and one or more client PCs run D.N.A. applications that access the data on the server. In a stand-alone installation, all of these elements (SQL database, **D.N.A. Server**, and D.N.A. applications) are installed on a single PC.

Time System Server (TSS) Configuration - An optional D.N.A. module that allows connection to an external time monitoring system. Through this interface, diversions can be entered in the time monitoring

system and registered in the D.N.A. directory database. TSI also allows control signals for message waiting indications to be sent from D.N.A. to the time monitoring system.

Trunk Manager (TRM) - Enables you to assign easily recognizable names to incoming trunks for efficient operator identification and routing.

Voice Server Unit (VSU) - Line Interface Module (LIM) hardware for storing voice messages.

Voice System Interface (VSI) - An optional D.N.A. module that allows voice mail integration. VSI acts as a compatibility interface between the PBX and Ericsson Voice Message Processing Systems. Capabilities include call diversion options, support for Message Waiting Indicators (MWI), and increased reliability of voice processing operations.

WAP – Wireless Application Protocol.

Wide Area Network (WAN) - Inter-office private communication network.

New Features

This new release concentrates on enhancing the integration with external applications as well as offering tools in line with the mobile Internet vision by adding amongst others the following functions:

- Support of Windows 2000
- Support of SQL 2000 and Desktop Engine 2000
- Improved search options and directory features
- Instant recognition of key customers via CLIP information
- Support of Lotus Notes Integration
- New application module: D.N.A. Mobile Executive The D.N.A. Mobile Executive enables the user to access some of the D.N.A. Application Suite features via WAP enabled devices.
- Support of LDAP version 3 (read/write)
- Redial function key
- Audible signal for calls being too long on hold

Applications

Description of Applications

The D.N.A. application suite is an integrated set of applications that allow you to operate and manage your PBX communication resources from stand-alone or networked PCs. The application suite includes the following applications.

D.N.A. Server	The operational and administrative platform for the D.N.A. utilities and data structures. Includes system configuration and maintenance utilities for supporting D.N.A. applications.
Directory Manager (DMG)	OWS support and administrative application that enables you to add, modify, and delete D.N.A. Directory entries.
Operator Workstation (OWS)	D.N.A. traffic management application. Allows operators to access D.N.A. Directory subscriber information and route telephone traffic.
D.N.A. Mobile Executive (DME)	A WAP application allowing users to access the D.N.A. directory, Message Diversion and Personal Number functions via a WAP enabled device like a cellular phone.

Limitations

The following limitations apply to BusinessPhone Operator Suite applications:

A maximum of three (3) operators supported at the same time. Due to free seating functionality more than three Operator Workstation application can be installed but only three can be active at the same time. Please consider that an operator telephone (e.g. Dialog 4224) also counts as an active operator even if the operator telephone is off-duty.

You can avoid this limitation if you use different types of telephone sets (e.g. Dialog 4223,) instead of a real oper ator telephone.

Following Digital Telephones cannot be used as a CTI operator instrument:

- (1) Analogue telephones
- (2) R-key instruments (e.g. POTS, Freeset)
- (3) Dialog 3210, Dialog 4220, (Basic Telephone)
- (4) IP Phone

To prevent misuse of the powerful operator abilities it is only possible to use dedicated (prede fined) extensions that are enabled within the system for the usage as operator instrument together with OWS.

The connection between D.N.A. Server and BusinessPhone PBX is exclusively established with BusinessPhone BusinessLink.

BusinessPhone Operator Suite applications can only be used in conjunction with Ericsson's BusinessPhone Communication System. The BusinessPhone Operator Suite, however, can interwork with Ericsson's MD110 switch in respect of sharing database contents, and advanced call management.

BusinessPhone OWS and DMG:

BusinessPhone Operator Workstation 5.0 and Directory Manager 5.0 are only compatible with DNA Server database version 5.0; i.e. a customer must upgrade all applications to get access to the improved functionality in the latest releases.

Although there is no limit in how many people can be entered into the database, as long as there is enough disk space, the external directory specification limit is 500. This means that 500 entries is the limit of what will be displayed in the list box; e.g. if there are 4.000 entries starting with letter 'A', 500 records will be pulled out of the database when the 'A' is entered to do a search. When the user progressively enter additional search criteria the right person will be pos sible to allocate.

The directory structure is designed to handle up to 40 user definable fields: 36 public and four confidential data fields for "Person" type subscriber. For "Room" and "Function" type subscrib ers, the limit is four public fields. Every subscriber can have an unlimited number of keywords.

The limitation on the number of Operator Workstations is a BusinessPhone Communication System limitation on any operator instrument: A maximum of 3 operator positions per system.

The Directory Manager has been tested with 250.000 entries.

When an operator searches against a given foreign LDAP server, it might not be possible to automatically dial any of the search results since the numbers might not be entered correctly.

Microsoft Data Engine (MSDE)

The maximum size of MSDE is 2 GB. This limit is per database not per server. A single MSDE can therefore support multiple MDSE databases, each containing up to the 2 GB limit. (If the required data space is expected to grow beyond 2 GB, then upgrading to SQL 7.0 will remove this limit).

D.N.A. Directory Browser - Technical Aspects

DNA Directory Browser is typically installed on a company's Web-Server. The Server component needs to communicate with the DNA server in order to fetch directory information. The DNA/WWW integration is provided by a search component using RDS as a protocol to query the Directory and to receive the result set. The DNA Directory database is replicated and stored locally on the WWW machine by the search component.

DNA Directory Browser does not put more strain on the D.N.A server than one single user since it copies the DNA data locally to the WWW server. DNA sees the Directory Browser as a single client regardless of the fact that several people simultaneously access the directory data. All changes in the DNA Directory Database will be propagated immediately to the Directory Browser WWW component.

The bandwidth allocation for queries to the Directory Browser is handled by basic WWW server administration tasks:

1) Deciding how many simultaneous connections are allowed.

2) Limiting the bandwidth usage by the WWW server.

In summary, the customer can control and manage easily the level of service provided by this application and it's impact on the network.

OneBox Mailbox Integration

Note: This functionality is a MD110 specific feature and is not fully verified with BusinessPhone Communication System.

D.N.A. systems with a OneBox mailbox can access voice mail, e-mail, or fax mail messages from a unified interface such as Microsoft Outlook or their telephone.

Integration of OneBox and D.N.A.

You may create, modify or delete OneBox mailboxes from the D.N.A. Directory Manager and Extension Manager applications. During D.N.A. setup, the system administrator can assign one or more OneBox servers to a PBX node via the RDS Setup. Supported attributes include a OneBox Server name or IP address, password, and extension ranges.

Technical Guide

OneBox Servers Settings		×
		exe ĉė
C3 BC11 C7 BC11 I 195.100.101.91 Non-MD110 Site I 195.100.101.91 E test3	From Extension 00000	To Extension 99999
		Close Help

OneBox Server Settings
Server
Name: 195.100.101.200
Mailbox ID: 29999
Password [,]
Confirm Password:
Extension Range
From: To:
Range:
From To -
00000 99999
OK Cancel Help

OneBox Controls

OneBox mailbox integration allows you to configure the following basic mailbox attributes.

• Extension Callout Capabilities

- Local or Long Distance
- Enabling/Disabling of Message Waiting Indicators
- Message Retention Duration
- Message Clearing Options
- Set-up of Tutorial Prompts

Desktop Options on OneBox Message Manager

Automatic Mailbox Creation/Deletion

OneBox mailboxes are automatically created or deleted when assigned subscribers are created or deleted in the D.N.A. Directory Manager.

OneBox Database Synchronization

There is no synchronization between the OneBox Directory and the D.N.A. Directory Manager Database. There is only one-way communication, from Directory Manager towards OneBox. If a mailbox is created with the OneBox System Administration, Directory Manager is not informed. Communication between OneBox and the D.N.A. Server is conducted via Local Area Network (LAN).



OneBox Compatibility with Other Network Elements

This integration is available for D.N.A. Directory Manager and Extension Manage. It is not compatible with D.N.A Application Suite for Mobility Server or the Application Suite for Business Phone.

OneBox Integration with D.N.A. Voice System Interface

Subscribers have six possible options for initiating message diversions. Any diversion reason that is entered is stored on the D.N.A. Application Suite Server. These options are:

- Entering a diversion code on the numeric keypad. E.g., * 23 * 4 *1300 # for "Lunch until 1300"
- From the Ericsson Communication Assistant web inteface
- D.N.A. users can initiate a diversion from Microsoft Outlook
- D.N.A. users can initiate a diversion from Lotus Notes

• Through the Telephone User Interface (TUI) of OneBox

An Operator using D.N.A. Operator Workstation can initiate a diversion for any subscriber.

Using Diversion Reasons

OneBox can query diversion reasons from the D.N.A. Server. OneBox can use this information to play an appropriate voice prompt to a caller matching the diversion reason, e.g., "Gina is out for lunch and will be back at 13:00. Please leave a message after the tone, or dial zero for operator."



Note Communication between OneBox and the D.N.A. Server requires a serial link.

OneBox Intercept Capabilities

Integration with D.N.A. provides OneBox with the ability to:

- Accept Intercept Call Diversion requests entered by a subscriber
- Store the diversion information
- Provide audio intercept messages to callers trying to reach the mailbox subscriber
- Support various "next action" options presented to the caller

Audio intercept messages can present callers a selected set of "next action" options, including:

- Leaving a message
- Transfer to operator or personal assistant
- Hang-up
- Transfer to another number

Technical Guide

Hear choices in another language

Messages left in mailboxes are available to mailbox users through normal Voice Mail services.

When a caller chooses the "transfer to operator" option, and the call is forwarded from OneBox to the PABX Operator, the original called extension is displayed for the operator. The operator can also retrieve the diversion reason from the D.N.A. Database.

The OneBox Telephone User Interface (TUI) is the only means of initiating message diversions from a remote location, without having access to a PC. This integration is available for D.N.A. Directory Manager.

Compatibility with Other Network Elements

- MD110
- Business Phone

BusinessLink

PCs running BusinessPhone Operator Suite applications require BusinessPhone BusinessLink.

BusinessLink is the computer-telephony integration (CTI) link that connects Ericsson's BusinessPhone Communication System with applications running on computers and computer networks.

Server

BusinessLink provides connectivity between the BusinessPhone Communication System and a host computer. BusinessLink can be installed in a CSTA environment to be connected to host servers and applications which are written for CSTA APIs such as Novell TSAPI, Dialogic CTConnect, SUN XTL, etc. The CSTA interface is described in Standard ECMA-179 Services for Computer Supported Telecommunications Applications (CSTA) Phase I. BusinessLink is fully ECMA CSTA compliant.

Client

Each Client, running a BusinessPhone Operator Suite application must have installed a BusinessLink 32bit Client DLL.



CCS / D.N.A. Application Suite Integration

It is possible to share DNA subscriber data with the BusinessPhone Call Center Supervisor (CCS). For more details please refer to the corresponding CCS documentation.

CCA / D.N.A. Application Suite Integration

It is possible to share DNA subscriber data with the BusinessPhone Call Center Assistant (CCA). For more details please refer to the corresponding CCA documentation.

Solidus eCare / D.N.A. Integration

Note: Solidus eCare is not a part of the BusinessPhone portfolio and therefore not supported by the BusinessPhone Communication System.

Solidus eCare can use the D.N.A. Directory Manager database. If a specially named user defined field (UDF) is configured in Directory Manager, Solidus eCare can import either the whole DMG Database or only subscribers with a "YES" entry in this field. The integration must be initiated manually from the Solidus eCare server. Upon log-on of a Solidus eCare user, the Directory Manager database is updated with the actual extension number of the agent (through the D.N.A. Directory Link, <see The D.N.A. Directory Link>). As well, the Solidus eCare agent can receive a copy of the D.N.A. Directory Manager Database is stored locally on the Solidus eCare Agent PC.



LDAP support in D.N.A

The Lightweight Directory Access Protocol (LDAP) standard dictates how clients, applications, and servers access directory information. LDAP is a directory service protocol that runs over TCP/IP. The LDAP Directory service is based on the client-server model.



D.N.A. includes LDAP Server in the D.N.A. Server and an LDAP Client in the Operator Workstation. The OWS can search any LDAP Server for a subscriber and can use this information in the same manner as

information from the Directory Manager Database. On the other hand, any LDAP Client (i.e. an Internet Browser) is able to search the Directory Manager Database through the D.N.A. LDAP Server.

Other Interfaces

Directory Link

The Directory Link interface allows non-D.N.A. applications to modify D.N.A. Directory data. Directory Link can be thought of as a DMG client without a user interface. Directory Link accesses and modifies directory databases through the database API library, and communicates with other DMG and OWS clients through RDS.

Directory Link specifications are available for interested Ericsson Partners through the Ericsson Partner Program.

D.N.A. CAAPI

The D.N.A. Call Accounting Application Programming Interface (CAAPI) enables Third-party Call Accounting Applications to utilize Directory Manager data. Directory Manager generates a file containing an extract of the DMG data. Call accounting applications can now import these data on a scheduled basis from a single point-of-entry.

D.N.A. CAAPI is compatible with the following Network Elements

- MD110
- Business Phone

Change Log

The Directory Change Log allows directory data changes to be collected by external applications like Call Accounting Packages, desktop applications, or other Ericsson CTI applications. With previous D.N.A. releases it was necessary to re-import all data after adds/moves/changes. With D.N.A, only changed data is imported.

The Change Log is a client component of the Remote Data Server (RDS) that sequentially records all Directory Manager and Directory Link modifications made to the Directory Database.

D.N.A. CTI

This schematic summarizes most D.N.A. CTI Interworking capabilities and illustrates the central role of the D.N.A. Directory.



Mobile Executive

This section contains the administrator issues for the Mobile Executive.

WAP Gateway

If you use your mobile operator's WAP-service, you will probably have to open up your company's firewall to accept and route WAP-traffic to your Mobile Executive server. If you set up your own WAP-gateway and dial-in connection, you open a "hole" where a potential hacker could sneak in. Many companies will probably not allow this, so to strengthen security, the RAS-server could, for example, be put on a separate LAN segment that is separated from the real company-intranet with a firewall (this is just one way to increase security, there are more).

Phone Setup

Setting up a WAP phone is telephone-specific, however, the following information is required for all phones.

- A phone number (to the company's or your mobile operator's RAS-server).
- Username and password (to log on to the RAS-server).
- The address of the WAP-gateway (IP-address).

Username and password for the WAP-gateway (if used).

The user needs the address for the Mobile Executive server. To log on to Mobile Executive the user needs a username and a password. When users have entered this information to their phones they are ready to use WAP.

R320s Phone setup for D.N.A. WAP

Perform the following steps to setup an R320s Mobile Phone to be used with the WAP Gateway in the D.N.A. If you don't have all the information required, see your mobile phone administrator.

Go to the WAP Services menu and select 6 WAP Settings.



Select one of the available profiles, select **4** Access on the WAP Settings menu, select **1** Access Type on the Access menu, and set the Access Type to GSM Data.



Return to the Access menu, select 3 Service Center, and enter your Service Center number.

Technical Guide



Return to the **Access** menu, select **4 GSM Data**, select **1 Phone number** on the **GSM Data** menu, and enter the number of the modem pool used to the WAP Gateway. GSM stands for Global System for Mobile Communications.



Return to the GSM Data menu, select 2 Dial Type, and set the Dial Type to Analog.



Return to the GSM Data menu, select 3 User ID, and enter the user's ID.



Return to the **GSM Data** menu, select **4 Password**, and enter the user's password.



Return to the **Access** menu, select **5 Gateway**, select **3 Data Access** on the **Gateway** menu, and enter the IP Address of the WAP Gateway server.



More Mobile Executive Information

Installation

Mobile_Executive_Problems Troubleshooting%Mobile_Executive_Problems

Directory Browser

Directory Browser is a web-based application to search the DNA directory and to perform several

other functions. It enables corporations to publish a real-time corporate wide phone directory on the

corporate Intranet or publish the service on their corporate web page on the Internet as a service to external customers. Directory browser is HTML-based and does not need any client set-up. Installation and administration tasks are limited to the server side only.



Directory Browser offers two user levels:

- "Log off" status allows to search the database, look into detailed subscriber information, etc.
- Being "logged on" means to get permissions to basic call handling and messaging features (see below). Please note that a BusinessLink connection and a CTI license (CTI FECU) are required to use the call handling features.

BusinessPhone Operator Suite 5.0

Features

Directory Search

Search the corporate phone directory stored in the D.N.A. directory database. Search criteria are First name, Last Name, Extension, Department and two user selected fields where other information such as fax number, e-mail address, etc. can be added to the search criteria. In these fields, pop-up menus will allow the user to specify the D.N.A. fields with which he wishes to search.

Note: Directory Browser accesses the subscriber database only. It is not possible to search in the external number list.

Display and set Information Message (Absence information)

Directory Browser can show real-time information such as current absence information. The user must move the cursor on top of the diversion icon to see the reason for the diversion.

The "Information Message" screen gives the user the possibility to divert the phone at a certain time with the reasons (lunch, meeting etc.) configured in the BusinessPhone (and the DNA Server). The absence information is forwarded to the D.N.A. Server and from there to the BP system.

View Subscriber Details

Clicking on the Name will result in a display of all subscriber details.

Dial (basic call handling)

This feature requires BusinessLink for Windows NT license (FECU CTI) for all users. Clicking on the Subscriber Number will result in a jump to the "Manual Dial" Screen. In the "Manual Dial Screen" the number will be filled into the "Dial Box". The "Manual Dial" screen gives the user the possibility to manually enter a number and dial.

Multi-site functionality

It is possible to search multiple D.N.A. sites as well as in the global corporate directory based on the client's D.N.A. solution. For this kind of search no information message data can be provided. With the "Logon" the user selects a D.N.A. Server (where the Browser will search) and an extension to dial from (if the dialing option is configured). If no Logon is made dialing is not possible and a search will be performed on a server configured as default.

Technical Guide

Send, View and delete messages

Messages can be sent to other subscribers and the OWS by clicking on the envelope symbol in the search screen. The "Messages Screen" enables the user to view messages sent to him from the operator or other subscribers.

Other functions

Protection of sensitive information: Web Administrator can exclude sensitive data from being displayed as search results. This is done via a special field in the D.N.A. 4 database.

Customisation of the application: The customer can customise the Directory Browser page to a certainextent. Technically, the programming language HTML allows anything to be customised. However, the "Ericsson" headline will apply so that people will be able to see that this is an Ericsson product.

Localizations: The Directory Browser is only available in English language. However the product can be localized very easily by editing the HTML data (e.g. with MS FrontPage).

Directory Browser technical aspects

DNA Directory Browser runs on IIS (Internet Information Server), and can be installed in any order with the rest of the installation. Directory Browser installation has to be run separately, not included in the OPS installation, it might be on any other machine, either on the server or on any client.

The Browsers supported (tested) are Internet Explorer 4.0 and Netscape 4.0 and hinger. There is no installation required on the user's (client) side – just distribute and http address and people can start using it by simply clicking the address.

D.N.A. Directory Browser is typically installed on a company's Web-Server. The Server component needs to communicate with the D.N.A. server in order to fetch directory information. The D.N.A./WWW integration is provided by a search component using RDS as a protocol to query the Directory and to receive the result set. The D.N.A. Directory database is replicated and stored locally on the WWW machine by the search component. Performance

D.N.A. Directory Browser does not put more strain on the D.N.A server than one single user since it copies the D.N.A. data locally to the WWW server. D.N.A. sees the Directory Browser as a single client regardless of the fact that several people simultaneously access the directory data. All changes in the D.N.A. Directory Database will be propagated immediately to the Directory Browser WWW component.

The bandwidth allocation for queries to the Directory Browser is handled by basic WWW server administration tasks:
- Deciding how many simultaneous connections are allowed.
- Limiting the bandwidth usage by the WWW server.

In summary, the customer can control and manage easily the level of service provided by this application and it's impact on the network.

SNMP Agent

SNMP Agent comes with Windows NT and Windows 2000, but is not part of the Typical Installation. To make the SNMP agent for D.N.A. work you have to do two things, install D.N.A. and install the Windows NT master agent. You must have administrator privileges to perform this installation.

SNMP is actually a DMI agent that pretends to be an SNMP agent. The following diagram shows an overview of the different components.



The Monitored Objects

SDS, RDS, TSS, VSI, SCS, LDS and OWS Supervisor are the components that are monitored. They all include a small piece of code that acts like a wrapper between the applications and the *as_dmi.exe* component. They call functions in the wrapper class to initialize, report status, and shutdown applications. When the applications run for the first time they are added to a persistent table that *as_dmi.exe* keeps in the registry. This can be seen under *HKLM*\Software\Ericsson\DMI\AppSuite.

InstalledAppSuiteComponents is a bit mask where the "known" applications APP_ID are or'd together.

Each application also has its own value there, describing its current state. These are named with the applications short name.

as_dmi.exe

This is the central repository for the status information. The applications store their current status here and DMI picks it up from here. This component is a singleton. That means that there should only be one instance of it running on the machine, all applications (running on this machine) plus *asdmi.exe* connect to the same object.

asdmi.exe

This component is the glue that actually makes this into a DMI agent. It's instantiated by the CIMgr (i.e. it comes and goes with it) and there is only one at a time on each machine.

CIMgr & Win32sI

These services make up the core of the DMI run-time system. Win32sI has to be started before you can start this service (dependency is set in the registry). Actually, CIMgr isn't a service. The service is called CIMgrLdr and its only purpose is to run CIMgr. The registry keys for CIMgr can be seen under *HKLM\Software\Intel\CIMgr*. The registry keys for Win32sI can be seen under HKLM\Software\Intel\DMI 2.0 SDK.

NT SNMP

This is the Windows NT master agent. Actually, this piece routes SNMP requests to the right DLL. All its functionality is built on installable sub-agents contained in DLL files that are loaded when the master agent is started (as an NT service). The registry keys for NT SNMP can be seen under *HKLM**System**CurrentControlSet**Services**SNMP*.

Dmi2snmp

This is both a DMI management application and an SNMP sub-agent. It performs this double duty as the middle layer that maps SNMP requests to DMI calls and transforms DMI events into SNMP traps. It has no user interface and no configuration, it's just loaded by the master agent when it starts and then does its job quietly. The registry keys for Dmi2snmp can be seen under *HKLM\Software\Inte\DMI* 2.0 to SNMP Mapper.

See Also:

SNMP Master Agent

Remote Data Monitor

The Remote Data Monitor (RDM) utility displays error information and audit messages for D.N.A. applications. To start RDM, double-click on DNA_S\SHARE\BIN\rdm.exe.

Technical Guide

Remote D	ata Monitor	×	
	Please enter LDAP/LDS/RDS/SCS/TSS/VSI Server name or press OK to accept the default.		
	BT_LIBRA		
	C LDAP Server		
	C LDS Server		
	RDS Server		
	C SCS Server		
C TSS Server			
	O VSI Server		
	Other Server		
	OK Cancel		
	Citt		

Some of the things you can see with RDM are:

- Local Database Transfers
- Clients Registering and Disconnecting from RDS
- LDAP Queries and Answers

GICI Codes Sent to and from the PBX

	Remote I	Data Moni	tor			
<u>F</u> ile	<u>O</u> ptions	: <u>H</u> elp				
[00, [00, [00, [00, [00, [00, [00, [00,	/08/09 (/08/09 (09:06:24] 09:06:24] 09:06:24] 09:06:34] 09:06:34] 09:09:06] 09:09:06] 09:09:06] 09:09:06] 09:09:06] 09:09:06] 09:14:06] 09:14:06] 09:14:06] 09:14:06] 09:15:00] 09:15:00] 09:17:28]	17024 17017 17019 17019 17465 17294 17179 17174 17178 17465 17294 17173 17178 17173 17178 17178 17178 17294 17102 17294 17001	 Message From Client 3224 on BT_LIBRA: Remote Data Mor Message To Client 3224: Message ID=0, Status=1 Message To Client 3224: Message ID=9, Port=None, Status Message To Client 3224: Message ID=9, Port=[Thunder]SCS SQL Database Server Status : Up Periodic Function End Of Event Signal Periodic Function Audit Event Signal NT Virtual Memory Usage Went Down to 53.80% NT Hard Disk Drive c:\ Usage Sustaining At 60.18% SQL Database Server Status : Up Periodic Function End Of Event Signal NT Virtual Memory Usage Went Down to 54.74% NT Virtual Memory Usage Went Up to 54.74% NT Hard Disk Drive c:\ Usage Sustaining At 60.18% SQL Database Server Status : Up Periodic Function End Of Event Signal Periodic Function Audit Event Signal Periodic Function End Of Event Signal 	nitor Registered, Versio =2, PortID=1 S<==>SerialDevice1, S	on No
	-					
1743	33				JRUS ⊂u ⊃jBT_LIBRA	

Visitor Registration

Customers can use Visitor Registration to have visitors to a facility register in the lobby. The Visitor Registration dialog box is opened from the **Start** menu.

Start > Programs > D.N.A. Application Suite > Visitor Registration

The Visitor Registration dialog box provides edit boxes for **Visitor Name**, **Contact Person**, **Extension**, and **Keyword**. The **Extension** field defaults to the contact person's extension, but can be changed. Visitor information is registered with the **Add** button and unregistered with the **Delete** button. The **Refresh** button updates the dialog box fields with the latest information from the database. Visitor information can be printed with the **Print...** button.

RichWin

Note: This functionality is a MD110 specific feature and is not fully verified with BusinessPhone Communication System.

D.N.A. has been verified with the RichWin for Windows NT 4.0 Workstation and Server, and Windows 2000 Professional and Server. This allows D.N.A. applications to run in the Simplified Chinese language on an English operating system.

The following products have been verified.

- RichWin for NT Server
 Provides support for Windows NT 4.0 Server
- RichWin for Windows 2000
 Provides support for Windows 2000

RichWin 97 for NT provides support for Windows NT 4.0 Workstation

The RichWin software must be installed prior to installing D.N.A.

Limitations when using Simplified Chinese

The following limitations apply when running D.N.A. 5.0 Sp3 in Simplified Chinese.

When using RichWin IME, all system components will remain in English, including OK and Cancel buttons in program property sheets.

When using the RichWin IME, it is necessary to press keys twice when editing. For example, to delete a character, you must press the backspace or delete key twice.

Installing RichWin on Windows 2000 with Service Pack 2

When installing RichWin for Windows 2000 on a system with Windows 2000 Service Pack 2 loaded you will need a patch for RichWin. This patch and more information can be found at:

http://richwin.sina.com.cn

Preinstallation

About Pre-Installation

Before installing D.N.A. Application Suite components, perform checks and preparations necessary for a smooth and successful completion. Specifically, make certain you perform the following:

- 1 Conduct a pre-installation meeting with the customer.
- 2 Verify that all PC hardware requirements have been addressed.
- 3 Verify that all software requirements have been addressed.
- 4 Verify that all PBX requirements have been addressed.

Pre-Installation Meeting

You can avoid many common D.N.A. installation problems by including at least one pre-installation meeting in your preparations. Use this meeting to coordinate your plans with the customer well in advance of the actual installation. The following manuals could be useful for Installation.

- Windows NT / 2000 System Guide
- SQL Server Books Online (BOL)

Addressing Important Issues

Try to cover all the major issues involved in the installation process. Don't make presumptions about issues that may seem "obvious." For example:

Who is responsible for arrangements and preparation of the computer network (Ericsson or the customer)?

Pre-installation Checklist

Ericsson provides a Pre-Installation Checklist to help with installation planning. Use this checklist to identify and verify the all-responsible persons and essential D.N.A. components.

PBX Hardware / Software Requirements

BusinessPhone Communication System

Any Digital Telephone Set of the following list:

- Economy telephones Dialog 2751 / Dialog 2601 and Economyplus telephones Dialog 3201 / Dialog 3211
- Standard telephones Dialog 2755 / Dialog 2631 / Dialog 3202 / Dialog 3212 / Dialog 4222
- Executive telephones Dialog 2753 / Dialog 2662 / Dialog 3203 / Dialog 3213 / Dialog 4223
- Operator telephones Dialog 2554 / Dialog 2663 / Dialog 3214 / Dialog 4224

PBX Licensing:

To run the OWS, no dedicated CT license is required in the PBX. The Basic license already includes the CTI-based operator functionality necessary for OWS.

However please note that the Directory Browser dialling functionality is supported for up to two (2) clients with the Basic license normally used with OWS. A dedicated CT licenses is required to enable Directory Browser dialling functionality for more than two (2) users.

PBX Software Requirements

All BusinessPhone Operator Suite applications support Ericsson's BusinessPhone 50/128i/250 system software:

• PBX System software: BusinessPhonePhone communication platform 4.0 or higher.

Note: Refer to BusinessPhone Documentation Suite 6.0 (FASBS 160 001) for additional information regarding BusinessPhone Communication System hard- and software requirements.

PBX Internal Settings

Before installing and using one of the Operator Suite applications some settings via BMS have to be executed before being able to start the BusinessPhone Operator Suite applications.

Some BusinessPhone Operator Suite specific features (e.g. voice paging, night switching, ...) require additional configurations in the internal settings of the PBX.

PBX Command Settings

These Settings are only minimum settings to make sure that the system is running properly. For enhanced settings please refer to the BusinessPhone Operation and Maintenance Manual.

Command Group	Command	Description	Value
General	0175	Use as CTI operator instrument?	Y
		Each extension used as a Operator Work station device must be set as CTI operator.	
Voice Paging	3006-3013	TCD: Voice Paging Group 0 - 7	Y*
	0301	Define key for paging and answer	#
	3102-3109	Program name of the group	#
	4801-4808	Group members	#
	4809	Volume control	#
Night Mode	3022	TCD: Day/Night System	Y
	3023-3030	TCD: Day/Night Trunk Group 0 7	Y*

YYes Y*Yes; depending on individual needs

..... refer to BusinessPhone Operation and Maintenance Manual

Configuration Options

Ericsson's D.N.A. Application Suite consists of flexible products that can be used in a wide range of configurations. For purposes of this help guide, however, the general configuration options are explained in the following table.

Configuration Options	Туре	Details	
Stand-alone Installation	Single Node	S View details	
Network Installation	Single Node	View details	
Network Installation	Single Node / Server and Client combined	S View details	
Network Installation	Single Node / Telephony Server	S View details	
Network Installation	Multi Node / Corporate Network	View details	

PC Hardware Requirements

This section lists basic hardware requirements for D.N.A. server and client PCs.

Server

Each PC that will be configured as a D.N.A. server should meet the following requirements.

Component	Minimum Requirement
PC CPU	Intel Pentium III / 500MHz
Memory	128 Mbytes RAM (Minimum 256 RAM for Windows 2000)
Monitor and Card	1024X768 monitor and video card resolution
Mouse	Microsoft-compatible two-button mouse.
CD-ROM	(Required for server PC only.)
Network Card	LAN network card – TCP/IP connection (not required for stand-alone system).
COM Ports	BusinessPhone Operator Suite communicates via LAN, there is no COM port required.
	If the BusinessPhone BusinessLink server service is installed on the BusinessPhone Operator Suite Server, one COM Port is required for the connection to the BusinessPhone PBX. No COM port is required,

	if the BusinessPhone PBX is equipped with an IPU-card, as the BusinessLink for Windows server (min. Version 3) can communicate with the BusinessPhone PBX via the LAN.
	(see BusinessPhone BusinessLink documentation).
Printer Ports	IEEE-488 parallel port for printer (LPT1).
Sound Board	Server (optional), OWS client (recommended for Visually Impaired option).
Speakers	Server (optional), OWS client (recommended for Visually Impaired option).
Specific Requ	irements
DMG	Database size: 45 Mbytes for the first 2000

DMG	Database size: 45 Mbytes for the first 2000
	subscribers.
	2.5 Mbytes for each additional 500 subscribers.
	10 Kbytes / photo (2.5 cm x 1.5 cm in 256 colors).

Client PC

Each PC that will be configured as a D.N.A. client should meet the following requirements.

Component	Minimum Requirement		
PC/CPU	Intel Pentium II / 300 MHz		
Memory	128 Mbytes RAM		
Monitor and Card	800x600 monitor and video card resolution		
Mouse	Microsoft-compatible two-button mouse.		
CD-ROM	Required for server only.		
Network Card	LAN network card – TCP/IP connection (not needed for a standalone installation)		
Printer Ports	IEEE-488 parallel port for printer (LPT1).		
Sound Card	OWS client (recommended for Visually Impaired option).		
Speakers	OWS client (recommended for Visually Impaired option).		

Additional Hardware Options

Additional hardware that can be installed on a PC includes Ethernet adapter, tape drive, and serial port adapter (or DigiBoard). To install the hardware, follow the manufacturer installation instructions to set the IRQ and I/O address. You may need to run setup programs from the vendor to configure the hardware. IRQ and I/O addresses must be unique for each port and hardware device.

Software Requirements

1 D.N.A. Server:

• Windows NT 4.0 (with Service Pack 6a), Windows 2000 (with Service Pack 3)

 Microsoft SQL Server® 7.0 (with Service Pack 4) and MSDE (with Service Pack 4) and Microsoft SQL Server® 2000 (with Service Pack 3a) and MSDE 2000 (with Service Pack 3a)

2 D.N.A. Clients:

- Windows NT 4.0 (with Service Pack 6a), Windows 2000 (with Service Pack 3), and Windows XP Professional (with Service Pack 1)
- Microsoft Windows 98 with Service Pack 1 (DOI clients only)

3 Internet Tools:

- IIS 4.0 or IIS 5.0
- D.N.A. Directory Browser, and Mobile Executive must be installed on a server containing Microsoft Internet Information Server
- IE 5.0 or later or Netscape Navigator 4.0 or later
- D.N.A. Directory Browser works with Internet browsers Microsoft Internet Explorer 5.0 or later, or Netscape Navigator 4.0 or later.

4 WAP Software:

- WAP Gateway: Mobile Executive requires Ericsson WAP Gateway 2.0 or 3.0
- WAP 1.1 or 1.2 browser: Mobile Executive supports the WAP-enabled handheld device with WAP 1.1 or 1.2 browser
- 5 BusinessPhone:
- BusinessPhone Version 4.0 system software or higher

6 Simplified Chinese language support

Using Windows NT or Windows 2000 with SQL Server 2000 or DTE in the Simplified Chinese operating system version

-or-

 English Windows NT or Windows 2000 with SQL Server 2000 or DTE and with the RichWin IME (Input Method Editor) software

Important You must have 100 MB free disk space on each server or client PC in order to run the D.N.A. installation program.

You should have all the recommended hardware installed on a PC before installing Windows NT. The installation program only loads device drivers for hardware detected during installation. If hardware is added later, after Windows NT installation, you will need to run the appropriate Control Panel application to load the necessary driver(s) and DLLs at that time from the installation CD.

The Windows 2000 family consists of the Professional, Server, Advanced Server, and Datacenter Server versions.

Windows 2000 Professional is a direct replacement for Windows NT 4.0 Workstation and is designed for standalone or network client PCs. It has a limited Web server and can handle two CPUs.

Windows 2000 Server has all of the features of Professional in addition to supporting 4 CPUs with up to 4 GB of RAM. It has an Active Directory controller and a full version of Microsoft Internet Information Services 5.0, XML support, and integrated Virtual Private Networking.

Windows 2000 Advanced Server can handle up to 8 CPUs, address 8 GB of RAM, and provides load balancing and clustering.

The Windows 2000 Datacenter Server has the ability to handle 32 CPUs and address 64 GB of RAM. It also contains a high level of scalability.

SQL Server

D.N.A. applications use Microsoft SQL Server 7.0 with SP3, MSDE with SQL Server SP3, Microsoft SQL Server 2000, or SQL Server 2000 Desktop Engine as a centralized database server. If a database application does not exist on the server, the D.N.A. application suite installation program prompts you to choose between SQL Server 2000 Desktop Engine and Microsoft SQL Server 2000 for Simplified Chinese, and between SQL Server 2000 Desktop Engine, MSDE, Microsoft SQL Server 2000, or Microsoft SQL Server 7.0 for General Latin.

Internet Tools

DNA Directory Browser and Mobile Executive must be installed on a server containing Microsoft Internet Information Server (IIS 4.0 for Windows NT 4.0 or IIS 5.0 for Windows 2000). PPM Lite and Ericsson Communication Assistant work with Internet browsers Microsoft Internet Explorer 4.0 or later, or Netscape Navigator 4.0 or later.

Supported D.N.A. Server / Client Configurations

Supported configuration:

DNA Server	DNA Client
NT4 Server	NT4 Workstation / Server
NT4 Server	Windows 2000 Professional / Server
NT4 Server	Windows XP Professional *
NT4 Workstation	NT4 Workstation / Server
NT4 Workstation	Windows 2000 Professional / Server
Windows 2000 / Server	NT4 Workstation / Server

Windows 2000 / Server	Windows 2000 Professional / Server
Windows 2000 / Server	Windows XP Professional *

* There are some known issues with DNA client on Windows XP. Please refer to section "D.N.A. Client Installation on Windows XP" in Technical Guide.

Not supported configuration:

DNA Server	DNA Client
Windows 2000 Professional	NT4 Workstation / Server
Windows 2000 Professional	Windows 2000 Professional / Server
Windows 2000 Professional	Windows XP Professional

Hard Disk Requirements

When estimating hard disk storage requirements, always allow for the storage requirements of all applications, data, and support files that will reside on the hard disk. The following tables list server and client PC disk space requirements for individual D.N.A. applications.

Note You must have 100 MB free disk space on each server or client PC in order to run the D.N.A. installation program.

Recommendation

For best reliability Ericsson recommends that you use the Windows NT File System (NTFS). NTFS has proven to be more stable than the FAT. If you are supporting a large system requiring data redundancy, you may use any of Windows NT's RAID software implementations. However, if you choose to employ a hardware RAID solution, make sure it is on the Windows NT hardware compatibility list (HCL).

Server Disk Space Requirements

The following table lists server PC disk space requirements for individual D.N.A. applications.

Note You must have 100 MB free disk space on each server or client PC in order to run the D.N.A. installation program.

Application Executable		SQL Database	Caching for GUI Execution		
			Local DB	Memory map files	Log Files
D.N.A.	30 MB for	DNACOMMONDAT 4 MB	12 MB/1000 subscribers	N/A S	(1MB / 1000) x Total extensions on all nodes x 15
Server	executable files	DNACOMMONLOG 2 MB			
	44 MB for	DNADFDAT 2 MB	Cabeenbere		
	client	DNADFLOG 10 MB			[See D.N.A.
	installation files	SECUDAT 4 MB			Server note
		SECULOG 2 MB			
		XDAT - 4 MB			
		XLOG - 4 MB			
Photos	N/A	10 KB per 2.5 cm x 1.5 cm (1" x $\frac{1}{2}$ ") photo in 256 colors	N/A	N/A	N/A
Customer Information Files	N/A	Customer dependent	N/A	N/A	N/A
Directory Manager	10 MB	DIRDBDAT -for fewer than 2000 subscribers = [20 MB]	1 MB	[1.5 MB + 4.6 KB x No. of subscribers]	N/A
		-For more than 2000 subscribers = [20 MB + 1 MB/200 x (No. of subscribers - 2000)]			
		DIRDBLOG -for fewer than 200 subscribers = [25 MB]			
		-For more than 2000 subscribers = [25 MB + 1MB/200 x (number of subscribers - 2000)]			
Operator Workstation	3 MB	N/A	6 MB/1000 subscribers	N/A	7 KB per logged-in User ID

*N/A = does not apply

Notes

D.N.A. Server

Assume that MDS is used not more than 15 days per month and the following month the log file is overwritten.

SQL Server Data Volume Estimates

To avoid confusion, it is important that you understand the difference between automatic recording and automatic data extraction. Recording is performed by the PBX and extraction is performed by Performance Data Manager.

SQL DB		Data	Log	Total	
Period			Files	Volume	
Primary	6 months	63 MB	10 MB	73 MB	
Auxiliary	12 months	108 MB	10 MB	118 MB	

Client Disk Space Requirements

The following table lists client PC disk space requirements for individual D.N.A. applications.

Important You must have 100 MB free disk space on each server or client PC in order to run the D.N.A. 4.0 installation program.

Application	Executable	SQL Databas e	Caching for GUI Execution		
			Local DB	Memory map files	Log Files
D.N.A. Server	(EXE - 10 MB)	N/A*	N/A	N/A	N/A
	(installation files - 1.5 MB)				
Photos	N/A	N/A	N/A	N/A	N/A
Directory Manager	3.5 MB	N/A	N/A	[1.5 MB + 4.6 KB x No. of subscribers]	N/A
Operator Workstation	3 MB	N/A	6 MB/1000 subscribers	N/A	7 KB per logged-in User ID

*N/A = does not apply

Software Licensing

The BusinessPhone Operator Suite is protected by a software protection device (WIBU-Box sourced by WIBU Systems in Germany). The software protection device carries the functionality of the software application (as purchased by the customer. In order to control the purchased functionality the WIBU-Box has to be connected to the parallel port of one of the customer's PCs, which is accessible over the customer's LAN (TCP/IP network).

To be able to run the software application, the software licensing software (WIBU-Key software) has to be installed. The WIBU-Key software is split up into a Server installation and Client installation. The PC with the connected WIBU-Box is acting as the WIBU-Key Server all other PC's which are using the applications are acting as the WIBU-Key clients.

The required installations are carried out either during the installation of the application or have to be done in a separate installation step. Please refer to the technical guide of the related product.

For further information please refer to the related documentation of BusinessPhone Software Licensing.

Hardware Connections

Connection Between Server PC and Client PC

For network installation of D.N.A. applications, each client PC must be connected to the central server PC that has the SQL database and Management Repository Server software. Each client PC is connected to the server PC using standard Ethernet or Token Ring cards and cabling. Once the client PC is connected to the server PC, use Windows 2000 to set up the network. Refer to the Windows 2000 documentation for a description of how to set up the network.

Note: Use TCP/IP to configure your network. The TCP/IP protocol is strongly recommended to be able to use BusinessPhone BusinessLink for Windows.

Connection Between PABX and BusinessPhone Operator Suite

BusinessLink for Windows is the computer-telephony integration (CTI) link that connects Ericsson's BusinessPhone Communication System with applications running on computers and computer networks.

The PC, running BusinessPhone BusinessLink for Windows Server Service is connected with the BusinessPhone 250/50 PABX via a V.24 (RS-232) interface using up to 19.200 Baud.

Windows and SQL Installation

NT 4.0 Server

When your PC has a CD-ROM drive, you will need to boot from the three Microsoft NT boot-diskettes. These diskettes will detect your hardware, and will load the necessary CD-ROM drivers for installing Windows NT.

- 1 At the "Welcome to Setup" screen, press Enter.
- 2 Press Enter again to allow Setup to detect mass storage devices in your computer.
- 3 Press Enter again to continue without manually specifying additional devices.
- 4 Read the Windows NT License Agreement and press **<F8>** to accept.
- 5 At the "Windows NT Server Setup", you may need to change the Keyboard Layout. (E.g., in Belgium the Keyboard Layout needs to be set to: **Belgian Dutch/French**)
- 6 Make sure that you "Format the partition using the NTFS file system"

Technical Guide

- 7 Choose the directory location where you want to install Windows NT. (The suggested location is \WINNT)
- 8 Press Enter to perform a thorough secondary examination of your hard disk(s)
- **9** Next, Setup will copy the Windows NT files to your hard disk.
- **10** When the files are copied, press **Enter** to restart your computer.

Note Remove diskette #3 from the disk drive. The PC will reboot, and start the 32-bit installation of NT/2000. The FAT formatted hard disk will be converted to NTFS.

- 11 Setup will request some information. Enter your Name and Organization
- **12** Enter the registration/licensing CD-Key. You will find this number on the yellow sticker on the back of your CD case.
- 13 Licensing Mode: Select **Per Server** or **Per Seat** mode. Normally, select **Per Server** and the amount of CLIENT ACCESS LICENSES that you have acquired.
- 14 Specify the Computer Name

Note Remember that every computer name needs to be unique on the entire Windows NT/2000 network, even if you work with separate domains. Therefore, do not use a common name like server. Also note that the customer does not have computer-names equal to your Ericsson L.C. site. Then you will get into problems when dialing-in via RAS (you then connect these two networks together, and this may result in NetBIOS-naming-conflicts). Please also try not to use underscores (_____) in the NetBIOS computer names, because these give problems in at the Domain Name Server (UNIX DNS). The underscores will be translated to dashes in DNS environments, and this can give unwanted results. Do not use computer names longer than 15 characters

- 15 Select the Server Type: Stand-Alone Server
- **15** Enter the Administrator Account Password

Note By default NT will install an account called "Administrator". When installing the NT Server as a PDC (see above), then this account will be the domain-wide administrator account (full control for all objects). And this "Administrator" password can be used domain-wide (also on all clients connected to this domain). See Account Strategy.

- 16 Select YES to create an emergency repair disk
- **17** Select components:
 - Accessibility Options
 - Accessories
 - Communications
 - Games
 - Multimedia
 - Windows Messaging

Note For D.N.A. Application Suite installations, please accept the default selections

18 Select that Windows NT is Wired to the network

Technical Guide

Note Verify that your network adapter is correctly installed (on a free IRQ), and physically connected to the network.

- 19 Select Start Search to look for Network Adapters
- 20 Select TCP/IP as the Network Protocol.
- 22 Install the default Network Services
- 23 Click Next to install the selected components
- 24 Answer the Windows NT Setup questions according to your selected components (see step 19.)
- 25 Set the Date/Time Properties.
 - Set the correct "Time Zone"
 - Enable "Automatically adjust clock for daylight savings changes"

Note Please make sure that all the client PC's have the same "Date/Time Properties" settings as the server PC.

- 27 Set the Display Properties and use at least the following settings:
 - Color Palette: 256 colors
 - Desktop Area: 800 by 600 pixels
 - Refresh Frequency: as high as possible (test with monitor)
- 28 Windows NT Setup will now start copying files.
- 29 Insert a floppy diskette labeled as "Emergency Repair Diskette", and let NT create it.
- 30 Restart the computer when installation is finished.
- **31** Select **My Computer** on the Windows NT Desktop, then **Control Panel** on the My Computer dialog box.
- 32 On the control panel, select Regional Settings, then select the Regional Settings tab.:
 - Select the appropriate language.
 - Also, Enable Set as system default locale

Note This setting will also effect your localization of the D.N.A. Application Suite.

- 33 On the Control Panel dialog box, select System, then select the Performance tab. Set the Application Performance slider control to None to give all programs equal amount of CPU time.
- 36 On the Control Panel dialog box, select System, then select the Startup/Shutdown tab.
- 37 Select "Windows NT Server" from the Startup drop-down list.
- 38 Select Show list for 5 seconds
- **39** Check all Recovery checkboxes, and type **%System Root%\MEMORY.DMP** into the **Write debugging information to** edit box.
- 40 Install the latest Microsoft Service Pack for Windows NT 4.0

Important There are no separate service packs for Windows NT Workstation and Windows NT Server.

- **41** In NT/2000 Event Viewer, set the Log Settings to:
 - Event Log Wrapping: Overwrite Events as Needed
- 42 Repeat this setting for System, Security and Application Log
- 43 Go to Control Panel. Select Network, Services, and Server. Set Server Optimization to Maximize Throughput for Network Applications
- 44 If you have more than 10 D.N.A. clients, we suggest increasing the HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Lanmanworkstation/Parameters registry value.
- **45** Change **MaxThreads** from 0x32 to 0x64 (if it does not exist, you may create it). This increases the server's performance in updating clients. Increasing the workstation services MaxThreads parameter increases the number of kernel threads that the registry will create, thus allowing more operations to be outstanding at any given time.

Note When you have a lot of warning messages of Event ID 232 in NT's Event Manager (**Failed To Write To Named Pipe Port XXXX; NT Error Code=232**), this value setting will improve performance of the Named Pipe LDB updating. Following this change you should not receive many of these warnings.

46 Verify that you have no errors in NT/2000's Event Viewer after a reboot.

NT 4.0 Workstation

Check Hardware before You Start

There are two methods of installing Windows NT.

- Installation when you have a local CD-ROM drive build in your client computer
- Network installation

Installing Windows NT from a Local CD-ROM Drive

When your PC has a CD-ROM drive, you will need to boot from the 3 Microsoft NT boot-diskettes. These diskettes will detect your hardware, and will load the necessary CD-ROM drivers to load the NT system.

Installing Windows NT from a Network Drive

When your PC has no CD-ROM drive, you will need to boot your PC with a network boot diskette. You can then download the NT installation via the network by running *WINNT.EXE* to start the installation.

- 1 At the "Welcome to Setup" screen, click **Enter** to set up Windows NT now.
- 2 Press Enter again to allow Setup to detect mass storage devices in your computer.
- 3 Press Enter again to continue and not to specify manually extra devices.
- 4 Read the Windows NT License Agreement and press F8 to agree.
- 5 At the "Windows NT Workstation Setup", you may choose to accept or change the Keyboard Layout. For example, in Belgium, Keyboard Layout needs to be set at: Belgian Dutch/French.
- 6 Make sure that you Format the partition using the NTFS file system.
- 7 Choose the location where you want to install Windows NT 4.0. (The recommended location is *\WINNT*).

- 8 Press Enter to perform an exhaustive secondary examination of your hard disk(s). Setup will now start copying the Windows NT files to your hard disk.
- **9** Remove the diskette # 3 from the disk drive
- **10** Press **Enter** to restart your computer. The PC will now reboot, and start the 32-bit installation of NT. The FAT formatted hard disk will now be converted to NTFS. Setup will ask issue additional prompts.
 - Setup Options: choose Typical
 - Enter your Name and Organization
 - Enter the CD-Key. You will find this number on the sticker on the back of your CD case.
 - Enter the Computer Name
 - Enter your Administrator Account Password

Remember, every computer-name needs to be unique on the entire network, even if you work with separate domains. Therefore, do not use a generic name like **server**. Also verify that the customer sight is not assigned computer names used by your Ericsson L.C. site. Otherwise, you will encounter problems when dialing-in via RAS. Once the two networks are interconnected, NetBIOS-naming-conflicts may arise. Do not use underscores (_) in NetBIOS computer names. Underscores in computer names can cause problems at the Domain Name Server (UNIX DNS). The underscores will be translated into dashes in DNS environments, causing unwanted results. Do not use computer names longer than 15 characters.

By default NT will install an account called "Administrator". This account will be added to the local account list (it will not be stored on the domain controller). Please see Account Strategy.

- **11** Select **YES** to create an emergency repair disk
- 12 Choose to install the most common Windows NT/2000 components.
- 13 Select Windows NT Wired to the network

Note Verify that your network adapter is correctly installed (on a free IRQ), and connected to the network

14 Select Start Search to look for Network Adapters

Note If NT does not automatically find your Network Adapter, choose **Select from list**. If you have a standalone installation, (only 1 PC, and no network) also install networking:

- 15 Install the default Network Services
- 16 Click Next to install the selected components
- **17** Answer the questions that the Windows NT Setup application asks. These questions will depend on your selected components (see above).

Date and Time Properties

- 1 Use the default settings for date and time properties unless you are experience with custom configuration options.
- 2 Choose the appropriate Time Zone
- 3 Enable Automatically adjust clock for daylight savings changes. Make sure that all client PC's have the same "Date/Time Properties" settings as the server PC.

Display Properties

Use the following minimum display color and quality settings.

- Color Palette: **256 colors**
- Desktop Area: 800 by 600 pixels
- Refresh Frequency: as high as possible (test with monitor)

Copying Files and Restarting

The Windows NT Setup applications will now start copying.

- 1 Insert a floppy to create an Emergency Repair Diskette
- 2 Restart the computer.

Regional Settings Properties

- 1 Select the My Computer icon on the Windows NT desktop, then Control Panel.
- 2 Double-click Regional Settings on the Control Panel, then select the Regional Settings tab.
- **3** Select the appropriate language.
- 4 Enable Set as system default locale. This selection will also effect localization of the D.N.A. Application Suite.

System Performance Settings

- 1 Select the My Computer icon on the Windows NT desktop, then Control Panel.
- 2 Double-click the **System** icon on the Control Panel, then select the **Performance** tab.
- 3 Set the Application Performance slider control to "Intermediate" (midway between **None** and **Maximum**).
- 4 Click the **Change** button. On the Virtual Memory dialog box, set the Paging File Size for Selected Drive to:

Initial Size= (2 x installed physical memory) Maximum Size= (2 x installed physical memory)

For OWS clients, the local database (LDB) files will be loaded into memory. If the physical memory is not big enough, virtual memory will be used. Microsoft's recommended size for the paging file is equivalent to the total amount of available RAM, plus 12 megabytes.

5 Ericsson recommends the following formula for an OWS Client PC:

Paging File Size: (OWS LDB Size + 40%) + (RAM + 12 MB) Example: With a total LDB size of 100 MB (large system), and your client PC has 48 MB of RAM, the recommended paging file size will be 200 MB.

System Startup/Shutdown Settings

- 1 Select the My Computer icon on the Windows NT desktop, then Control Panel.
- 2 Double-click the System icon on the Control Panel, then select the Startup/Shutdown tab.
- 3 In the System Startup box, select Windows NT Workstation 4.00 and Show list for 5 seconds.
- 4 For the Recovery box, ENABLE Write an event to the system log, DISABLE Send and administrative alert, ENABLE Write debugging information to %System Root%\MEMORY.DMP. Ericsson recommends disabling Send, an administrative alert so that the "Alerter" service does not need to be installed on the client computer.

Install NT Service Packs

Install the latest Microsoft Service Pack for Windows NT 4.0. Both Windows NT Workstation and Windows NT Server use the same service packs. Use the same language in Service Pack as for your Windows NT language version. In \Programs\Administrative Tools\Event Viewer, set the "Log Settings" to:

Event Log Wrapping: ENABLE **Overwrite Events as Needed** Repeat these settings for System, Security and Application Logs

Install Microsoft Excel

Install Microsoft Excel 97 / 200 or XP before you install the D.N.A. Application Suite. Install Excel on all systems that will run Performance Presentation Manager. MS Office Service Pack 2 is required for *Excel* 97.

Note MS Excel versions 5.0 and 7.0 not compatible with D.N.A. 5.0. You must install a later version.

Reboot and Verify Setup Success

Reboot the PC and verify that you have no errors in NT/2000's Event Viewer.

Windows 2000 Upgrade

There are two methods of installing Windows 2000.

- Installation when you have a local CD-ROM drive build in your client computer
- Network installation

Installing Windows 2000 from a Local CD-ROM Drive

- 1 Insert a Windows 2000 CD in the CD-ROM drive.
- 2 Respond **Yes** to the following message.

would you like to upgrade to Windows 2000?

- 3 Follow the instructions in the Windows 2000 Setup Wizard and accept the default options.
- 4 Select the appropriate configuration option for your network in the Windows 2000 Configure Your Server window.

Installing Windows 2000 from a Network Drive

When your PC has no CD-ROM drive, you will need to boot your PC with a network boot diskette. You can then download the NT installation via the network and run the "WINNT.EXE" command to start the installation.

SQL Server 7.0

Before installing SQL Server 7.0, you can run SQL Server Books Online directly from the compact disc. We recommend that you review the "Getting Started" and "Installing SQL Server" sections prior to installing this release.

Important When installing SQL Server 7.0 for the D.N.A. Application Suite, it is recommended you do the Custom installation and select Dictionary Order, case-sensitive for the Sort Order.

When installing SQL Server 7.0 from a network drive, do not use a Universal Naming Convention (UNC) file path such as:

\\<Servername>\Microsoft\MsSql.70\AUTORUN.EXE

Instead, map a drive to the appropriate location and run the Setup program from the drive letter, for example:

F:\MsSql.70\AUTORUN.EXE

To install SQL Server 7.0

- 1 Use AUTORUN.EXE to install SQL Server 7.0 from a network drive or CD-ROM.
- 2 In the opening Microsoft SQL Server window, select Install SQL Server 7.0 Components.
- 3 From the Install SQL Server 7.0 Components menu, select Database Server Standard Edition.
- 4 Click **Next** > on the Select Install Method page to accept the default installation method (**Local Install Install to the Local Machine**).
- 5 Make sure no Windows programs are running and click **Next** > on the Welcome screen.
- 6 Click Yes on the Software License Agreement screen to accept the license agreement.
- 7 Enter your Name and Company on the User Information screen and click Next >.
- 8 Enter your CD Key on the Setup screen and click OK.
- 9 Verify your Product ID is correct on the second Setup screen and click OK.
- **10** On the Setup Type screen, select the **Custom** option. If desired, you can change the Destination Folders for Program and Data files. When finished, click **Next** >.
- 11 Click Next > on the Select Components screen to accept the default Components and Sub-Components.
- 12 On the Character Set/Sort Order/Unicode Collation screen, select **Dictionary order, case-sensitive** from the **Sort Order** drop-down list and click **Next** >.
- 13 Click Next > to accept the defaults on the Network Libraries screen.
- 14 On the Services Accounts screen, select the Use the Local System account option and click Next >.
- 15 Click Next > on the Start Copying Files screen to proceed.
- **16** Use the Licensing Mode dialog box to set up the Licenses. The choices you make here depend on the type of SQL Server license the customer has purchased. When finished, click **Continue** to start the installation.
- 17 When the installation completes, click Exit on the Microsoft SQL Server options page.
- **18** Install SQL Server Service Pack 4.

Security

For security reasons, you should change the default **sa** Login ID and blank password of MS SQL Server.

- 1 In the Service Manager window, open the registered D.N.A. Server's tree and the Logins tree.
- 2 Double-click on **sa** to open the Manage Logins dialog box.
- 3 Change the Login Name and Password and click Modify.

Note After changing the "sa" password, also change your "Login ID Password" for the registered D.N.A. Server in SQL Enterprise Manager. You can do this by right-clicking the Server Name.

Memory

SQL Server 7 is configured dynamically. However, memory should be limited to ½ for SQL Server use.

To set a maximum value for memory (Enterprise Manager)

- 1 Expand a server group.
- 2 Right-click a server.
- 3 Click Properties.
- 4 Click the Memory tab.
- 5 In the memory box, select maximum size (MB), and slide it to the desirable position.

SQL Server 2000

Upgrading from Microsoft® SQL Server[™] version 7.0 to Microsoft SQL Server 2000 is one of the basic choices offered by the SQL Server Setup program on the initial Installation Selection screen. When you select the option to **Upgrade**, **remove**, **or add components to an existing installation of SQL Server**, Setup detects your current installation and initiates the correct sequence of setup screens for the upgrade selected. Upgrade variations include:

- A complete installation upgrade from SQL Server 7.0 to SQL Server 2000 (installing over SQL Server 7.0)
- Adding components to an installation of SQL Server 2000
- An upgrade to the feature set of an existing installation of SQL Server 2000 (edition and component upgrade)
- An upgrade to SQL Server 2000 from SQL Server version 6.5 using the SQL Server Upgrade Wizard
- An online database upgrade of SQL Server 7.0 databases to SQL Server 2000 database format using the Copy Database Wizard

During the upgrade from SQL Server 7.0, external packages, such as Microsoft Management Console and the Microsoft Distributed Transaction Coordinator, must be installed for each upgrade, and the registry updated. The Master database and other system databases are upgraded in various ways involving a series of scripts run on the server with specific options. If the upgrade process fails, built-in recovery mechanisms restart and resume the upgrade.

Upgrade

To upgrade from SQL Server 7.0 to SQL Server 2000

- 1 Use AUTORUN.EXE to upgrade to SQL Server 2000 from a network drive or CD-ROM.
- 2 Select SQL Server 2000 Components on the Microsoft SQL Server 2000 Enterprise Edition screen.
- 3 Select Install Database Server on the Install Components screen.
- 4 Click **Next >** on the Welcome screen.
- 5 Click **Next >** on the Computer Name screen to accept the default **Local Computer** option.
- 6 Select the Upgrade, remove, or add components to an existing installation of SQL Server option and click Next >.
- 7 Click **Next >** on the Instance Name screen.
- 8 Click Next > on the Existing Installation screen to accept the default **Upgrade your existing installation** option.
- 9 Check Yes, upgrade my SQL Server Tools and data on the Upgrade screen and click Next >.
- 10 On the Connect to Server screen, select the Authentication Mode setup should use to connect to SQL Server and click Next >.
- **11** Click **Next** > on the Start Copying Files screen to proceed.

- 12 Use the Choose Licensing Mode dialog box to set up the Licenses. The choices you make here depend on the type of SQL Server license the customer has purchased. When finished, click Continue to start the installation.
- 13 Click Next > on the Microsoft Data Access Components 2.6 Setup screen to shut down the tasks in the Task list.
- **14** When setup completes the installation of Microsoft Data Access Components 2.6, click **Finish** to begin the installation.
- 15 Click Finish on the Setup Complete screen to complete setup.

New Installation

Important When installing SQL Server 2000 for the D.N.A. Application Suite, it is recommended you do the Custom installation and select Case-sensitive for the Sort Order.

To install SQL Server 2000

- 1 Use AUTORUN.EXE to install SQL Server 2000 from a network drive or CD-ROM.
- 2 Select SQL Server 2000 Components on the Microsoft SQL Server 2000 Enterprise Edition screen.
- 3 Select Install Database Server on the Install Components screen.
- 4 Click **Next >** on the Welcome screen.
- 5 Click Next > on the Computer Name screen to accept the default Local Computer option.
- 6 Click Next > on the Installation Selection screen to accept the default Create a new instance of SQL Server, or install Client Tools option.
- 7 Enter your Name and Company in the edit boxes on the User Information screen and click Next >.
- 8 On the Software License Agreement screen, read the agreement, and select **Yes** to accept the license agreement and proceed.
- **9 9** Click **Next** > on the Installation Definition screen to accept the default **Server and Client Tools** option.
- 10 Click Next > on the Instance Name screen to use the **Default** if this is the first instance of SQL Server 2000. Enter a unique instance name if this is not the first instance on this server.
- 11 Select **Custom** on the Setup Type screen and change the desired destination if desired.
- 12 Click Next > on the Select Components screen to accept the default Components and Sub-Components.
- 13 On the Service Account screen, select the Use the Local System account option for Service Settings.
- 14 On the Authentication Mode screen, select the **Mixed Mode (Windows Authentication and SQL Server Authentication** option. Enter a password or check the **Blank Password** option.
- 15 On the Collation Settings screen, select SQL Collations option and Dictionary order, casesensitive, for use with 1252 Character Set for all languages except Chinese. For Chinese select Collation designator and Chinese_PRC. Check Case sensitive and uncheck Accent sensitive for Sort order.
- **16** Click **Next >** on the Network Library screen to accept the default settings.
- 17 Click Next > on the Start Copying Files screen to proceed.
- **18** Use the Choose Licensing Mode dialog box to set up the Licenses. The choices you make here depend on the type of SQL Server license the customer has purchased. When finished, click **Continue** to start the installation.

- 19 Click Next > on the Microsoft Data Access Components 2.6 Setup screen to shut down the tasks in the Task list.
- **20** When setup completes the installation of Microsoft Data Access Components 2.6, click **Finish** to begin the installation.
- 21 Click Finish on the Setup Complete screen to complete setup.

Unattended SQL Server Installation

Unattended SQL Server installation is convenient if you want to install several SQL Servers with identical configurations. The Setup program reads the installation settings from a pre-defined installation information file instead of prompting in the SQL Server installation wizard.

If a database application does not exist on the server, the D.N.A. application suite installation program prompts you to choose between SQL Server 2000 Desktop Engine and Microsoft SQL Server 2000 for Simplified Chinese, and SQL Server 2000 Desktop Engine, MSDE, Microsoft SQL Server 2000, or Microsoft SQL Server 7 for General Latin. If you select SQL Server, you are asked for the SQL Server CD key, setup files, and the location of the installation information file (*.iss). The installation information file location defaults to the template that comes with D.N.A. installation. The default installation information file provided in the D.N.A. application suite installation contains the recommended options for the SQL Server Enterprise edition.

The following language settings are used in these files:

General Latin - Dictionary order, case-sensitive, for use with ISO code page 1252 character set.

Simplified Chinese – Dictionary order, case-sensitive, for use with Simplified Chinese code page 936 character set.

If you need to create your own *.iss file you can find a text file "SQL2000_Collation_Name.txt" located on the installation CD under \dna\DBEngineInstall. This file contains all SQL collation names and you can use it as reference if another SQL Collation is preferred than the predefined ones.

Note D.N.A. database files must be deleted manually after MSDE un-installation. The MSDE un-installation process only removes the databases installed at MSDE installation time such as Master database. All databases created later have to be removed manually.

Install SQL Server 2000 Standard Edition Unattended

A pre-defined SQL Server configuration template is provided for customers who use SQL Server 2000 Standard Edition. The template std_template.iss is located at OPS 5.0 installation CD \dna\DBEngineInstall\MSSQL2000\Configurations. Please follow the procedures below to use it.

1. Copy setup_std_template.iss to a system on the network that can be accessed by DNA Server installation.

- 2. Modify setup_std_template.iss
 - Add your SQL Server CD key at line CDKey= xxxxx-xxxxx-xxxxx-xxxxx. This step is mandatory.
 - ISO code page 1252 character set with Dictionary order, and case-sensitive is used in the template (defined at line collation_name = SQL_Latin1_General_CP1_CS_AS). If another SQL Collation is preferred, you can use "SQL2000_Collation_Name.txt" located on the installation CD \dna\DBEngineInstall. This file contains all SQL collation names
- 3. During DNA Server installation
 - At Database Application Selection dialog box, select Microsoft SQL Server 2000
 - At Database Application Installation Configuration dialog box, enter or browse for the **destination** path of SQL Server files. Enter or Browse for the location of the SQL Server **installation files**. Enter the location of your SQL Server **configuration file**. This is where the modified setup_std_template.iss with your SQL CD key defined. Leave SQL Server CD Key as blank.

Install SQL Server Service Pack

Unattended SQL Server installation does not cover Service Pack installation. You must install the SQL Server Service Pack depending on your SQL Server version.

Service Pack 4 for SQL Server 7 or MSDE 1.0

You can install SQL Server 7 SP4 from OPS 5.0 installation CD as follows:

- 1. Double click \dna\DBEngineInstall\ServicePack\SQL7_SP4\sql70sp4.exe to unpack the file
- 2. Double click \<sql7 sp4 package>\X86\setup\setupsql.exe and follow the wizard to install the service pack

Service Pack 3a for SQL Server 2000

You can install SQL Server 2000 SP3a from OPS 5.0 installation CD as follows:

- 1. Double click \dna\DBEngineInstall\ServicePack\SQL2000_SP3a\sql2ksp3.exe to unpack the file
- 2. Double click \<sql2k sp3a package>\X86\setup\setupsql.exe and follow the wizard to install the service pack

Service Pack 3a for MSDE 2000

You can install SQL Server 2000 SP3a from OPS 5.0 installation CD as follows:

- 1. Double click \dna\DBEngineInstall\ServicePack\SQL2000_SP3a\sql2kdesksp3.exe to unpack the file
- 2. Install service pack via command line:

```
(a) change directory
```

- cd \<sql2kdesk sp3a package>\sql2ksp3\msde (b) launch setup by type in
 - setup.exe /upgradesp SQLRun blanksapwd=1

– or –

- (a) COpy \dna\DBEngineInstall\ServicePack\SQL2000_SP3a\
 Install_MSDE2000_SP3a.bat to \<sql2kdesk sp3a package>\
 sql2ksp3\msde
- (b) Double click the batch file
- 3. Restart the system after service pack is installed

SNMP Master Agent

Windows NT

The D.N.A. SNMP agent requires Windows NT service pack 6a. Make sure you have the service pack and the Windows NT 4.0 distribution CD handy before starting this installation. You must also have administrator privileges to perform this installation.

- 1 Open the Control Panel by selecting Start > Settings > Control Panel.
- 2 Open the Network dialog box by double-clicking on Network.
- 3 Click the **Services** tab.
- 4 Open the Select network Service dialog box by clicking the Add button.
- 5 Scroll down in the list-box until you see **SNMP Service**. Click once on that line to select it and then click the **OK** button.
- 6 After a few seconds the Windows NT Setup dialog-box is opened. This means that Windows needs to know where it can find the necessary files to complete this installation. These files are on the Windows NT distribution CD. Insert the CD in the CD-drive of this machine or enter the path to where this CD is. When this is done, click **OK** and the process will continue.
- 7 After the SNMP installation is done, the SNMP properties screen will come up. This dialog-box has three tabs. On the first tab, named **Agent**, enter your name in the contact field and the address where the machine is located in the second text field. You can leave the checkboxes under **Service** with default values.
- 8 On the **Traps** tab, enter **public** as community name and click the **Add** button next to it. Click the **Add...** button under the **Trap Destinations** list and enter the IP address or hostname of the machine running EVM in the small dialog-box that pops-up and click **Add...** to close it.
- 9 On the Security tab, make sure Send Authentication Trap is checked, that public has READ CREATE rights and that Accept SNMP Packets from Any Host is checked. These settings are a

good starting point since they don't put many restrictions on the SNMP traffic. When you feel comfortable with SNMP configuration, feel free to change them.

- **10** When you now click the **OK** button, the Microsoft SNMP Properties dialog-box will close and you'll have to restart the machine.
- **11** After the machine starts up again you might get an error message about a function entry point not found. This is normal if you had service pack 6A installed before the SNMP installation. The solution is to re-apply the service pack again.

Windows 2000

- 1 Open the Control Panel by selecting Start > Settings > Control Panel.
- 2 Open the Add/Remove Program Properties dialog box by double-clicking on Add/Remove Windows Components.
- 3 Scroll down to Management and Monitoring Tools.
- 4 Click this line once (don't click in the checkbox).
- 5 Click the **Details...** button. A new dialog-box appears.
- 6 Find the line **Simple Network Management Protocol**, click in the checkbox to enable it and click the **OK** button.
- 7 Click the **Next...** button; Windows2000 will now start to install this component. After a few seconds the Insert disk message box is opened.
- 8 Click **OK**. The Insert disk dialog box is opened. This means that Windows needs to know where it can find the necessary files to complete this installation. These files are on the Windows 2000 distribution CD. Insert the CD in the CD-ROM drive of this machine or enter the path to where this CD is located.
- 9 Click **OK** to continue the process.
- 10 When the Windows Component Wizard is displayed, click the Finish button.
- 11 This returns you to the Add/Remove Windows Components dialog box.
- 12 Click Close.
- 13 Close the Control Panel.
- 14 Click Start > Programs > Administrative Tools > Services.
- 15 In the right pane, find the line SNMP Service, right-click and choose Properties.
- **16** The SNMP Service Properties dialog box is opened. This dialog-box has seven tabs. Click the **Agent** tab.
- 17 Enter your name in the **Contact** field and the address where the machine is located in the second text field. You can leave the checkboxes under **Service** with the default values.
- 18 Click the Traps tab.
- **19** Enter **public** as the community name and click the **Add** button next to it.
- 20 Click the Add... button under the Trap Destinations list and enter the IP address or hostname of the machine running EVM in the small dialog-box that pops-up.
- 21 Click the Add... button.
- 22 Click the Security tab.
- 23 Make sure Send Authentication Trap is checked, that public has READ CREATE rights, and that Accept SNMP Packets from Any Host is checked. These settings are good starting points since they don't put many restrictions on the SNMP traffic. When you feel comfortable with the SNMP configuration, feel free to change them.
- 24 Click **OK** to save these settings. Remember to stop and re-start the SNMP service to make the settings active.

Related Topics Networking (SNMP) Access Agent SNMP Agent

D.N.A. Installation

About Installation

Before installing D.N.A. application software, be sure all PCs and PBX nodes are set up as described in Hardware Requirements. Software installation for most D.N.A. applications is separated into server installation and client installation.

Hardware Connections

You must perform or verify installation of all necessary communications and signaling connections before proceeding to software installation.

Software Installation

- Server Installation. For a D.N.A. Server installation, all server software is installed on one PC, and the client software is then installed on one or more PCs connected to the server.
- Client Installation. Client software can be installed from a network D.N.A. Server or directly from a D.N.A. software CD-ROM inserted in the client PC's CD-ROM drive.

Installation Checklists

This section provides checklists for D.N.A. server and client workstation installation. Use these checklists to assist in installing D.N.A. Application Suite Version components.

Using the Checklists

These checklists help insure that important installation issues are not overlooked. Perform the steps listed in each checklist and check off each item as you proceed through each D.N.A. component installation. For future reference, leave copies of these records with the customer and with the responsible Ericsson Customer Services location.

For More Information

For more information, see the user documentation delivered with the individual D.N.A. products.

Submit Your Comments

Send comments and remarks about D.N.A. installation checklists and other Technical Guide issues to the EBC Enterprise Support Center.

Pre-installation Checklist

Use this pre-installation checklist to verify and identify all hardware and software components before beginning the installation process.

Installation Profile

List the your customer identity along with all software and hardware components to be included in this installation.

Customer:

Responsible Contact:

Technical Guide

BusinessPhone Operator Suite 5.0

Hardware Server:				
Software D.N.A.: Software PBX: PBX Type: Number of client PC's: Installation Eng. D.N.A.:	□ BP 250 □ BP 50 □ BP 128i			
Installation Date:	20			
Installation Component Verific Microsoft Windows NT Server/Datacenter Server Microsoft Windows NT Worl Microsoft SQL Server 7.0 + Microsoft MSDE + SP 3 Microsoft SQL Server 2000 Microsoft SQL Server 2000 D.N.A. Access Agent: Base Date:	 ation 'er + Service Pack 6A or Windows 2000 Server/Advanced kstation + SP6A or Windows 2000 Professional SP 3) + SP 3) Desktop Engine + SP 3 System Version RV 			
Installation Product Identificat Product ID NT/2000 Server: Product ID NT/2000/XP Worksta Product ID SQL SERVER: Product ID (D N A Server):	ion,,			
Product ID DMG: Product ID OWS: Product ID DDB:	, , ,			

Windows is a trademark[™] of Microsoft Corporation.

The information in this document is subject to change without notice.

ERICSSON MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Ericsson shall not be liable for errors contained herein nor for incidental or consequential damages in connection with the furnishing, performance or use of this material.

Product ID DME:

Application Suite Installation

This section helps you to prepare for the decisions and responses required during the installation process. You will encounter a different prompts and dialog boxes depending on whether yours is a new installation, a re-installation, a server installation, or a client installation.

You can install D.N.A. applications on a client PC or server. When you install the D.N.A. applications, you may include just the components you want, ranging from a minimal configuration to the entire suite of D.N.A. applications. The full installation installs all D.N.A. components.

D.N.A. Application Suite runs on the following Microsoft Windows operating systems.

Windows NT 4.0 Workstation Windows NT 4.0 Server Windows 2000 Professional Windows 2000 Server Windows 2000 Advanced Server

Warning It is against Microsoft's End User License Agreement to use, in any way, Windows NT 4.0 Workstation or Windows 2000 Professional as a server.

Installation Features

New installation features for D.N.A. include:

Customizable System — The application licenses must be turn on through License Administration and user privileges through User Configuration. The node information such as node name, communication method, etc. must be set through RDS Setup. The user-defined fields in the Directory database must be defined through Directory Configuration.

Pre-configured System — The installation sets up licenses and turns on the application licenses. The defined users and privileges will be assigned and the node information and communication with the BusinessPhone will be configured. The desired user-defined fields for Directory Manager will also be defined.

Silent Installation — You may use the graphical D.N.A. *setup.exe* interface, or the "Silent Installation" method supported by a pre-configured *.ini* file. (Silent Installation only applies to client installations.)

Pre-Configured System

You can use a pre-configured installation file (*dna.cfg*) to retrieve system information and make the installation automatic. The *dna.cfg* file contains default settings for pre-configured information that you can edit for your installation. The installation program prompts you for the location and file name. In addition, the installation program validates the pre-configured information file to make sure all required information is defined correctly.

> See also Configuration BusinessPhone File Parameters below

User Names and Privileges

There are two types of users can be defined in the pre-configuration information file:

Administrator Account — All application with pre-defined (highest privilege) privileges are assigned. Regular User Account — The desired application with associated pre-defined privilege (highest privilege) will be assigned.

PBX Communications

Node Information — All information associated with a node can be defined. For example: Node name, release and password.

Communication with the PBX — Your choice of communication with the PBX can be defined.

GICI Configurations

You can specify GICI/CSTA configuration methods. For the BusinessPhone communication system configure here the BusinessLink connection as described in the BusinessLink documentation.

Data Synchronization

After installation has completed successfully and the system is rebooted, the system will be automatically logged on with the NT user and password you defined. The synchronization of data then can be started automatically from a batch file that contains the command for data synchronization for each individual node. The synchronization is executed one node at a time.

User-defined Fields for Directory Manager

The desired user-defined fields for all categories such as Department, Profile, Person, Confidential, Room, Function, External, and Information can be defined. The searchable flag and icon can also be identified.

Configuration BusinessPhone File Parameters

You can edit the following parameters in the *dna.cfg* file for a pre-configured installation.

See also a .cfg example for BusinessPhone

```
[NTlogon]
Validate=YES (validate user)
DomainName=domain
UserName=user
Password=123456
;sample of MDS remote connection with phone number specified
[MDSConfiguration1]
Enable=1
ConnectionType=REMOTE
SiteName=Test Remote
NIU_Password=HELP
IPU Password=HELP
NIULoginUserName=MDUSER
ASB501Release=8
Port=1
phonesetup1=6632
;sample of MDS direct connection
[MDSConfiguration2]
```

BusinessPhone Operator Suite 5.0

Technical Guide

Enable=1 ConnectionType=DIRECT SiteName=Test Direct NIU_Password=HELP IPU_Password=HELP NIULoginUserName=MDUSER ASB501Release=8 Port=2 ;sample of MDS telnet connection [MDSConfiguration3] Enable=1 ConnectionType=TELNET TelnetSetup1=195.150.112.120,4,,, TelnetSetup2=195.150.101.182,3,agent,password, SiteName=Test Telnet NIU_Password=HELP IPU_Password=1HELP NIULoginUserName=MDUSER ASB501Release=8 [GICIPortConfiguration1] Enable=1 PortName=test direct ConnectionType=DIRECT DNFillerCharacter=@ InformationSystemID=00 MaxDNLength=5 MaxTerminalID=2 BaudRate=9600 DataBits=8 StopBits=1 Parity=1 FlowControl=0 OutputTimeDelay=50 Port=COM2 [GICIPortConfiguration2] Enable=1 PortName=test niu ConnectionType=NIU DNFillerCharacter=A InformationSystemID=00 MaxDNLength=5 MaxTerminalID=2 NIUPortID=12345 [GICIPortConfiguration3] Enable=1 ConnectionType=TELNET PortName=test telnet

Technical Guide

DNFillerCharacter=@ InformationSystemID=00 TelnetAddress=195.150.113.98 TelnetAccount=abcd TelnetPassword=test OutputTimeDelay=100 DNFillerCharacter=64 InformationSystemID=00 MaxDNLength=8 MaxTerminalID=2 [Licence] Enable=1 NumberOfExtensions=100 NumberOfSubscribers=200 NumberOfConcurrentUsers=-1 [UserPrivileges] Enable=1 tstusr=test user;test user description;USER;MDS,1,2,3;PCOPI tstusr2=test user2;test user2 description;all,3 [UserDefinedFields] Enable=1 ;Number of Profile fields is even number from 8 to 20 NumberProfileFields=14 Profile1= Prof Assistant, 6, Yes, Assistant Profile2= Prof Cost_Center, 1, No,None Person1 = Person Home, 43, Yes, HOME Confidential1 = Conf password, 53 Department1 = My department, 31, NONE External1 = My external, 3, MAIL Function1 = function Cellular number, 38, Yes, CELLULAR Room1= room Secretary Name, 6, NO, SECRETARY Information1 = My info, 29, yes, NONE

Upgrading To Operator Suite 5.0

This information only applies to customers with existing D.N.A. systems already installed, if you are doing a new installation from the CD you will not need to upgrade your system.

To apply Operator Suite 5.0 to your existing D.N.A. system you will need to upgrade using the new CD containing Operator Suite 5.0.

There are basically two different environments of older DNA systems.

- 1. Operator Suite 3.4 running on SQL Server 6.5
- 2. Operator Suite 4.1 running on either SQL Server 6.0 / 7.0 or MSDE.

For any scenario it is strongly recommended to backup the older system before starting the upgrade.

The ways to upgrade these two different environments are as follows:

From D.N.A. running on SQL Server 6.5

1. Upgrade SQL Server

Upgrade SQL Server 6.5 to either 7.0 or 2000 using the SQL Server upgrade wizard. Make sure that your SQL Server 6.5 has at least 10MB of data space available in the tempdb database and is replying correct with it's name to the "select @@servername" SQL statement before starting the upgrade.

2. Upgrade D.N.A.

Upgrade the existing D.N.A. system to 5.0.

After this you can chose to upgrade your Windows NT to 2000 or to transfer your DNA installation from this computer to another.

From D.N.A. running on SQL Server 7.0 or MSDE

<u>1. Upgrade D.N.A.</u> First upgrade the existing D.N.A. system to 5.0.

2. Upgrade SQL Server

Secondly upgrade SQL Server 7.0 to 2000 or upgrade MSDE to DTE or keep the database engine that the system is currently using. This step is optional.

After this you can chose to upgrade your Windows NT to 2000 or to transfer your DNA installation from this computer to another.

Transferring D.N.A. from one computer to another

If your existing D.N.A. installation is running on an older hardware platform there might be a need to transfer the complete system from one computer to another.

Upgrade D.N.A. Server and SQL Server on your current D.N.A. Server computer

The upgrading of SQL Server and D.N.A. should always be carried out on the computer that is currently running the D.N.A. system. If you after that want to move your D.N.A. installation from one computer to another you must make sure that the two computers are on the same network and are able to use named pipe connections between them.

Install the new D.N.A. 5.0 Sp3 system

Then you have to install a new D.N.A. 5.0 system on your new machine. Use either SQL Server 7.0 or 2000, Windows NT or 2000, but install with the same number of extensions, sites and extensions per site as the old system.

Transfer the databases

Finally use the D.N.A. dbcp tool to backup the databases to flat files. Move the files from the old system to your new and use the dbcp tool to restore data from files to the database engine you are using at the new system. Reboot the PC after restoring the databases.

Upgrade D.N.A. clients

Do not forget to load any available service packs or hot fixes for Windows, SQL Server or D.N.A. When done test the applications on the server computer and finally upgrade the clients.

Server Installation

D.N.A. application setup now recommends which applications to install and where to install them. For example, you will probably want to choose the **Typical** option in the installation wizard, which installs all D.N.A. applications. Alternatively, you may choose the **Custom** option that allows you to select individual applications to include in the installation, omitting those you do not want.

The D.N.A. Server installation process installs the D.N.A. operating platform, all applications (except Ericsson Communication Assistant, Mobile Executive, PPM Lite, Lotus Notes, and Outlook Integration), and all administrative tools on your Windows NT/2000 Server PC. Windows NT/2000 Workstation client PCs may then connect to this server to install D.N.A. applications and support utilities.

Auto-Run Installation

Insert the D.N.A. CD in the CD-ROM drive. If supported by your PC, auto-run will activate the installation program and you will be presented with the following auto-run options.

- Install Application Suite
- Install Lotus Notes Integration 4.6
- Install Lotus Notes Integration 5.0
- Install Mobile Executive
- View Technical Guide
- View Release Notes

Exit

Taskbar Installation

Use this procedure to install from the CD-ROM on a PC that does not support auto-run.

- 1 Insert the installation CD.
- 2 Click Start, Run on the Windows NT/2000 taskbar.
- 3 Type the network path to the desired setup program (for example, installing from CD, type: d:\dna\setup.exe. Alternatively, use the **Browse** button to browse to the appropriate *setup.exe* program file.
- 4 Click the **Server** installation option button and follow the instructions from the installation wizard.

New Server Installation

le5.0 required for SQL Server 2000 or desktop engine
If you are going to use the embedded SQL Server installation from within the D.N.A. installation program please make sure that the pre requisites for installing SQL Server 2000 or SQL Server Desktop Engine are met. This includes having Internet Explorer 5.0 or later installed.

MDAC 2.6 required

When MDAC 2.6 is not installed on the PC, the Question message box is displayed. Click **Yes** if any of the following pre-requisites are met.

- Windows NT 4.0 and IE 4.01 + SP 2 or later
- Windows 2000 and IE 5 or later

DNA installation (both Server and Client) will install MDAC 2.6 if it is not found. However, the system must have right version of IE installed before MDAC can be installed properly.

Question		\times
?	MDAC 2.60 is not installed on this system. After installing MDAC, DNA Installation will reboot the system and resu Would you like to continue?	ime.
	<u>Yes</u> <u>N</u> o	

Server Installation Wizard

This table lists the screens and prompts displayed when you perform a new installation.

Wizard Screen and Options	Explanation			
Welcome	Overview of what the installation will accomplish, instructions for closing other applications, copyright warnings.			
Software License Agreement	Conditions for using the installed D.N.A. software.			
Installation Type	Choose whether the PC you are setting up will be a			
Server	D.N.A. Server or Client. The server installation			
C Client	applications. The client installation places selected applications in a \\dna_c directory and assigns the connected server as the local server.			
Database Server Language Collation	This screen is displayed only when SQL Server is not installed.			
General Latin				
Simplified Chinese				
Database Application Selection	If installation cannot detect a database engine and			
SQL Server 2000 Desktop Engine	General Latin was selected on the Database Server			
O MSDE	You must have licensed SQL Server if you choose the Microsoft SQL Server option. Microsoft SQL Server 2000 Desktop Engine or MSDE is provided by			
O Microsoft SQL Server 2000				

Microsoft SQL Server 7	the D.N.A. Installation.
 Database Application Selection SQL Server 2000 Desktop Engine Microsoft SQL Server 2000 	This page is displayed when the installation cannot detect SQL Server and Simplified Chinese was selected on the Database Server Language Collation screen. You must have licensed SQL Server if you choose the Microsoft SQL Server option. Microsoft SQL Server 2000 Desktop Engine is provided by the D.N.A. Installation.
Database Application Installation Configuration	
Destination Path	Enter or browse for the destination of SQL Server files. The default is the MSSQL7 directory on the OS
Installation Files (not displayed of you chose Desktop Engine of MSDE) Configuration File CD Key (not displayed of you chose	drive. Enter or Browse for the location of the SQL Server setup files. Enter the location of the SQL Server configuration file. The D.N.A. Installation displays the default configuration file provided by the installation package. Enter the SQL Server CD Key if required
Desktop Engine of MSDE)	Enter your name and company
Registration Confirmation	Click Yes if the registration is correct.
Database Application Administrator Password	Enter a password for the Database Administrator (sa) account if desired. If the D.N.A. installation program installed MSDE or DTE for you the password will be blank.
Nodes and Extensions for Database	Select from 1-256 nodes and 500 to 200,000
Number of Nodes (drop-down list) Total Number of Extensions (drop-down list)	extensions for your network. This information is used to determine the amount of disk space needed for the installation. You may change these options.
Select Installation Method	Choose Typical to install all available D.N.A. components (applications, databases, and D.N.A. Server support utilities and components), <u>excluding</u> Numbering Plan Manager.
Custom	Choose Custom to select specific components to install, <u>including</u> Numbering Plan Manager.
Select Components	This screen is displayed when you select Custom on the Select Installation Method page. Check the components you want to install in the list.
Locale Support	This screen is displayed when running a Custom Installation. Select the language of your choice from the list. The Typical Installation automatically installs English, and local support if the Regional Settings of the PC are supported.
Extension Per Node	Click the Change button to change the number of

	extensions for a selected node.
DNA PreConfiguration Option	This option can be skipped. To use this option, enter the full path name of the pre-configuration file or browse to it. Check Run MD Support synchronization if you want installation to start PBX data synchronization after installation is completed.
Choose Destination Location	Click Next > to accept the default folder for your installation, or click the Browse button to select another.
Data Files and Log Files Locations	Accept or choose locations for D.N.A. SQL database components. Use this screen to change the location of Log and Data files if desired.
RDS Scheduled Jobs	Select or unselect tasks that will be scheduled for automated execution after the installation completes.
Start Copying Files	Review a comprehensive summary of your installation choices. Click Next > to begin the installation process based on your choices. Click Back to change your selections before proceeding. Click Cancel to abort the installation.
Summary Installations	After the installation has finished, this screen displays a list of the D.N.A. components installed. It also displays any problems encountered during the installation.
Setup Complete	Choose Yes , I want to restart my computer now to restart your PC and complete the installation process. Choose No , I will restart my computer later to close the installation program and restart the PC later.

Installation Options

At any time after D.N.A. server software has been installed, you may use the Auto-Run or Taskbar installation methods to add, re-configure, and remove components using the following options.

Option	Explanation
Add Components	Allows you to add D.N.A. components not already installed.
Install Locale	Installs new language capabilities to installed components.
Reinstall	Allows you to repeat the last installation to restore missing or corrupted files.
Remove All	Deletes all installed D.N.A. components. (You may also perform this task using Add/Remove Programs from the Windows NT/2000 Control Panel.)

Resize Database Allows you to change the number of nodes, extensions, and other capacity parameters for the existing installation.

Add Components

On the Ericsson Setup dialog box, select **Add Components**. You will encounter the following dialog boxes when adding D.N.A. components to an existing installation.

Select Components – Lists components available to be added. Locale Support – Select language support for the new applications. Database Application Administrator Password Data Files and Log Device Locations Start Copying Files Summary Installations Setup Complete – Setup program has performed the requested upsizing tasks.

Click Finish. The system will now restart to complete the installation.

Resize Database

You will encounter the following dialog boxes when resizing D.N.A. components in an existing installation. On the Ericsson Setup dialog box, select **Resize Database**.

Nodes and Extensions for Database

Upsizing Components – Lists components eligible for upsizing. Upsizing Extension Per Node – Allows you to change node and extension quantities. Upsizing [Application ...Setup] SQL Administrator Password Start Copying Files Summary Installations Setup Complete – Setup program has performed the requested upsizing tasks. Click Finish.

Client Installation

The latest D.N.A. installation application improves the installation process. It now recommends which applications to install and where to install them. For example, you'll probably want to choose the **Typical** option in the installation wizard, which installs all the D.N.A. applications available on the selected D.N.A. server. Alternatively, you may choose the **Custom** option that allows you to select individual applications to include in the installation, omitting those you do not want.

Important If you're using a virus-protection utility, disable it before you run the D.N.A. *Setup* program. Also, close any open Windows applications.

Auto-Run Installation

Use this procedure to install from CD-ROM on a PC that supports auto-run.

Insert the D.N.A. CD in the CD-ROM drive. If supported by your PC, auto-run will activate the installation program and you will be presented with the following auto-run options.

Install Application Suite

Install Lotus Notes Integration 4.6

Install Lotus Notes Integration 5.0

Install Mobile Executive

View Technical Guide

View Release Notes

Exit

- 1 Select Install Application Suite.
- 2 Click the **Client** installation option button and follow the instructions from the installation wizard.

Taskbar Installation

Use this procedure to install from the network, or from CD-ROM on a PC that does not support auto-run.

- 1 If you are installing from a network location, connect to it. If you are installing from CD-ROM, insert the installation CD.
- 2 Click Start, Run on the Windows NT/2000 taskbar.
- 3 Type the network path to the desired setup program (for example, installing from CD, type: d:\dna\setup.exe; installing from network, type: d:\dna_s\mrs\InstallationFiles\ClientInstallation\setup.exe). Alternatively, use the Browse button to browse to the appropriate setup.exe program file.
- 4 Click the **Client** installation option button and follow the instructions from the installation wizard.

New Client Installation

When MDAC 2.6 is not installed on the PC, the Question message box is displayed. Click **Yes** if any of the following pre-requisites are met.

- Windows NT 4.0 and IE 4.01 + SP2 or later
- Windows 2000 and IE5 or later

DNA installation (both Server and Client) will install MDAC 2.6 if it is not found. However, the system must have right version of IE installed before MDAC can be installed properly.

Question	
?	MDAC 2.60 is not installed on this system. After installing MDAC, DNA Installation will reboot the system and resume. Would you like to continue?
	(<u>Y</u> es <u>N</u> o

Client Installation Wizard

This table lists the Screens and prompts displayed when you perform a new installation.

Wizard Screens and Options	Explanation		
Welcome	Overview of what the installation will accomplish, instructions for closing other applications, copyright warnings.		
Software License Agreement	Conditions for using the installed D.N.A. software.		
Installation Type Server Client	This screen is displayed when you install from the CD. Choose whether the PC you are setting up will be a D.N.A. Server or Client. The client installation places selected applications in a \\dna_c directory and assigns the connected server as the local server.		
User Information	Enter your name and company.		
Registration Confirmation	Click Yes if the registration is correct.		
D.N.A. Server Name	This screen is displayed when installing from a CD. Enter the network name of the D.N.A. server you wish to use as your installation source. Be sure to select a server that contains the same version of D.N.A. you are installing and all the components you need to install.		
Select Installation Method			
	Choose Typical to install all the components installed on the server.		
	Choose Custom to select specific components installed on the server.		
Select Components	This screen is displayed when you select Custom on the Select Installation Method page. Check the components you want to install in the list.		
Locale Support	This screen is displayed when running a Custom Installation. Select the language of your choice from the list. The Typical Installation automatically installs English, and local support if the Regional Settings of the PC are supported.		
Choose Destination Location	Click Next > to accept the default folder for your installation, or click the Browse button to select another.		
Start Copying Files	Review a comprehensive summary of your installation choices. Click Next > to begin the installation process based on your choices. Click Back to change your selections before proceeding. Click Cancel to abort the installation.		
Summary Installations	After the installation has finished, this screen displays a list of the D.N.A. components installed. It also displays any errors encountered during the installation.		

Setup Complete

Choose **Yes, I want to restart my computer now** to restart your PC and complete the installation process. Choose **No, I will restart my computer later** to close the installation program and restart the PC later.

Client Installation Options

At any time after D.N.A. client software has been installed, you may use the Auto-Run or Taskbar installation methods to add, re-configure, and remove components using the following options.

Note You must perform these operations using the D.N.A. server that was the source for the original installation. To change to a different server, you must first un-install all D.N.A. software and repeat the installation using the new server.

Option	Explanation
Add Components	Allow you to add D.N.A. components not already installed.
Install Locale	Installs new language capabilities to installed components.
Reinstall	Repeats the latest installation to restore missing files and / or settings.
Remove All	Deletes all installed D.N.A. components. (You may also perform this task using Add/Remove Programs from the Windows NT/2000 Control Panel.)

Silent Installation

You may now offer customers file-directed D.N.A. client installation assistance without being present at the installation site. This installation feature supports client **New Installation**, **Re-installation**, and **Add Component** options. Client **Un-install** is NOT supported.

Note Your users can run silent client setup from the D.N.A. Application Suite CD-ROM or from a local D.N.A. server. For the CD-ROM method, however, you must maintain an input file such as *dnasuite.ini* and use it as the input file for running the setup.

The installation process gets system setup information from a .ini file created by the system administrator. The administrator provides approved installation parameters via a configuration (.ini) file. The client PC user can then initiate the installation. The installation will proceed automatically without further intervention.

Modifying the Setup (dnasuite.ini) File

As a starting point, use the *dnasuite.ini* file (located in the same installation directory as *setup.exe*) that comes with the D.N.A. installation software. Copy and carefully modify this file for your needs. DO NOT delete any parts of this file, since all existing statements are used during the installation process. Make the following changes to the temporary installation file.

dnasuite.ini	Statement	Notes
[SETUP]	InstallClientPath=	Type a destination path for the installed files on the client PC, or leave blank to accept the default location (c:\dna_c).
	ServerName=	Type the name of your local server. If left blank, the install program will prompt the user for a response. This is a required parameter.
	LaunchEXE=ADO\MDAC_TYP.EXE, /Q, /C:"setup /QNT",WAIT	You must include the '/Q' switch to run ADO in quiet mode.
[OWS]	Install=1 Level=Professional	Set to 1 to install, 2 to not install* <i>Level</i> options are: Professional for fully configurable Operator Work Station interface and options; Basic for no configurable options and no remote search capabilities; Centrex for a BSS (service provider) configuration.
[DMG]	Install=1	Set to 1 to install, 2 to not install*
		* You can only install components that have been installed on the connected D.N.A. Server.

Installation Procedure

At the client PC, the installer performs the following steps.

- 1 From the taskbar and click **Start**, **Programs**, **Command Prompt**. The Command Prompt window will be displayed.
- 2 To get command prompt help, type:

command SETUP /?

3 At the client PC, use the following setup command to execute the file-driven installation. (See details on SETUP command below.)

SETUP.EXE silent ini=full path of dnasuite.ini

Using the Setup Command

There are three versions of the setup command for silent installation. One each for: New Installation, Re-Install, and Add Components.

Туре	Setup Command	Notes
New Installation	SETUP.EXE silent ini=[full path of dnasuite.ini]	You can only install components that have been installed on the connected D.N.A. Server.
Re-install	SETUP.EXE silent reinstall	Parameter <i>ini=filename.ini</i> is not needed. The setup will process using the current installed .ini file settings.
		You can only install components that have been installed on the connected D.N.A. Server.
Add Components	SETUP.EXE silent add ini=[full path of dnasuite.ini]	Setup will add components that have been flagged <i>Install=1</i>
		You can only add components that have been installed on the connected D.N.A. Server.

Mobile Executive

The basic D.N.A. Server client must be installed before you can install Mobile Executive. This section explains installation requirements and procedures for Mobile Executive. Mobile Executive is installed on an Internet server. Even though the Internet server and the D.N.A. server can be on the same machines, we recommend they be on separate machines for better performance. In addition, Internet servers are periodically taken down for maintenance.

Warning Mobile Executive will not function properly without a session state. The Session Timeout feature for your Mobile Executive web site must not be disabled.

Installing with Auto-Run

D.N.A. provides auto-run support for PCs that support this feature. When you insert the software installation CD into an auto-run compatible PC, the installation process is automatically started. The system will display an installation panel containing the following auto-run options.

Install Application Suite Install Lotus Notes Integration 4.6 Install Lotus Notes Integration 5.0 Install Mobile Executive View Technical Guide View Release Notes Exit

Select Install Mobile Executive to install from the Auto-Run interface.

Important If you're using a virus-protection utility, disable it before you run the D.N.A. *Setup* program. Also, close the control panel and any open Windows NT/2000 applications.

To install Mobile Executive on a server PC

1 Insert the D.N.A. installation CD in the CD-ROM drive.

-or-

If you're installing from a network location, connect to it.

- 2 Find and run the *MobileExec\setup.exe* program. Double-click **setup.exe** to start the installation.
- 3 Proceed through the Welcome, Software License Agreement, and User Information dialogs.
- 4 For New Virtual Directory, accept the mobileexec default for Name, or type another choice.
- 5 Accept the default **Destination Folder** settings or browse to a new location of your choice. The installation program will copy files and complete the installation settings.
- 6 When the installation completes, choose **Yes**, **I want to restart my computer now**. The system will shutdown, restart, and the installation will be complete.

Installation Options

The Mobile Executive installation provides **Reinstall** and **Remove All** options. **Remove All** can run from CD and Control Panel.

Option	Explanation
Reinstall	Allows you to repeat the last installation to restore missing or corrupted files.
Remove All	Deletes all installed Mobile Executive components. (You may also perform this task using Add/Remove Programs from the Windows NT/2000 Control Panel.)

Post Installation Setup

Windows NT

- 1 Select Programs ► Windows NT 4.0 Option Pack ► Microsoft Internet Information Server ► Internet Service Manger from the Start menu.
- 2 In the Tree pane, locate and click on the Internet Server name.
- 3 Click Default Web Site.
- 4 In the View pane, right-click **mobileexec**, and select **Properties**.
- 5 On the Virtual Directory tab (default), check Run in separate memory space (isolated process).
- 6 Click the HTTP Headers tab.
- 7 Click the File Types... button.
- 8 In the File Types dialog box click the **New Types...** button.
- 9 In the File Type dialog box, enter .wml in the Associated Extension edit box and text/vnd.wap.wml in the Content Type (MIME) edit box.
- 10 Apply all the settings and close all the dialog boxes by clicking **OK** in each one.
- 11 If NTFS is used, make sure **read and write** permissions are given to *Inetpub\WWWRoot\MobileExec\bin\session.mdb* (uncheck **Read-only** checkbox in properties).

Windows 2000

1 Select **Programs > AdministrativeTools > Internet Service Manger** from the **Start** menu.

- 2 In the Tree pane, locate and click on the Internet Server name.
- 3 Click Default Web Site.
- 4 In the View pane, right-click **mobileexec**, and select **Properties**.
- 5 On the Virtual Directory tab (default), select High (Isolated) from the Application Protection drop-down list.
- 6 Click the HTTP Headers tab.
- 7 Click the File Types... button.
- 8 In the File Types dialog box click the **New Types...** button.
- 9 In the File Type dialog box, enter .wml in the Associated Extension edit box and text/vnd.wap.wml in the Content Type (MIME) edit box.
- 10 Apply all the settings and close all the dialog boxes by clicking **OK** in each one.
- 11 If NTFS is used, make sure **read and write** permissions are given to *Inetpub\WWWRootMobileExec\bin\session.mdb* (uncheck **Read-only** checkbox in properties).

More Mobile Executive Information

- Phone Setup
- Troubleshooting

Directory Browser - Installation and Configuration of Directory Browser

Installation

1 Make sure that MS IIS is installed on the Web Server.

Note: It is recommended NOT to use the same Server PC for MS IIS and D.N.A. Server

- 2 Make sure that MS IIS is up and running. To start the Web Server Modules following Win dows NT Services must be started:
 - IIS Amin Service
 - WorldWide Web Publishing Service
- 3 Install D.N.A. Server Client on the Web Server To install a D.N.A. Server - Client start the normal Operator Suite Installation (from CD-ROM: ..\software\dna\setup.exe) and select "Client Installation". There is no need to install an OWS or a DMG Application.
- 4 Install D.N.A. Directory Browser on the Web Server

The installation files for D.N.A. Directory Browser are located on the product CD-ROM under the following directory: ..\software\ddb\setup.exe

Note: Make sure you have Windows NT Administrator priviledges.

User Configuration

To configure the D.N.A. Directory Browser it is mandatory to have specific user priviledges. The user priviledges can be set via BusinessPhone Operator Suite > Administrative Tools > User Configuration. Make sure that the user for configuring the D.N.A. Directory Browser has the READ/WRITE Access for the DDB Configuration.

Note: Access privileges for DDB Configuration can only be configured after the DDB Setup has been successfully executed.

Directory Configuration

In the Profile Tab of the User Defined Fields (UDF) configuration add following Data Types:

USER ID PASSWORD COMPUTER NAME

Save the changes

In the Directory Manager update the subscribers (for the subscribers who want to use DOI) with the User ID, Password and Computer Name information.

The User ID and the Password must be identical with the Windows NT Account of the specific person.

DDB Configuration

Following Settings has to be executed if the BusinessLink for Windows NT (for all Clients in the network) and a appropriate FECU is available.

🧱 DDB Configuration Utility - [L	ocal DNA S	erver] nina			_ 🗆 ×
<u>Application ⊻iew H</u> elp					
2 2 2					
CSTA Nodes					
Node ID	Port ID	Server Name			
1	2555	future23	Settings >>>		
			Add		
			Delete		
Log File					
Enable Log File Capture	e r			_	
Path Name Of Log File	······ [-	- 11	
Number Of Captured Log F	iles		 5		
Number Of Days Before De	eleting Log File.		 . 2		
Options					
Enable Free Seating				_	
Number of Seconds for D.N	N.A. Server Co	mmunication Timeout	 30		
For Help, press F1				NUM	SCRL //

Click Add and configure the connection to the BusinessLink for Windows NT Server PC.

DNA Directory Browser No	ode Information 🛛 🔀
CSTA Node ID	2
CSTA Server Name	ServerName
CSTA Port ID	2555
ОК	Cancel

Mark the "Enable Free Seating" check-box under the Options area.

Save the changes.

OPERATION

To start the D.N.A. Directory Browser

Open the Internet Browser.

In the Web Site enter one of the following addresses:

http://WebServerName/dirb

http://IP-Address/dirb

The **WebServer Name** is the Computer Name of the PC where the MS IIS / DNA Server - Cli ent is installed. Optionally it is also possible to enter the IP-Address instead of the Computer Name.

To work with the D.N.A. Directory Browser

For further information regarding the operation of the D.N.A. Directory Browser consult the Online Help accessable from the main page of D.N.A. Directory Browser.

Outlook Integration

The D.N.A. Outlook Integration (DOI) provides a bi-directional Integration between the Microsoft Office Outlook Calendar and D.N.A. Directory Calendar. This allows D.N.A. Directory Subscribers using Outlook's Calendar to synchronize the message diversion information with other D.N.A. applications through the D.N.A. Remote Data Server (RDS). Several pre-installation tasks must be completed before installing and running Outlook Integration. Usually these tasks are completed after D.N.A. server installation.

1 Before Installation, Microsoft Outlook 98 or greater must be installed on the system. If Outlook is not installed, the installation process will report an error. Outlook Integration does not need the exchange server.

- 2 Use the MD110 Support utility to synchronize **Operator Message Diversion** for **All** applications on the D.N.A. server. (not applicable for BusinessPhone)
- 3 Use the RDS Configuration utility to set **Default Diversion Duration** and **Default Diversion Stop Time** for all **Message Diversion Reason Codes** on the D.N.A. server.
- 4 Use the RDS Configuration utility to configure a **GICI/CSTA Port**.
- **5** Use the Directory Configuration Utility to add a Person UDF of type **Computer** to the database.
- 6 Use Directory Manager to add the Outlook computer name information to D.N.A. Directory.

Outlook Integration needs to be installed on both client and server machines.

To install Outlook Integration

Double-click on *DNA_S\DMG\CALENDAR\setup.exe* and follow the instructions in the Setup Wizard. **To uninstall Outlook Integration**

- 1 Open the Control Panel and double-click on Add/Remove Programs.
- 2 Remove D.N.A. Integration with Outlook.

Description of DOI

At Startup:

- DOI will look for the appointments with the subject "Message Diversion for <Reason Code>". Then DOI will read the Reason Code from the subject field, instead of opening the actual appointments.
- The message diversions from the DNA server are called "Message Diversion from DNA Server". DOI will not go through these message diversions, since they are already in the DNA server database.
- Then DOI sends the message diversions to the RDS (DNA server process) which in turn adds them into the DNA server database.

At Synchronization Interval:

- When you set or delete a message diversion with DOI, this information is stored in your local calendar.
- When the synchronization interval occurs, the message diversions are sent to the DNA server and the RDS will add or remove them from the DNA server database.

Registry Value For Synchronization Interval

You can change the synchronization interval with the Windows Registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Ericsson\Integration\Outlook\SynchInterval.

By default the value is set to 120 seconds (=78 Hex value).

Message Diversions from DNA server are sent instantly to the DOI client and are not affected by the SynchInterval value.

Registry Value For User ID instead of Computer UDF

In the D.N.A. Server Registry, change the following registry key.

 $\label{eq:hkey_local_MACHINE\SOFTWARE\Ericsson\MRS\RemoteDS\Manager\UseUserIDF or Calendar Integration$

Technical Guide

This value is set to 0 by default, which requires you to link a computer name (UDF type **Computer**) with a DMG subscriber. Setting this value to 1 changes Outlook Integration from using the PC name as the identity reference, to using the NT user's login name as the identity for Outlook calendar diversion settings. The advantage of using the NT user's login name allows you to use a Person UDF of type **User ID** instead of type **Computer**. This makes Outlook Integration more flexible and easier to manage.

After changing this registry key, stop and restart the Ericsson RDS service. It may take a few minutes for RDS to repopulate the local database. You can then use the Directory Configuration utility to add a UDF of type **User ID**, and then Directory Manager to add the Outlook user ID information to the D.N.A. Directory.

Limitations For Recurrent Diversions

The RDS can handle hourly, daily and weekly message diversion.

Weekly, has different interpretation in RDS compared to the Outlook Calendar. In RDS weekly means only one time per week. In Outlook, users can select multiple days during the week.

Ex. 1

If a user in Outlook selects "Daily" and "Every weekday", the DOI will pass this information to the RDS as weekly with every Monday to Friday. But RDS can only accept weekly and ignore the Monday to Friday. The result of this is that; the first time it will work (e.g. Wednesday), when the message diversion has expired, the record in the DNA server database will change to the next start time (i.e. Wednesday the next week).

Ex. 2

If a user in Outlook selects "Weekly" and multiple days (e.g. Monday, Wednesday, Friday), only the first one will be activated (i.e. Monday). The others will not be activated on the phone.

Ex. 3

If a user in Outlook selects "Monthly" or "Yearly", only the first message diversion will be activated. The others will not be activated on the phone.

Lotus Notes Integration

Before Lotus Notes Client Installation, Lotus Notes must be installed on the client. Before D.N.A. 5.0 Server installation, make sure the D.N.A. Server is configured to handle Message Diversion.

To install, insert the CD into the CD-ROM drive on a Lotus Notes client or D.N.A. server machine and run *setup.exe*. You will be prompted to choose one of the following installation options.

- Lotus Notes Integration Template Installs only D.N.A. Integration templates to \\DNA_S\MRS\InstallationFiles\ClientInstallation\LotusNotes \Template\ on a D.N.A. server
- D.N.A. Server (Integration Installation) Installs D.N.A. Integration installation software and templates on a D.N.A Server machine to \\DNA_S\MRS\InstallationFiles\ClientInstallation\LotusNotes\
- Lotus Notes Client Installation Installs D.N.A. Integration software on a Lotus Notes client machine into the \\...\Wotes directory or a directory of your choice

When Lotus Notes Integration is installed on a D.N.A. Server, users can install to their client machines from the D.N.A. Server by locating the server with Explorer and double-clicking on:

\\DNA_S\MRS\InstallationFiles\ClientInstallation\LotusNotes\Setup.exe.

COMPUTER or USER ID User Defined Fields

You need to link a User Defined Field (UDF) with DMG subscribers for Message Diversion to work with Lotus Notes Integration. The default UDF type is COMPUTER and the USER ID type is an option. When COMPUTER type is used, the extension associated with the computer name can be diverted. With this option, Lotus Notes client computers can only handle message diversions to one extension regardless of the user logged on. When USER ID type is used, the extension associated with the logged on user ID can be diverted. With this option, Lotus Notes client computers can handle message diversions for any logged on user.

To use the COMPUTER type default

- 1 Run the Directory Configuration utility and add an unshareable UDF of type COMPUTER to the database.
- 2 Run Directory Manager and add the Lotus Notes client computer name information to D.N.A. Directory.

To use the USER ID type option

- 1 Change the following registry key from 0 to 1.
- 2 HKEY_LOCAL_MACHINE\SOFTWARE\Ericsson\MRS\RemoteDS\Manager \UseUserIDForCalendarIntegration
- 3 Stop and restart the Ericsson RDS service.
- 4 Run the Directory Configuration utility to add an unshareable UDF of type USER ID.
- 5 Run Directory Manager and add the Windows user ID information to the D.N.A. Directory.

Lotus Notes Integration Templates

Before Lotus Notes clients can use the D.N.A. Lotus Notes Integration additions, the Lotus Notes Integration template for the installed language needs to be placed on the Lotus Notes Domino Server from the D.N.A. Server. There is more than one method do this, and you must have Lotus Notes Administrative privileges. For example, you can use Explorer to copy the template from the D.N.A. Server to the Lotus Notes Domino Server, or use Lotus Notes on the Domino Server to replicate the template on the Domino Server. Lotus Notes templates are stored in the Lotus Notes \\...\Data directory.

User Help

After installation to a Lotus Notes Client Machine, the D.N.A. Lotus Notes Integration User Help can be accessed using the **Start** menu from the same program group as D.N.A. Integration. For example:

Programs > Lotus Notes > D.N.A Integration Help

Settings and Configuratin after Installation

Directory Setup for Network Installations

If this is a network installation, use the Windows Explorer on the server PC to set the DNA_S directory as a shared directory.

Basic Configuration for the Server

Share and connect printers on/from network

After installation of all clients you can remove the share on the directory DNA_S (for security reasons – otherwise a client might be able to delete files in this directory.

Update the Emergency Repair Diskette on the Server (it has now Microsoft Service Pack (SP), new accounts/domains/settings/ ... included). From the command prompt run "RDISK /S" for this.

Administrative Tools

Important: Refer to the *corresponding Help file* for further information about the specific Administrative Tool.

Use the User Configuration utility to set up user accounts and their logon information and access privileges. Refer to the MRS User's Guide for a description of how to use the User Configuration utility.

Per default 3 users for BusinessPhone Operator Suite have been created:

- Administrator Privileges: User Configuration
- Ericsson Privileges: User Configuration
- OWS Privileges: Read/Write access to DMG, Read/Write access to OWS

Do not configure BusinessPhone Operator Suite user accounts for several people to share. This will cause problems when users are changing the profile of an account, because only the last changes are recorded. Use one BusinessPhone Operator Suite account for each BusinessPhone Operator Suite user. Sharing BusinessPhone Operator Suite accounts is also against free seating philosophy.

The OWS user account might be enough for most of the BusinessPhone Operator Suite users. Therefore this user account can be copied for each individual user. For some reason however the OWS user privileges can be enhanced with some privileges such as "Directory Configuration" and "Operator Configuration". This user will then be able to modify directory settings, to add new directory fields and to modify Operator configurations.

The Ericsson user can be used for creating new users in the future or to modify user privileges for individual and enhanced users.

The Administrator user account shall be enhanced with the following privileges:

Privilege	Element	Setting
RDS Configuration	Access	Read/Write
Trunk Configuration	Access	Read/Write
Directory Configuration	Access	Read/Write
D.N.A. Server Configuration	Access	Read/Write
Name Identity Conversion	Access	Read/Write
Operator Configuration	Access	Read/Write
LDS Configuration	Access	Read/Write
Directory Manager	Access	Read/Write
Directory Manager	Confidential	Read/Write
Export Utility	Access	Read
Operator Work Station	Access	Read/Write
Operator Work Station	Confidential	Read
Operator Work Station	Preferences	Read/Write
DDB Configuration ^a	Access	Read/Write

^a... DDB Configuration is only available after DDB Setup (Installation) has been successfully executed.

This user account will then be able to configure the complete BusinessPhone Operator Suite system after installation and during work later on.

For safety reasons modify the default passwords which are the same as user name per default.

We recommend also to configure one user responsible for maintaining Directory Manager:

Privilege	Element	Setting
Directory Configuration	Access	Read/Write
Name Identity Conversion	Access	Read/Write
Directory Manager	Access	Read/Write
Directory Manager	Confidential	Read/Write
Export Utility	Access	Read

A complete system shall have at least:

- 1 Administrator account
- 1 account for configuring and creating user accounts (can also be the administrator)
- 1 account for maintaining and configuring Directory Manager
- x accounts for the "normal" users

D.N.A Server Configuration

Use the MRS Server Configuration Utility to define a list of available servers. Check if the Time Zone is set according to your local settings. Add new server names if available in your network.

Directory Configuration

Configure all individual data fields for public, confidential, department, external, function and room data information.

If you are not sure which data you are going to use later on you will be able to modify it at any later time.

Note:	Make sure that DMG and / or Dirpon is not running	
10101	make sure that bine and / of bipop is not farming	

RDS Configuration

Configure the RDS Options according to your individual needs

This feature is only recommended for small installations that have limited number of SQL connections. To make sure that this feature takes into effect the administrator needs to stop and restart the RDS Service.

- · Configure the Local Database Population
- Configure Message Waiting Options (optional)
- Configure Message Diversion Options (optional)
- Configure PBX Information
- GICI/CSTA Ports
- Trunk Configuration

Configure trunk names, route names, custom names and access codes if available

Settings for Operator Workstation

Busy Lamp Field

Before the Busy Lamp Field (BLF) can be used in the main display it has to be configured. The configuration can be carried out via the Configure Busy Lamp Fields dialog, which is opened from the Options menu in the Operator Workstation application.

Feature Settings

Before being able to use special BusinessPhone Operator Suite features some configuration in the Windows NT Registry must be executed.

- Use the Windows NT Explorer to locate and execute (double-click) the Registry Editor pro gram **REGEDT32.EXE** in the \WINNT\SYSTEM32\ directory.
- Locate the HKEY_LOCAL_MACHINE dialog panel. To locate the Registry entries you want to configure, double-click **SOFTWARE | Ericsson | OPI**, then click **CurrentVersion**.

Night Switching

Double-click the **Night** entry to open the String Editor dialog box. Then type the code for Night switching (for BusinessPhone: *8#).

Number

Double-click the **Number** entry to open the String Editor dialog box. Then type any internal or external subscriber number you want to access quickly.

Malicious

Double-click the Malicious entry to open the String Editor dialog box. Then type the code for Malicious Call Identification (for BusinessPhone: *39#).

URL

Double-click the **URL** entry to open the String Editor dialog box. Then type the Internet lo cation, which you want to access by clicking the Browse button. (e.g. <u>http://www.ericsson.com</u>).

Common Queue Number (Operator)

Double-click the **OperatorQue** entry to open the String Editor dialog box. Then type any number you want to assign to the Operator Queue (BusinessPhone default value: 9). With the Operator Queue number you can always access the operator via the common queue.

Info File Configuration

Note: The configuration options described below are specifically included for users who wish to cus tomize their installation. Others may ignore this information.

You can configure OWS function keys to provide special operator instructions for situations like calling emergency services, lost & found items, reserving conference rooms, etc. You must configure the Windows NT OWS Registry options to execute the desired information file or applications when the given function key is pressed or selected. You can configure OWS to open a specific file using the Windows NT cardfile or notepad tools, or to access another information resource such as your company's World Wide Web home page.

It is recommended that you use either the notepad or cardfile option. However, the third option is also available.

NT Notepad Procedure

- Use the Windows NT Explorer to locate and execute (double-click) the Registry Editor pro gram REGEDT32.EXE in the \WINNT\SYSTEM32\ directory.
- 2 Locate the HKEY_LOCAL_MACHINE dialog panel. To locate the Registry entries you want to configure, double-click SOFTWARE Ericsson OPI, then click CurrentVersion. The Info File configuration options will be displayed in the edit window on the right.
- 3 Double-click the NotepadExeLocation entry to open the String Editor dialog box. Then type the path and name for the display application for your operators' instructional text file (e.g., C:\WINNT\NOTEPAD.EXE).
- ⁴ Double-click the **NotepadTxtFile** entry to open the String Editor dialog box. Then type the path and name of your operators' instructional text file (e.g., C:\INFODATA\INFO.TXT). Although it is possible to specify a network drive in these steps, we recommend that you place the information file on the OWS PC to assure access in the event of network problems.

NT Cardfile Procedure

- 1 Use the Windows NT Explorer to locate and execute (double-click) the Registry Editor pro gram **REGEDT32.EXE** in the \WINNT\SYSTEM32\ directory.
- 2 Locate the HKEY_LOCAL_MACHINE dialog panel. To locate the Registry entries you want to configure, double-click SOFTWARE Ericsson OPI, then click CurrentVersion. The Info File configuration options will be displayed in the edit window on the right.
- 3 Double-click the CardfileExeLocation entry to open the String Editor dialog box. Then type the path and name for the display application for your operators' instructional text file (e.g., C:\WINNT\CARDFILE.EXE).
- 4 Double-click the **CardfileCrdFile** entry to open the String Editor dialog box. Then type the path and name of your operators' instructional text file (e.g., C:\INFODATA\INFO.CRD).

Although it is possible to specify a network drive in these steps, we recommend that you place the information file on the OWS PC to assure access in the event of network problems.

Settings for the Directory Manager

- **5** Use the directory configuration utility on the server to set up the directory structure. Re fer to the *Help file* for a description of how to use the directory configuration utility.
- **6** Use the database import utility on the server to set up the initial directory data. Refer to the *Help file* for a description of how to use the database import utility.

Performance

Performance Enhancements

This section introduces steps you can take to improve D.N.A. performance, following system installation. Some of the improvements covered include:

- Creating more available memory (RAM)
- Improving OWS Supervisor performance
- Improving RDS performance

Note Not all of these performance remedies may apply to your situation. You must evaluate these options individually, with respect to your system requirements, system stability, and your own technical capabilities.

RDS Performance

This section provides the following performance remedies and enhancements for the Remote Data Server (RDS).

- Enable/Disable Local Database Integrity Check
- Reduce I/O Completion Ports in Large Systems
- Enable/Disable Incremental LDB Updates from DMG
- Configure RDS to Use Fewer SQL Connections.

LDB Integrity Check Feature (RDS 2.x)

There is a feature in RDS to check the integrity of local databases. By default this feature is set to **OFF**, to activate this feature, set the following NT/2000 Registry key on the D.N.A. Server to 1. Stop and restart RDS to take into account the modified registry flag.

HKEY_LOCAL_MACHINE\SOFTWARE\Ericsson\RemoteDS\Manager\VerifyLDBIndexIntegrity

After each change in Directory Manager, RDS will run an integrity check of the master local database files. If this check is successful, the changes will be synchronized to all client LDBs. This causes RDS to repopulate corrupted local databases whenever it detects DMG updates. This helps prevent corrupted server LDBs from being distributed to client PC's.

Important The disadvantage of enabling this integrity check will be a performance degrade of the server.

Reduce I/O Completion Ports in Large Systems (RDS2.1)

Support I/O Completion Ports in RDS. This allows the D.N.A. administrator to select the option to run RDS to allocate one thread per connected client or to allocate an I/O Completion port per connected client. This option can be selected by toggling the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Ericsson\RemoteDS\Manager\UseMultiThreadedClientCon nections

The default setting for this flag is 1; i.e. use multi-threaded client connections. For installation sites with more than 50 D.N.A. client installations, it is recommended that this flag be set to 0; i.e. use I/O completion ports instead.

For example, in a large system (more than 50 clients), RDS may run 410 threads at normal operation and 650 threads during peak times. With this change, RDS will run at 20 threads at normal operation and 260 threads during peak time. This should improve your server performance.

Note If you choose to change this flag, you must stop and restart RDS to have the change take effect.

Enable/Disable Incremental LDB Updates from DMG

By default, this feature is enabled. Therefore, when DMG makes any updates, RDS broadcasts those updates to all clients; e.g. Operator Workstation. If this feature is disabled, RDS will not broadcast DMG updates until next scheduled LDB update.

To configure the "Incremental Local Database Updates" flag, modify the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Ericsson\RemoteDS\Manager\EnableIncrementalLDBUpdat es

=0: No incremental updates are sent to LDBs. Also, when DMG moves a department, it will not start a repopulation of the related LDB tables. Only scheduled updates will repopulate the LDB with the latest changes.

=1: This is the default setting. The LDBs are updated immediately after a DMG change to the SQL database.

=2: This option enables incremental updates (this is small work for RDS), but with the condition to ignore any updates that force RDS to fully repopulate the LDB. Therefore, when DMG moves or changes the name of a department, RDS will not start the repopulation of related tables. This task is left to the scheduled nightly repopulation routine.

The above settings only effect DMG changes. So if you select configure RDS for maintenance repopulation, it will execute based on the current **EnableIncrementalLDBUpdates** setting. If you choose to change this flag, you must stop and restart the RDS Service to have the changes take effect.

This function is implemented in REMOTEDS.EXE 2.1.016 & REMOTEDS.EXE 3.0.008.

Function =2 is implemented in REMOTEDS.EXE 2.1.021 & REMOTEDS.EXE 3.0.019.

Configure RDS to Use Fewer SQL Connections

System administrators can configure RDS to use fewer SQL connections by sharing the ODBC connections between threads. This feature is only recommended for small installations such as startup packages using a limited number of SQL connections (e.g., when using SQL Workstation 6.50 you have only 15 user connections). You may configure this option by modifying the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Ericsson\RemoteDS\Manager\ShareODBCConnection

This flag is set to default to **0** (Disabled). To activate this option, set the flag to **1** (Enabled). If you choose to change this flag, you must stop and restart the RDS Service to have the changes take effect. This feature is implemented in REMOTEDS.EXE 3.0.009 and REMOTEDS.EXE 2.1.017

Installation Problems

Log Files

The D.N.A. installation program creates two logs that can be used to troubleshoot installation problems. The Detail log contains all operations performed during the installation process. The Summary log contains the final status (success or failure) for each installed component. These ASCII text files can be viewed with the Windows NT/2000 notepad.

Server Installation Logs

Located at: \dna_s\detail.log and \dna_s\summary.log

Client Installation Logs

Located at: \dna_c\detail.log and \dna_c\summary.log

Event Log Messages

The following table lists D.N.A. Server error messages and recommended remedies.

Application	Error Message	Corrective Action
Ericsson ClockSync	1001 Could not load resource library: %1	Initialization error. Verify that the cloksync.III is in the same directory as the service. %1 = file name
Ericsson ClockSync	1001 Could not duplicate thread handle.	Initialization error. Lack of system resources. Reduce the number of running applications and start the service again.
Ericsson ClockSync	1002 Could not create event handle.	Initialization error. Lack of system resources. Reduce the number of running applications and start the service again.
Ericsson ClockSync	1003 Could not open registry key %1, using defaults.	Initialization error. Verify the permission level of the service. Restart the service. %1 = Registry key name.
Ericsson ClockSync	1004 Client is enabled, but server machine name is invalid.	Initialization error. Restart the service.

Technical Guide

Client disabled.

Ericsson ClockSync	1005 Receive broadcasts is enabled, but server machine name is invalid. Receive disabled.	Initialization error. Restart the service.
Ericsson ClockSync	1006 Could not open process token, client disabled.	Initialization error. Lack of system resources. Reduce the number of running applications and start the service again.
Ericsson ClockSync	1007 Could not enable time set privilege for process, client disabled.	Initialization error. Lack of system resources. Reduce the number of running applications and start the service again.
Ericsson Installation	0 %1 unable to connect to database %2.	Refer to database manual for detailed information of database error. Correct the problem per database manual and redo the installation. %1 = Application name. %2 = Database error message.
Ericsson Installation	0 %1 error inserting application %2.	Refer to database manual for detailed information of database error. Correct the problem per database manual and redo the installation. %1 = Application name. %2 = Database error message.
Ericsson Installation	0 %1 error inserting elements %2.	Refer to database manual for detailed information of database error. Correct the problem per database manual and redo the installation. %1 = Application name. %2 = Database error message.
Ericsson Installation	0 %1 error inserting sites %2.	Refer to database manual for detailed information of database error. Correct the problem per database manual and redo the installation. %1 = Application name. %2 = Database error message.

Ericsson Installation	0 %1 number of licensed elements does not match element table.	Refer to database manual for detailed information of database error. Correct the problem per database manual and redo the installation. %1 = Application name. %2 = Database error message.
Ericsson Installation	1000 %1 number of elements in element table does not match site table.	Refer to database manual for detailed information of database error. Correct the problem per database manual and redo the installation. %1 = Application name. %2 = Database error message.
Ericsson Installation	1001 %1 error updating number of element licenses %2.	Refer to database manual for detailed information of database error. Correct the problem per database manual and redo the installation. %1 = Application name. %2 = Database error message.
Ericsson Installation	1002 %1 the element type was not defined.	Refer to database manual for detailed information of database error. Correct the problem per database manual and redo the installation. %1 = Application name. %2 = Database error message.
Ericsson LFS	1000 Could not load resource library.	Initialization error. Verify that the <i>lfs.lll</i> is in the same directory as the service.
Ericsson LFS	1001 Failed to initialize application.	Initialization error. Reduce the number of running applications and restart the service.
Ericsson LFS	1002 Failed to duplicate thread handle.	Initialization error. Reduce the number of running applications and restart the service.
Ericsson LFS	1003 Failed to open named pipe acceptor.	Initialization error. Reduce the number of running

		applications and restart the service.
Ericsson LFS	1004 Failed to initialize database.	Initialization error. Reduce the number of running applications and restart the service.
Ericsson LFS	1005 Failed to set low water mark.	Initialization error. Reduce the number of running applications and restart the service.
Ericsson LFS	1006 Failed to set high water mark.	Initialization error. Reduce the number of running applications and restart the service.
Ericsson LFS	1007 Failed to push module on Ustream.	Initialization error. Reduce the number of running applications and restart the service.
Ericsson LFS	1008 Failed to open reactor.	Initialization error. Reduce the number of running applications and restart the service.
Ericsson LFS	1009 Failed to set security attributes.	Initialization error. Reduce the number of running applications and restart the service.
Ericsson LFS	1010 Failed to create message queue thread.	Initialization error. Reduce the number of running applications and restart the service.

Ericsson LFS1200 Failed to retrieve security
data server name from registry.Initialization error.
Restart the service.Ericsson LFS1201 Failed to initialize security
data server client.Initialization error.
Reduce the number of running
applications and restart the
service.

Ericsson LFS 1200 Cannot retrieve the Run-time error. password format data from the Neither the primary nor the

	local database. Notify the system administrator.	backup databases are available. Password cannot be changed with this condition. Contact your system administrator.
Ericsson LFS	1201 Cannot retrieve the password format data from the server database. Notify the system administrator.	Run-time error. Cannot retrieve data from the primary database. Password cannot be changed with this condition. Contact your system administrator.
Ericsson LFS	1202 Cannot retrieve the user data from the local database. Notify the system administrator.	Run-time error. Neither the primary nor the backup databases are available. Password cannot be changed with this condition. Contact your system administrator.
Ericsson LFS	1203 Cannot retrieve the user data from the server database. Notify the system administrator.	Run-time error. Cannot retrieve data from the primary database. Password cannot be changed with this condition. Contact your system administrator.
Ericsson LFS	1204 Cannot save the new password. The server database is unavailable.	Run-time error. Cannot store data to the primary database. Password cannot be changed with this condition. Contact your system administrator.
Ericsson LFS	1205 Cannot save the new password. Unable to connect to the security data server.	Run-time error. Cannot store data to the primary database, due to communication problems with the security data server. Password cannot be changed with this condition. Contact your system administrator.
Ericsson LFS	1206 Cannot retrieve the user data from the server database. The application may not be installed. Notify the system administrator.	Run-time error. Verify that the application is installed. Reinstall the application, if needed.

Technical Guide

Ericsson LFS	1207 Cannot retrieve the user data from the local database. The application may not be installed. Notify the system administrator.	Run-time error. Verify that the application is installed. Reinstall the application, if needed.
Ericsson LFS	1500 Failed to close message queue normally.	Shutdown error. Notify the system administrator.
Ericsson LFS	1700 Out of memory.	Initialization error. Reduce the number of running applications and restart the service.
Ericsson SDS	1000 Could not load resource library.	Initialization error. Verify that the <i>sds.III</i> is in the same directory as the service.
Ericsson SDS	1001 Failed to initialize application.	Initialization error. Reduce the number of running applications and restart the service.
Ericsson SDS	1002 Failed to duplicate thread handle.	Initialization error. Reduce the number of running applications and restart the service.
Ericsson SDS	1003 Failed to open named pipe acceptor.	Initialization error. Reduce the number of running applications and restart the service.
Ericsson SDS	1004 Failed to initialize database.	Initialization error. Reduce the number of running applications and restart the service.
Ericsson SDS	1005 Failed to set low water mark.	Initialization error. Reduce the number of running applications and restart the service.
Ericsson SDS	1006 Failed to set high water mark.	Initialization error. Reduce the number of running applications and restart the service.

Ericsson SDS	1007 Failed to push module on Ustream.	Initialization error. Reduce the number of running applications and restart the service.
Ericsson SDS	1008 Failed to open reactor.	Initialization error. Reduce the number of running applications and restart the service.
Ericsson SDS	1009 Failed to set security attributes.	Initialization error. Reduce the number of running applications and restart the service.
Ericsson SDS	1010 Failed to create message queue thread.	Initialization error. Reduce the number of running applications and restart the service.
Ericsson SDS	1200 Database server error: %1.	Initialization error. Refer to the database manual for information on database error. Correct the problem per database manual and try again. %1 = Database error message
Ericsson SDS	1201 Failed to connect to database server. Retrying in %1 seconds.	Run-time error. Check whether database server is running and restart, if necessary. %1 = Database error message
Ericsson SDS	1202 Failed to create database server connection thread.	Run-time error. Reduce the number of running applications and restart the service.
Ericsson SDS	1203 Failed reading the database source from the registry. Application type = %1.	Run-time error. Check the content of the registry setting with RDS configuration. Check the access permission to the registry entries with the Registry Editor. %1 = Application type
Ericsson SDS	1500 Failed to close message queue normally.	Shutdown error. Notify the system administrator.

Ericsson SDS	1700 Out of memory.	General error. Reduce the number of running applications and restart the service.
Ericsson UserConfig	1000 Cannot connect to database server %1.	Refer to database manual for detailed information of database error. %1 = Database error message.
Ericsson UserConfig	1001 Cannot open user table %1.	Refer to database manual for detailed information of database error. %1 = Database error message.
Ericsson UserConfig	1002 Cannot update the user %1.	Refer to database manual for detailed information of database error. %1 = Database error message.
Ericsson UserConfig	1003 Cannot delete the user %1.	Refer to database manual for detailed information of database error. Correct the problem per database manual and try again. %1 = Database error message.
Ericsson UserConfig	1004 Cannot reset the user's password %1.	Refer to database manual for detailed information of database error. Correct the problem per database manual and try again. %1 = Database error message.
Ericsson UserConfig	1005 Cannot access the privilege/authority codes %1.	Refer to database manual for detailed information of database error. Correct the problem per database manual and try again. %1 = Database error message.
Ericsson UserConfig	1006 Cannot update the password properties %1.	Refer to database manual for detailed information of database error. Correct the problem per database manual and try again. %1 = Database error message.

Ericsson UserConfig	1007 Cannot load the application table %1.	Refer to database manual for detailed information of database error. Correct the problem per database manual and try again. %1 = Database error message.
Ericsson UserConfig	1008 Cannot load the site table %1.	Refer to database manual for detailed information of database error. Correct the problem per database manual and try again. %1 = Database error message.

D.N.A. Server

Facilities and Services

The D.N.A. Server is the security and support platform for the Dynamic Network Administration (D.N.A.) applications. The D.N.A. Server provides the structural platform for flexible integration of D.N.A. applications. Major components include the Open Database Connectivity (ODBC) module, the Remote Data Server (RDS), the common SQL database, security administration, license management facilities, and a set of comprehensive application support utilities. The D.N.A. Server is a collection of secured facilities and services that provide support and software security for D.N.A. applications. Primary D.N.A. Server facilities and services include:

Security Data Server - The Security Data Server (SDS) provides high-level security in the form of licensing enforcement. SDS references encrypted licensing data to enforce authorized license limits. SDS also accesses data based on Logging Facilities Server requests.

Remote Data Server - Remote Data Server (RDS) is a D.N.A. service module that maintains continuous network database synchronization between PBX nodes, the D.N.A. SQL server, and all D.N.A. local databases.

Logging Facilities Server - When a you attempt to log-on to a D.N.A. application, the Logging Facilities Server (LFS) performs user authentication. LFS attempts to connect to SDS for on-demand access to D.N.A. SQL server security data. If the attempt fails, LFS connects to a local version of the database allowing essential security operations to proceed. When you attempt to access a remote data server (a server on a different network), LFS attempts to validate your access authorization at the remote server.

Time System Interface - D.N.A. Time System Interface (TSI) is an optional D.N.A. service module that connects to an external time monitoring system. TSI allows diversions to be entered in the time monitoring system, transferred to the D.N.A. Directory Manager application, and registered in the D.N.A. Directory database. As well, Message Waiting (MWT) indications can be sent from D.N.A. to the time monitoring system.

Ericsson ECA Scheduler - This service runs on the D.N.A. Server and supports up to 50 nodes.

These support resources are maintained and operated by network administrative and technical specialists. The following diagram illustrates the interaction between these D.N.A. client and server support resources.



Administrative Tools

Administrative tools installed with the D.N.A. Server platform and with individual applications support various system configuration operations. The D.N.A. installation process automatically installs these tools. The following table explains how these utilities are used.

Tool	How It Is Used	Installed On
RDS Configuration	Allows you to configure the Remote Data Server for D.N.A. database and application support roles, including network database synchronization between PBX nodes, the D.N.A. SQL Server, and D.N.A. Local Databases (LDBs).	Server
User Configuration	Provides controls for assigning and managing user descriptions and corresponding application access privileges.	Server
TSS Configuration	Use the D.N.A. Time System Server Configuration Utility to set up and maintain communications and translation settings for Diversion and Message Waiting features.	Server

D.N.A. Server Configuration	Use this D.N.A. Server administrative tool to build and maintain a list of database servers accessible on the network.	Server
SCS Configuration	The Serial Communications Server Utility allows you to manage direct, Telnet, SCS, and third party serial communications port settings.	Server and Client
License Viewer	Allows you to display D.N.A. site license information.	Server
Directory Configuration	Enables you to set up Operator Workstation subscriber directory assistance structures that best meet the needs of organizations they support.	Server
LDAP Configuration	The LDAP Configuration Utility enables you to configure the Lightweight Directory Access Protocol (LDAP) Server from anywhere on the network. It also allows you to add more LDAP directories to be used for searching people over the Internet/intranet from the Operator Workstation application.	Server
LDS Configuration	Allows you to setup other local database servers from one that is already configured.	Server and Client
Operator Configuration	Gives D.N.A. system administrators the ability to assign operators access to various departments within the organization. Determines what department data a given operator can access.	Server
Trunk Manager	Enables you to assign easily recognizable names to incoming trunks for efficient operator identification and routing.	Server
VSI Configuration	Use the D.N.A. Voice System Voice System Interface Configuration Utility to set up and maintain Diversion and Message Waiting communications settings	Server

Technical Guide

	between external Voice Systems and the D.N.A. Voice System Interface (VSI).	
License Administrator	Provides controls for application licenses and corresponding network resource licenses.	Server
Directory Import	For initial population of OWS directory assistance database. Runs on D.N.A. server and selected D.N.A. client workstations.	Server and Client
Directory Export	Use the Export Utility to create . <i>dat</i> text files of Dynamic Network Administration subscriber directory databases. The <i>.dat</i> files can then be imported into another D.N.A. installation with the Directory Import utility.	Server and Client

Changing Users, Servers, and Passwords

As with D.N.A. applications, most D.N.A. Server utilities are protected by access security controls. Access facilities allow you to change logged users, change D.N.A. servers, and change your personal password.

To Change Logged Users

- 1 Select Change Current User on the Application menu.
- 2 When the User Log On dialog box appears, type the new User Name and Password into the corresponding edit boxes. As you type the password, a string of asterisk characters (*******) appears in the Password edit box, one asterisk for each character you type. Both the User Name and Password fields are case-sensitive, and you are allowed only a limited number of attempts.
- 3 Select a local or remote server from the **DNA Server** drop-down list. The initial security authorization check and all subsequent validation actions are directed toward the server you select.
- 4 Click the **OK** button. If the user name and password are valid, the new user will be logged on to the application with the access authorizations permitted in their user profile. If the logon attempt fails, the Logging Facilities Server (LFS) restores the original user as the currently logged on user.

To Change Logged D.N.A. Servers

- 1 Select Change Current User on the Application menu.
- 2 When the User Log On dialog box appears, type the new User Name and Password into the corresponding edit boxes. As you type the password, a string of asterisk characters (*******) appears in the Password edit box, one asterisk for each character you type. Both the User Name and Password fields are case-sensitive, and you are allowed only a limited number of attempts.
- 3 Select a new local or remote server from the DNA Server drop-down list.
- 4 Click the **OK** button. If the user name and password are valid, user authentication and all subsequent actions will be directed to the new server.
To Change Your Password

Your password is your personalized access code that, along with your User Name, D.N.A. uses for verifying your access authorization. Changing your password from time to time is a recommended security precaution that helps prevent unauthorized access.

1 Select Change Password... on the Application menu. The Change Password dialog box is displayed. A user password can be up to 20 characters in length, and is case-sensitive. The **Password Format** box explains minimum character requirements for defining passwords.

Field	Explanation	
Total Length:	Minimum number of characters required for a valid password.	
Alphabetic:	From the Total Length, the minimum number of alphabetic characters required.	
Numeric:	From the Total Length, the minimum number of numeric characters required.	
Non-alphanumeric:	From the Total Length, the minimum number of non-alphabetic characters required. Example of non-alphanumeric characters are: -,&*# etc.	
	a second into the Old Deserve ad edit have	

- 2 Enter your existing password into the **Old Password** edit box.
- 3 Enter your new password into the **New Password** edit box.
- 4 Again, enter your new password into the Confirm New Password field.
- 5 Check your entries and click the **Save** button.

Registry

Registry Settings

The Windows NT/2000 Registry is a database repository for information about a computer's configuration. It is organized in a hierarchical structure of sub-trees and their keys, hives, and value entries. This section explains registry settings that correspond to D.N.A. component properties not found in the GUI.

Operator Workstation Registry Settings

Setting up Subscriptions and Publications in RDS and/or LDS controls the D.N.A. directory servers accessed by Operator Workstation. Use the **RDS Replication** tab in RDS Configuration on your D.N.A. server.

Server Identification

Use the D.N.A. Server Configuration Utility to build and maintain a list of available database servers. Ericsson's Dynamic Network Architecture relies on uniquely identified servers for centralized database and application support services. D.N.A. applications and utilities accessing network servers through security services require user logon and server selection. The Server Configuration Utility allows you to specify names and other attributes for the servers appearing in the User Logon D.N.A. Servers selection list.

LDS Servers

After a D.N.A. Client machine has been removed, the list of LDS servers in the D.N.A. Server must be updated manually by deleting the following registry keys and restarting RDS.

Hkey_Local_Machine\Software\Ericsson\MRS\RemoteDS\RDSClients\NumberOfLDSClients Hkey_Local_Machine\Software\Ericsson\MRS\RemoteDS\RDSClients\LDS000x

RDS will rebuild these registry keys with the correct number of LDS servers.

Maintenance

SQL Database

This section explains SQL database upsizing and maintenance procedures.

Database Upsizing

You can re-size D.N.A. database components to accommodate changes in the network. Use the Resize Database option.

- 1 Re-run the D.N.A. installation and choose the **Resize Database** button on the Ericsson Setup dialog box.
- 2 Choose or enter new space requirements in the Nodes and Extensions for Database, Upsizing Extension Per Node, and Upsizing Performance manager Node Setup dialogs.
- **3** Respond to the remaining prompts and instructions from the installation wizard.

Tasks

You must schedule or perform maintenance tasks such as backing up databases and dumping transaction logs in support of SQL Server database operations. Refer to your SQL server documentation for information on managing these maintenance tasks.

Transaction Log

Important Do not confuse the SQL transaction log with the D.N.A. Transaction Log. These resources serve two unrelated purposes.

Expired message diversions are kept as reference information until being deleted daily. Message Waiting indications are updated daily. Use the SCHEDULE1 on the RDS Schedules tab to schedule daily database clean up for message diversion and message waiting. RDS performs this maintenance routine CheckDB once per day.

The CleanDB Routine

To maintain efficient D.N.A. operation, run CleanDB. CleanDB is an RDS function that deletes unused User-defined Fields (UDFs) and keywords. This routine is performed on a nightly basis. You may reschedule CleanDB from the **RDS Schedules** tab. If you choose to do so, it is recommended that you schedule this task to be run at least once per day.

Logging Facilities Server

When you attempt to log-on to a D.N.A. application, the Logging Facilities Server (LFS) performs user authentication. LFS attempts to connect to SDS for on-demand access to D.N.A. SQL server security data. If the attempt fails, LFS connects to a local version of the database allowing essential security operations to proceed. When you attempt to access a remote data server (a server on a different network), LFS attempts to validate your access authorization at the remote server.

Ovwin.log File

This file records all failed API calls.

Short Message Service

The Short Message Service (SMS) provides the capability to transfer short messages, up to 120 characters, between Short Message Terminals and DECT Mobile Stations via a Short Message Service Center (SMSC). SMSC is connected to the PBX via the IPU board (BusinessPhone) or the NIU board (for the MD110). The procedure to initiate an SMS involves three steps:

- A generic extension is initiated with the license parameter set to SMS.
- The SMS server number is initiated using CXSYI with the SMSN parameter set to the generic extension initiated in previous step.
- Connection between the SMS server and the NIU I/O device is established using MSCOI command.

Extension Manager supports initiation, change, and removal of SMS. An SMS message will continually attempt to send the message to the phone until it is received.

Limitations

You can only send SMS messages from Operator Workstation. Sending an SMS message to more than 1 handset at a time or from one handset to another are not supported. You cannot have the D.N.A. SMS server and another SMS server connected to the PBX at the same time. This is a PBX limitation.

Local Database Compression

The Local Databases used by Operator Workstation can be compressed. If you have WAN links, we recommend you enable this feature. To enable this feature, you have to set the following registry key. This default setting for this flag is 0 (Disabled). Set it to 1 to enable it.

HKEY_LOCAL_MACHINE\SOFTWARE\Ericsson\RemoteDS\Manager\EnableFilexfrCompression

The compression is done just before the Local Database (LDB) files are sent over the network. They are then uncompressed by Operator Workstation right after they are retrieved from the network. Thus, the files can be accessed by Operator Workstation uncompressed.



The machines at both ends must have D.N.A. installed. The supporting components are in the client files in *DNA_C\SHARE\BIN*. Both machines must have the registry value set to 1. You can see when compression is active by watching the file transfers in Remote Data Manager.



Maintenance

Archival Backup

PDM (**not available in BusinessPhone Operator Suite**) creates one archive file for each PBX node that is written to the *Dna_s\Siten\Pmg\Archive* directory on the server PC (where *n* is the node number). Automatic or manual data extraction that exceeds the disk space configured for the primary D.N.A. server traffic measurement database causes the overflow to be extracted to archival flat files. For example, if D.N.A. traffic measurement disk space has been allocated for 3 months of data and you attempt to manually extract 6 months of data, the first 3 month's data will be placed in three separate monthly files, and the most recent 3 month's data are stored in the primary database.

Important It is imperative that there be a minimum of 4 MB of disk space free for each node on the server disk where the *Dna_s* directory resides. To maintain available disk space, the archival files in the *Archive* subdirectory for each node should be periodically backed up to auxiliary storage and deleted from the server disk drive.

The archival files are used when setting up the auxiliary database, and all required files must be in the appropriate directory in order for it to be set up correctly. Therefore, when setting up the auxiliary database, you should restore any required files that were backed up and deleted from disk.

Temporary Workspace

PDM uses local drives for temporary files to store data during data extraction and to display PBX system information. There must be at least 2 MB of free space free on the disk drive where the D.N.A. directory is installed. Be sure to maintain this minimum of 2 MB of free space on the disk drive where the D.N.A. directory is installed.

Database Utility

The purpose of the DNA database utility (*DBCP.EXE*) is to backup/restore DNA application related databases to/from a files running on Microsoft SQL Server 7, Microsoft SQL Server 2000, Desktop Engine, and MSDE. The backup feature provided by SQL Server sometimes may corrupt *ogins/users/ownership* of databases. Therefore, DBCP is preferred as a more secure backup/restore method. Besides, this is the only way to backup databases if MSDE is used.

Options

The Following command line options are available when you execute this console application.

- -B Backup database from SQL server to file
- -D DNA application (All, MRS, DMG, EMG, NPM, or PMG)
- -F Display full path where data file is residing
- -O Change database ownership to D.N.A. default account
- -P User account password, defaults to (blank)
- -R Restore database from file to SQL server
- -U User account name for accessing SQL server (defaults to sa)
- ? Help and usage information

The following table shows what is backed up or restored with the **D** option.

DNA	Backed Up/Restored	
Application	_	
All	All installed DNA databases	
MRS	Dnadfdb emgdb security db_xaction	
DMG	Dirdb	
EMG	SiteX	
NPM	Npmdb	
PMG	Pmglocks auxXpmg siteXpmg	

All will be used, if -D is omitted

Note X indicates the site number.

Capacity and Limitations

This backup/restore utility cannot be stopped while the operation is in progress. It can only be executed on the same machine where Microsoft SQL Server 7, Microsoft SQL Server 2000, Desktop Engine, or MSDE is installed. During the restore process, the target database should not be accessed or connected by other processes or applications.

Troubleshooting

Technical Support

The Troubleshooting book contains information needed to resolve most problems that can occur with the D.N.A. applications. However, there may occur situations in which you are unable to resolve problems

using troubleshooting information. For additional technical assistance, contact your Ericsson representative.

Before Contacting Technical Support

In order to help restore your productivity as rapidly as possible, Ericsson engineers will need the following information.

Versions for:	Windows NT/2000 + Service Pack Level SQL Server + Service Pack Level D.N.A. + Service Pack Status TAU or CT Adapter Revision Level
Local Area Network:	Type of LAN and LAN configuration
System size:	Number of: OWS clients DMG clients Names in subscriber database
If Hotfixes loaded:	Version of "fixed" .exe files (To view, use the Windows NT/2000 Explorer to select and right- click the .exe file, select Properties from the pop-up menu, click the Version tab.
PBX setup:	software release number Any special OWS patches System size (i.e., nodes, extensions, etc.)
Include:	A detailed description of the problem. And although it is not necessary, it will be helpful if you can try to guess the source of the problem and then try to provide Ericsson engineers with detailed information relating to that part of your system.

Reporting Your Problem

To assist our support staff, please obtain the following information before contacting technical support. You should include as much information as is available on system specifications, applications, and the problem itself.

Problem Description

State each problem description clearly and include any available details relating to the problem, including:

- Time-of-day problem occurred
- Operations in progress when the problem occurred
- Applications and/or databases involved
- General type of failure (i.e., transitory, repeatable/non-repeatable, application halt, system halt, etc.) **PBX**

DA

Туре

Version			

No. of Nodes	_	
Operating System Informa	tion (mark all that apply)	
Windows NT/2000 Worksta	ation Windows NT/2000 Server	
Version	Language	
Configuration		
Workgroup	Domain	
Stand Alone	File System	
FAT	NTFS	
Network Protocol (mark al	l that apply)	
NetBUEI	TCP/IP	
IPX/SPX	Other	
None	Software	
PC		
Manufacturer	Model	
CPU	_ Clock Speed	
Memory (RAM)	Hard Disk	
D.N.A. Applications		
Report each application that and which national language	was running when the problem occurr the application supports.	red. Include the version/release level
Application	Version/Release Level	Language Supported
Directory Manager (DMG)		

Extension Manager (EMG) Operator Workstation (OWS)

Other

Event Viewer

D.N.A. applications utilize the event logging facility to record error messages returned from the SQL server. If you encounter database operation difficulties, you can use the Windows NT/2000 Event Viewer to display information for events related to the problem and assist in problem isolation. Event Viewer displays system events registered by Windows NT/2000 and application events recorded by the various applications. Event Viewer can also display events for other PCs on the same network. Refer to the "Windows NT/2000 System Guide" for information about using Event Viewer.

Error Messages

Event ID	Error messages	Corrective Action
1.	- CPBXLINK: InputHandler() cannot get timer capabilities.	Fix PC hardware.
2.	CPBXLINK: Unable to contact the telephone.	Check phone, connection cable, and proper ELU initiation
4.	Unable to open registry key.	Check and correct registry and user permissions.
5.	No response from PBX port.	Check all TAU connecting cables and cycle power on the TAU 2520. This message ONLY appears when Operator Workstation is explicitly configured to use TAU 2520 with ELU5.
6.	Unable to detect a terminal adapter on the PBX port.	Check all TAU connections and COM port assignments.
7.	The terminal adapter reports no PBX connection.	Check connection to the PBX jack on the TAU.
8.	The terminal adapter reports no phone connection.	Check connection to PHONE jack of the TAU.
9	CPBXLINK: SendSignal(%1!s!) failed. GetLastError returned %2!s!.	Restart Operator Workstation. This usually appears if the program is aborted unexpectedly.
10.	Error reading registry value. RegEnumValue() returned %1!s!.	If the returned value is 234, there is a registry value of type REG_SZ longer than 80 characters. Shorten that value.
14.	SetCommState() Failed. GetLastError returned "%1!s!".	Fix COM port configuration or hardware problem.
15.	CreateFile(%1!s!) failed. GetLastError returned "%2!s!".	Fix COM port assignment problem. This can also occur if Operator Workstation is configured to use a non-existing port.
16.	CreateThread() for CCommLink::InputHandler failed. GetLastError return "%2!s!".	Reinstall Windows NT/2000. If error recurs, contact system administrator.
18.	No response from the Operator Workstation keyboard port.	Check Operator Workstation keyboard connection and COM port assignment.

19.	Failed to connect to directory server.	Verify that both the SQL server and D.N.A. Server are installed and running on the server PC.
20.	Failed to open directory database.	Verify that both the SQL server and D.N.A. Server are installed and running on the server PC.
21.	Failed to retrieve subscriber user-defined fields.	Correct database setup using the Directory Configuration utility.
22.	ODBC Error: SQLState: "%1!s!", ODBCError: "%2!s!", NativeError: "%3!s!".	Check SQL and ODBC driver using SQL utilities.
23.	ODBC Information: SQLState: "%1!s!", ODBCInfo: "%2!s!",NativeInfo: "%3!s!"	None (information message)
24.	Warning physical memory is running low.	Either increase memory or close (exit) non-essential programs.
25.	Warning Virtual memory is running low.	Increase the paging file size via the Windows NT/2000 Control Panel. Select System and virtual memory.
26.	Equipment status signal reports telephone is faulty.	Replace the telephone.
27.	Warning Signal Buffer has exceeded 90%	Signals from the PBX and/or the phone are not being processed fast enough. This is usually due to some other process consuming most of the available CPU time. Use the Task Manager to determine which process is at fault and end it.
28.	Warning Operator Workstation will not try to connect to Database. ODBC driver is not installed in registry.	Re-install the D.N.A. Server client software.
29.	Error Signal Buffer Overflow Count	Signals from the PBX and/or phone have been lost. This is an increase of the severity of the problem indicated by event 27. Take the same corrective action.
30.	Error Signal Buffer Overflow Loop Count	The signal buffer pointer has advanced beyond its upper boundary. It is unlikely

that this would occur in the absence of more serious operating system problems.

- 31. Department diversion database connection disconnected. There is a problem with one or more services on the server or the client, or a network problem. Try to stop and restart the Ericsson LFS service on the local machine. Verify that RDS and SDS on the server are running. Verify that the server is reachable over the network.
- 32. External search database connection disconnected. This event is obsolete and not used in D.N.A. 4.0.
- 33. Message and Diversion database connection disconnected.
- 34. Department diversion database connection complete.
- 35. External search database connection complete.
- 36. Message and Diversion database connection complete.

Same as event 31. If these two events (31 and 33) occur independently, there

may be an installation related problem.

None. This is an information message. The absence of this message indicates a service or network problem similar to events 31 and 33.

This event is obsolete and not used in D.N.A. 4.0.

None. This is an information message. The absence of this message indicates a service or network problem similar to events 31 and 33.

Error Messages for SNMP Agent

GetAppSuiteRegInstalled: RegOpenKeyEx failed: 0xnnn

Make sure that the *HKLM\SOFTWARE\Ericsson\DM\AppSuite* registry key actually exists and that system account has permission to read it. Make a note of the error code "0xnnn".

GetAppSuiteRegInstalled: RegQueryValueEx failed: 0xnnn

Make sure that the *HKLM\SOFTWARE\Ericsson\DMI\AppSuite\InstalledAppSuiteComponents* registry key actually exists and that system account has permission to read it. Make a note of the error code "0xnnn".

GetAppSuiteRegState: RegOpenKeyEx failed: 0xnnn

Make sure that the *HKLM\SOFTWARE\Ericsson\DMI\AppSuite* registry key actually exists and that system account has permission to read it. Make a note of the error code "0xnnn".

GetAppSuiteRegState: RegQueryValueEx failed: name 0xnnn

Make sure that the *HKLM\SOFTWARE\Ericsson\DMI\AppSuite\"name*" registry key actually exists and that system account has permission to read it. Make a note of the name and error code "0xnnn".

SetAppSuiteRegInstalled: RegCreateKeyEx failed: 0xnnn

Make sure that the system account has permission to create and/or write registry key *HKLM\SOFTWARE\Ericsson\DM\AppSuite*. Make a note of the error code "0xnnn".

SetAppSuiteRegInstalled: RegSetValueEx failed: 0xnnn

Make sure that the system account has permission to create and/or write registry key *HKLM\SOFTWARE\Ericsson\DM\AppSuite\InstalledAppSuiteComponents*. Make a note of the error code "0xnnn".

SetAppSuiteRegState: RegCreateKeyEx failed: 0xnnn

Make sure that the system account has permission to create and/or write registry key *HKLM\SOFTWARE\Ericsson\DM\AppSuite*. Make a note of the error code "0xnnn".

SetAppSuiteRegState: RegSetValueEx failed: name 0xnnn

Make sure that the system account has permission to create and/or write to registry keys under *HKLM\SOFTWARE\Ericsson\DM\AppSuite\"name"*. Make a note of the name and error code "0xnnn".

AddAppX: GetAppSuiteRegInstalled failed

Make sure that the *HKLM\SOFTWARE\Ericsson\DMI\AppSuite* registry key actually exists and that system account has permission to read it.

AddAppX: SetAppSuiteRegInstalled failed

Make sure that the system account has permission to create and/or write registry key *HKLM\SOFTWARE\Ericsson\DM\AppSuite\InstalledAppSuiteComponents*.

AddAppX: SetAppSuiteRegState failed

Make sure that the system account has permission to create and/or write to registry keys under *HKLM\SOFTWARE\Ericsson\DM\AppSuite*.

RemoveApp: GetAppSuiteRegInstalled failed

Make sure that the *HKLM\SOFTWARE\Ericsson\DMI\AppSuite* registry key actually exists and that system account has permission to read it.

RemoveApp: SetAppSuiteRegInstalled failed

Make sure that the system account has permission to create and/or write registry key *HKLM\SOFTWARE\Ericsson\DM\AppSuite\InstalledAppSuiteComponents*.

Init: AddApp failed: 0xnnn

Make sure that the system account has permission to create and/or write registry key *HKLM\SOFTWARE\Ericsson\DM\AppSuite\InstalledAppSuiteComponents*. Make a note of the application id "0xnnn".

SetAppState: Can't find app: 0xnnn

The function SetAppState was called with an invalid application id. Make a note of the application id "0xnnn".

SetAppState: SetAppSuiteRegState failed

Make sure that the system account has permission to create and/or write to registry keys under *HKLM\SOFTWARE\Ericsson\DM\AppSuite*.

SetModified: Can't find id: 0xnnn

The function SetModified was called with an invalid application ID. Make a note of the application id "0xnnn".

CheckPID: SetAppSuiteRegState failed

Make sure that the system account has permission to create and/or write to registry keys under *HKLM\SOFTWARE\Ericsson\DM\AppSuite*.

GetApps: Map is empty

A list of known applications has been requested and the list was empty. This might or might not be an error.

GetEventType: Can't find id: 0xnnn

The function GetEventType was called with an invalid application ID. Make a note of the application id "0xnnn".

GetEventSeverity: Can't find id: 0xnnn

The function GetEventSeverity was called with an invalid application ID. Make a note of the application id "0xnnn".

GetAppStart: Can't find id: 0xnnn

The function GetAppStart was called with an invalid application ID. Make a note of the application id "0xnnn".

GetAppSuiteServerName: RegOpenKeyEx failed: 0xnnn

Make sure that the *HKLM\SOFTWARE\Ericsson\MRS\CurrentVersion*\ registry key actually exists and that system account has permission to read it.

GetAppSuiteServerName: RegQueryValueEx failed: 0xnnn

Make sure that the *HKLM\SOFTWARE\Ericsson\MRS\CurrentVersion\ServerName* registry key actually exists and that system account has permission to read it.

GetAppSuiteServerID: RegOpenKeyEx failed: 0xnnn

Make sure that the *HKLM\SOFTWARE\Ericsson\MRS\CurrentVersion*\ registry key actually exists and that system account has permission to read it.

GetAppSuiteServerID: RegQueryValueEx failed: 0xnnn

Make sure that the *HKLM\SOFTWARE\Ericsson\MRS\CurrentVersion\ServerID* registry key actually exists and that system account has permission to read it.

GetAppVer: Can't find id: 0xnnn

The function GetAppVer was called with an invalid application ID. Make a note of the application id "0xnnn".

GetAppState: Can't find id: 0xnnn

The function GetAppState was called with an invalid application ID. Make a note of the application id "0xnnn".

Directory Manager

The following table lists error messages displayed by the Directory Manager application that may indicate a setup problem.

Error Message	Corrective Action	
An error occurred while closing the database.	Verify that there is a connection to RDS (Remote Data Server) and the SQL server, and verify that RDS and the SQL server are responding to data retrieval and update requests.	
Cannot get user ID for transaction register entry.	Verify that the D.N.A. Server utilities are running and that Remote Data Server is set up correctly.	
Could not add a new department to the database.	Verify that there is a connection to RDS (Remote Data Server) and the SQL server, and verify that RDS and the SQL server are responding to data retrieval and update requests.	
Could not add extension.	Verify that there is a connection to RDS (Remote Data Server) and the SQL server, and verify that RDS and the SQL server are responding to data retrieval and update requests.	
Could not add the external directory entry.	Verify that there is a connection to RDS (Remote Data Server) and the SQL server, and verify that RDS and the SQL server are responding to data retrieval and update requests.	
Could not connect to the Extension Manager database.	Verify that there is a connection to RDS (Remote Data Server) and the SQL server, and verify that RDS and the SQL server are responding to data retrieval and update requests.	
Could not connect to the transaction database.	Verify that there is a connection to RDS (Remote Data Server) and the SQL server, and verify that RDS and the SQL server are responding to data retrieval and update requests.	
Could not delete subscriber.	Verify that there is a connection to RDS (Remote Data Server) and the SQL server, and verify that RDS and the SQL server are responding to data retrieval and update requests.	
Could not delete the department.	Verify that there is a connection to RDS (Remote Data Server) and the SQL server, and verify that RDS and the SQL server are responding to data	

retrieval and update requests.

Could not delete the external directory entry.	Verify that there is a connection to RDS (Remote Data Server) and the SQL server, and verify that RDS and the SQL server are responding to data retrieval and update requests.
Could not get a valid record ID from IDMSC.	A record in the delete_id table is locked.
Could not retrieve authorization code from the logging services.	Verify that the Management Repository Server utilities are running and that Remote Data Server is set up correctly.
Could not retrieve database source information from the logging services.	Verify that the Management Repository Server utilities are running and that Remote Data Server is set up correctly.
Could not update extension data.	Verify that there is a connection to RDS (Remote Data Server) and the SQL server, and verify that RDS and the SQL server are responding to data retrieval and update requests.
Could not update external directory data.	Verify that there is a connection to RDS (Remote Data Server) and the SQL server, and verify that RDS and the SQL server are responding to data retrieval and update requests.
Could not update subscriber.	Verify that there is a connection to RDS (Remote Data Server) and the SQL server, and verify that RDS and the SQL server are responding to data retrieval and update requests.
Data for the selected department could not be retrieved.	Verify that there is a connection to RDS (Remote Data Server) and the SQL server, and verify that RDS and the SQL server are responding to data retrieval and update requests.
Data for the selected external directory entry could not be retrieved.	Verify that there is a connection to RDS (Remote Data Server) and the SQL server, and verify that RDS and the SQL server are responding to data retrieval and update requests.
Data for the selected subscriber could not be retrieved.	Verify that there is a connection to RDS (Remote Data Server) and the SQL server, and verify that RDS and the SQL server are responding to data retrieval and update requests.

Technical Guide

See your Database Administrator.	A record in the delete_id table is locked.
The department could not be updated.	Verify that there is a connection to RDS (Remote Data Server) and the SQL server, and verify that RDS and the SQL server are responding to data retrieval and update requests.

More Directory Manager Information

- Frequently Asked Questions
- Database Organization

Operator Workstation

This table lists problems that may occur during Operator Workstation operation. It provides an explanation of the probable causes and recommended remedies.

Problem	Possible Cause	Corrective Action
Cannot deliver (send) e-mail messages to D.N.A. subscribers from Operator Workstation.	OWS may not have successfully attached to a MAPI session.	Use the Windows NT/2000 Performance Monitor to check the exchng32.exe and mapisp32.exe processes. See Troubleshooting in E-mail Integration for OWS.
Error dialog box displayed when starting Operator Workstation.	Database settings configured incorrectly. PBX interface problem.	Check D.N.A. Server installation and restart Operator Workstation after correcting database configuration.
		Perform the suggested corrective action and restart Operator Workstation. If the problem recurs, verify the RS- 232C connection between the TAU and the PC by using a breakout box, and verify the line by initiating the line as a digital station and verify that the D3 works on that line.
IRQ conflict or I/O address problem.	Multiple ports or devices assigned the same IRQ (interrupt request), or address settings improperly configured.	Use the <i>winmsd.exe</i> utility in the <i>system32</i> directory for Windows NT/2000 to view IRQ and address settings. Reassign IRQs and/or address settings to resolve conflicts.
Operator Workstation starts, but cannot get any on/off duty indications.	Line initiation or cabling problem.	Verify the RS-232C connection between the TAU and the PC by using a breakout box, and verify the line by initiating the line as a digital station and

verify that the D3 works on that line.

Check the class of service and call origin group for this operator interface in the PBX.

Operator Workstation starts Setup problem. and you can go "on duty" but cannot make or answer calls.

More Operator Workstation Information

- Directory Assistance Databases
- Frequently Asked Questions
- NCOP-OWS
- E-mail Integration

Mobile Executive

The following table contains recovery information for phone error codes.

Symptoms	Error on Phone	Possible Cause
Failed to load Mobile Executive URL	WAP ERR-500 Internal server error	Make sure the <i>MobileDNAObject.dll</i> has been registered and assigned the correct permission (read + execute).
Failed to Logon	WAP ERR-500 Internal server error	Make sure the <i>session.mdb</i> has the correct permission (read + write), and the Mobile Executive logged on user's phone number is assigned in the DMG database.
Failed to Logon	WAP ERR-408 Server timeout …	Make sure SQL server and RDS are running.
Failed to access Personal Number	WAP ERR-408 Server timeout …	Make sure SQL server is running
Failed to update the Personal Number	Error code: xxxx Failed to activate profile!	Make sure EMG is not running in the foreground on the same machine where Mobile Executive is installed, the MD connection is OK, and the SYSTEM user has been added in DNA User Configuration with EMG privileges.
Search results always empty		Make sure RDS is running and LDB files exist in \ <i>DNA_C</i> or <i>DNA_S\DDB\DATA</i> .

More Mobile Executive Information

Phone Setup

Installation

Outlook Integration

Outlook Integration would not start

This problem is caused because Outlook was not installed on the system or there is no Outlook profile created in the logged on user's account.

Make sure Outlook is installed and able to run under the logged on user's account.

Outlook Integration would not logon to the DNA Server

This problem is caused when there is no subscriber entry found with the current computer name defined in the D.N.A. Directory.

Make sure you added the computer name to the subscriber's entry in the D.N.A. Directory.

Diversion information does not match between Outlook Integration and DNA

This problem is caused when the current desktop extension does not match the primary extension of the D.N.A. subscriber entry that has the computer name (or user ID) defined for that subscriber.

Make sure the subscriber entry in the D.N.A. directory has the correct primary extension with the correct computer name (or user ID).

Trouble shooting with Remote Data Monitor

Use the Remote Data Monitor to help determine if the correct messages are transferred between Outlook Integration and RDS. This utility reports Remote Data Service events. You can run REM by doubleclicking on DNA_S\SHARE\BIN\rdm.exe.

Corrected Features

The following corrections are included in this build in addition to previously released builds:

#	Tacos Id	Symptom/Short Description	Comme nt
1	38728	RDSsetup.de based on old version	ln Build2
2	38780	BPCSTA32.DLL cause Rose-wq in Blink	ln Build2
3	39001	BpPbxCom crash / two Clients	In Build2
4	39003	Off duty OWS present diverted call to Operator Queue	In Build2
5	39133	DrWatson from BpPbxCom	ln Build2
6	39028	OWS Dialling	ln Build2
7	39175	BpPbxCom take all PC resources	ln Build2
8	33497	Permission for hey_key_local_machine on W2k	ln Build2

9	38755	Pre Configuration can not create User Privileges	ln Build2
1 0	38756	Registry Setting> Operatorque:Reg-SZ 9 is missing	ln Build2
1 1	38784	RDS can't create new message diversion in BP250	ln Build2
1 2	38794	OPS on W2k BpPbxCom registration	ln Build2
1 3	38969	No Access to Trunk Manager	ln Build2
1 4	39002	LDAP service is missing	ln Build2
1 5			ln Build2
1 6	39833	Operator Console Configuration-Alert Configuration	ln Build3
1 7	39753	Trunk Manager allows only numeric entry	ln Build3
1 8	39762	Help about no SP info	ln Build3
1 9	39823	DDB Configuration license disabled	ln Build3
2 0	39760	Incorrect Version entry in registry	ln Build3
2 1	39759	Problems after remove OPS 5.0	ln Build3
2 2	39781	DNA Pre-Configuration Option window	ln Build3
2 3	39821	Upgrade from OPS4.1	ln Build3

Application Data

Report Generation

Although D.N.A. applications can be used to display and report a wide variety of information, you may want to extract data directly from the application databases and use other applications to manipulate the data or generate reports.

To Generate Reports Using Access

- 1 Click the Attach Table tool on the Access toolbar to attach the SQL Database.
- 2 After selecting SQL Database, Access prompts you for a data source. Select the data source pointing to the SQL server with PBX data.

- 3 Login to the SQL server by entering **thirdpty** as the user ID and password. Click on the **Options** buttons to select a database.
- 4 Select a table from the list and attach all tables that you want to use for your reports.
- 5 Click on the **Query** tab, and then on the **New** button to define a New Query. In order to correctly set the table relations, you should refer to the technical documentation for the specific D.N.A. application.
- 6 After setting the table relationships, run the query and check the results to see if the data is coming back correctly. Click on the ! tool on the toolbar to run the query.
- 7 Once you are satisfied with your query, click on the **Report** tab and then click on the **New** button. Access prompts you with the Database dialog box. Select the query that you defined in the previous steps, and then click on the **Report Wizard** button.
- 8 The report wizard guides you through the steps of defining a report.
- **9** Select the fields and the sort order that you want to include in your report, and define the report style and page orientation.
- **10** The Report Wizard asks you for a report title. After you have entered the title of the report, you can choose to run the report or go to report design view to further customize the report layout.

Directory Manager Database Organization

The following table lists the directory database tables used by D.N.A. applications and utilities.

Table Name	Field Name	Field Type	Max Characters	Description
subscriber	recID	int		record ID
	middle_name	varchar	30	middle name
	absent	bit		subscriber alert
	first_name	varchar	30	first name
	honorary	varchar	30	honorary
	last_name	varchar	30	last name
	options	int		
	primary_extension	varchar	30	ext. number
	primary_nodeID	int		node ID
	record_type	tinyint		
	sort_priority	tinyint		print priority
		int		dept record ID
	main_department_recl	varchar	30	picture file name
	D	varchar	30	alternative spelling
	picture_resid	varchar	30	alternative spelling
	middle_name_alt1	varchar	30	alternative spelling
	middle_name_alt2 middle_name_alt3 middle_name_alt4	varchar	30	alternative spelling
subscriber	first name alt1	varchar	30	alternative spelling
	first_name_alt2	varchar	30	alternative spelling
	first_name_alt3	varchar	30	alternative spelling
	first_name_alt4	varchar	30	alternative spelling
	last_name_alt1	varchar	30	alternative spelling
	last_name_alt2	varchar	30	alternative spelling
	last_name_alt3	varchar	30	alternative spelling
	last_name_alt4	varchar	30	alternative spelling
	udf1_recID	int		UDF record ID
	udf2_recID	int		UDF record ID

	udf3_recID udf4_recID udf5_recID udf6_recID udf7_recID udf8_recID udf9_recID udf9_recID udf10_recID udf11_recID udf11_recID udf13_recID udf13_recID udf15_recID udf15_recID udf16_recID udf17_recID udf17_recID udf17_recID udf19_recID udf19_recID udf20_recID	int int int int int int int int int int		UDF record ID UDF record ID
subscriber	udf1_field udf2_field udf3_field udf4_field udf5_field udf6_field udf7_field udf9_field udf9_field udf10_field udf11_field udf13_field udf15_field udf15_field udf16_field udf18_field udf18_field udf19_field udf19_field udf19_field udf19_field	varchar varchar	$ \begin{array}{c} 160\\ 160\\ 160\\ 160\\ 160\\ 160\\ 160\\ 160\\$	Personal UDF value
department	recID name dept_type_recID parent_recID child_recID udf1_recID udf1_recID udf2_recID udf3_recID udf4_recID sort_priority	int varchar int int int int int int int int int	60	dept. record ID dept. name parent record ID child record ID sibling record ID UDF record ID UDF record ID UDF record ID UDF record ID UDF record ID Sort priority
extension	recID nodeID	int int		ext. record ID node ID

	directory_number options	varchar int		directory number
	primary_user_recID	int		user record ID
site	nodeID sitename nodename remote_nodeID remote_server options	int varchar varchar int varchar int	50 50 30	node ID site name node name remote node ID remote server
numser	recID nodeID start_extension end_extension type options	int int varchar varchar int int	30 30	record ID node ID start extension end extension
keyword	recID value	int varchar	45	record ID text value
external_directory	recID department_recID address listed_number name udf1_recID udf2_recID udf3_recID udf4_recID udf5_recID udf6_recID	int varchar varchar varchar int int int int int int int	160 30 50	record ID dept. record ID address phone number name UDF record ID UDF record ID UDF record ID UDF record ID UDF record ID UDF record ID UDF record ID
field_ definition	recID SQL_type field_name	int tinyint varchar	30	record ID field name
	field_type	tinyint	00	field type
	tield_resid label_name record_type options	varchar varchar tinyint int	30 30	label display
	table_name display_sequence	varchar int	20	display sequence
	UDF_number	int		
	max_data_length	int		personal UDF max length
char_fields	recID value def_char_recID share_count	int varchar int int	45	record ID text value
sub_dept	department_recID subscriber_recID	int int		dept. record ID sub. record ID
sub_ext	extension_recID	int		ext. record ID

	subscriber_recID	int		sub. record ID
sub_key	keyword_recID subscriber_recID	int int		keyword record ID sub. record ID
trunks	recID nodeID trunkID trunk_name options	int int varchar varchar int	20 30	record ID node ID trunk number trunk name display
global_name	groupID	int	30	global group ID
	name	varchar	30	global name
access_codes	recID nodeID exchangeID access_code nodeID_connection remote_server	int varchar varchar int varchar	20 20 30	Table "access codes" for multiple tenants
deleted_id	table_name recID	varchar int	20	deleted table record ID
dept_recid_tmp	recid terminal	int varchar	16	temporary department record ID table
dial_extension_info	recID country_code area_code prefix suffix options numser_recID	int varchar varchar varchar varchar int int	10 10 10 10	extension dialing information
dirdb_info	schema_ver_no created_date released_date database_server database_server_ver_n odbc_ver_no	varchar datetime datetime varchar varchar varchar	30 30 30 30	Directory database version and release information
diversion	recID start_time end_time duration reason_code reason_text cancel_text counter options status is_diverted_recID diversion_type dept_diversion_recID	it datetime datetime int varchar varchar varchar int int tinyint int int int	160 80	Message diversion

	link_diversion_recID	int		
	owner_appID	int		
	repeat_type	int		
	repeat_every	int		
	repeat_type_day_0	int		
	repeat_type_day_1	int		
	repeat_type_day_2	int		
	repeat_type_day_3	datetime		
	repeat_end_time	int		
	oper_div_recID	varchar		
	operatorID		60	
divr	nodeID pbx_reason_code dna_reason_code pbx_description dna_description tdn duration reference method options	int int varchar varchar varchar int varchar varchar varchar int	10 30 1 40 30	Message Diversion Reason Table (Synchronized from extension database by RDS)
	priority	int		
message	recID msg_text cancel_text phone status when_received oper_msg_recID received_recID options operatorID	int varchar varchar tinyint datatime int int int varchar	160 80 30	Message Waiting (incl. E-mail) indication
outbound_dialer	recID userID external_extension sub_extension sub_recID status options name	int varchar varchar varchar int int int varchar	20 30 30	OWS Outbound Dialer dynamic log
reserved_id_table	table_name reserved_flag	varchar int	20	reserved table record ID
ts_trans_codes	portID ts_reason_code reason_code	int varchar varchar	4 1	time system translation codes

	diversion_flag tdn ts_reason_text	varchar varchar varchar	1 1 80	
ts_msg_convert	portID ts_msg_byte msg_byte	int varchar varchar	1 1	time system message conversion
ts_card_no_range	portID start_card_no end_card_no diversion_flag	int varchar varchar varchar	20 20 1	time system card number range
ts_message	recID received_recID msgID card_no portID	int int varchar varchar int	10 20	time system message waiting
user_search_access	recID userID department_recID	int varchar int	20	logged-in user search access
vs_mail_box_no_range	portID start_mail_box_no end_mail_box_no diversion_flag	int varchar varchar varchar	20 20 1	voice system mailbox number range
vs_message	recID received_recID msgID mail_box_no portID	int int int varchar int	20	voice system message waiting
vs_reason_codes	portID reason_code reason_text	int varchar varchar	1 80	voice system reason codes
sub_activation_expiration	subscriber_recID activation_time	int datetime		subscriber to be activated
	expiration time	datetime		time to activate
	options	int		time to expire
	description	varchar	80	description of activation
vs_diversion	rec_ID is_diverted_recID divID	int int int		voice system diversion
	mail_box_no portID	varchar int	20	

More Directory Manager Information

Troubleshooting

Frequently Asked Questions

Extension Manager Database Organization

Table Name	Field Name	Field Type	Max Characters	Default
accnt	accountcode	varchar	15	
	description	varchar	60	null
acdpam	acdnum	smallint		
	acdval	smallint		null
	acdmisopt	smallint		null
acdsup	extno	varchar	5	
acgrp	groupno	varchar	5	
	traffic	smallint		null
	limno	smallint		null
	queuelen	varchar	11	null
	service	varchar	10	null
	selcat	varchar	5	null
	qindchannel	varchar	3	null
	cust	smallint		
	name1	varchar	20	null
	name2	varchar	20	null
	info	varchar	20	null
	pres	varchar	2	null
	sat	smallint		null
	aveconvtime	smallint		null
	bkgroupno	varchar	5	null
acmem	groupno	varchar	5	
	extno	varchar	5	
	clericaltime	smallint		null
	qpriority	smallint		null
	qpritype	smallint		null
adn	extno	varchar	5	
	catno	smallint		null
	traffic	varchar	8	null
	service	varchar	8	null

	calldivcat	varchar	9	null
	routingcat	varchar	6	null
	transcat	varchar	1	null
	addcat	varchar	11	null
	callalt	varchar	1	null
	cust	smallint		null
	name1	varchar	20	null
	name2	varchar	20	null
	info	varchar	20	null
	pres	smallint	2	null
	datype	smallint		null
ancdgrp	ancd	varchar	5	
	lim	smallint		null
	serv	smallint		null
	sel	smallint		null
	traf	smallint		null
	cust	smallint		null
	sat	smallint		null
	maxtim	varchar	4	null
	name1	varchar	20	null
	name2	varchar	20	null
	pres	smallint		
	status	varchar	64	null
ancdmbr	ancd	varchar	5	
	sat	varchar	5	null
	node	smallint		null
	distno	varchar	10	null
	string	varchar	20	null
	startTraf	smallint		null
	status	varchar	64	null
anndesc	annnum	smallint		
	annname	varchar	60	null
apppam	pamnum	smallint		null
	pamval	int		
authcode	authcodeno	varchar	7	

	calllogcode	varchar	6	null
	comcat	smallint		null
	checkcode	smallint		null
	dir	varchar	5	null
	cust	smallint		null
	csp	smallint		null
auxana	extno	varchar	5	
	prianano	varchar	5	null
	auxananext	varchar	5	null
	cat	smallint		null
	traffic	varchar	8	null
	service	varchar	9	null
	calldivcat	varchar	9	null
	routingcat	varchar	6	null
	addcat	varchar	9	null
	icat	varchar	4	null
	transcat	varchar	1	null
	cust	smallint		null
	name1	varchar	20	null
	name2	varchar	20	null
	info	varchar	20	null
	pres	varchar	2	null
bcrelease	bc	int		
bpos	id	char	9	null
callbyname	dir	varchar	20	
	name1	varchar	20	
	name2	varchar	20	
	type	smallint		
	aux	varchar	10	null
cbgrp	groupno	varchar	5	
	traffic	smallint		null
	service	smallint		null
	queuelen	smallint		null
	cust	smallint		null
	name1	varchar	20	null

	name2	varchar	20	null
	info	varchar	20	null
	pres	varchar	2	null
channel	icuind	smallint		
	node	smallint		null
	cho	smallint		null
	status	varchar	64	null
chgrp	groupno	varchar	5	
comabb	comabbno	varchar	5	null
	transno	varchar	26	null
	class	varchar	4	null
	cust	smallint		null
comabbdesc	comabbno	varchar	5	
	description	varchar	60	null
	cust	smallint		null
comabbinfo	comabbno	varchar	5	
	status	smallint		
comdiv	comdivno	varchar	10	null
	divtype	int		null
	cust	smallint		null
compg	pageno	varchar	5	
	searchcode	varchar	5	null
	speechsrcarea	int		null
	pagecat	varchar	3	null
compgm	pageno	varchar	5	
	psano	smallint		
comsrvprf	cspno	int		
	traf	varchar	10	null
	serv	varchar	12	null
	cdiv	varchar	8	null
	roc	varchar	6	null
	npres	varchar	3	null
	desc	varchar	60	null
cordless	extno	varchar	5	
	access	smallint		

	authkey	varchar	8	null
	ipei	varchar	13	null
	authpar	varchar	48	null
corg	operator_id	int		null
	corg_id	smallint		null
	primary_f	tinyint		
cpagrp	cpgrpno	varchar	5	
	cpagrpno	varchar	5	
cpgrp	groupno	varchar	5	
	limno	smallint		null
csta	equ	varchar	11	
cstagrp	cstano	varchar	5	
	odnno	varchar	5	null
	adnno	varchar	5	null
	odnkey	varchar	3	null
	adnkey	varchar	3	null
cstaiodev	iodevice	varchar	14	
	equ	varchar	11	null
	devtype	smallint		null
cstalgrp	linkgroupid	varchar	14	
	iodevice	varchar	14	
custinfo	custno	int		
	custname	varchar	30	null
custmusic	custno	smallint		null
	parkedann	smallint		null
	queuedann	smallint		null
dat	extno	varchar	5	
	tau	smallint		
	datcat	smallint		
	traffic	varchar	8	null
	service	varchar	2	null
	termcat	varchar	10	null
	transcat	varchar	14	null
	routingcat	varchar	2	null
	devtype	varchar	10	null

	modgrp	varchar	5	null
	addcat	varchar	6	null
datapool	dpnum	varchar	5	
	dpgrp	smallint		
	dptype	smallint		
dayn	route	smallint		null
	type	smallint		null
	extno	varchar	5	null
	trunk	varchar	6	null
dcat	catno	smallint		
	traffic	varchar	8	null
	service	varchar	2	null
	termcat	varchar	10	null
	transcat	varchar	14	null
	routingcat	varchar	2	null
	descp	varchar	30	null
deftfunc	insttype	int		null
	keyno	varchar	3	
	ktype	varchar	3	
	kvalue	varchar	5	null
dgrp	groupno	varchar	5	
	traffic	smallint		null
	service	smallint		null
	modemgrpno	varchar	2	null
	disturbinfo	varchar	4	null
dgrpstatus	groupno	varchar	5	
	used	smallint		null
dirpg	pageno	varchar	5	
	searchcode	varchar	5	null
	speechsrcarea	int		null
	pagecat	varchar	3	null
dirpgm	pageno	varchar	5	
	psano	smallint		
dnisnums	dnisnum	varchar	5	
	used	smallint		null

138

dnisused	dnisnum	varchar	5	
	servgrp	varchar	5	
	servtype	smallint		null
	name1	varchar	20	null
	name2	varchar	20	null
	info	varchar	20	null
	pres	varchar	2	null
emdev	emdevnum	smallint		
emdevname	dmdevnum	smallint		
	devname	varchar	60	null
equloc	equpos	varchar	11	
	location	varchar	60	null
extdesc	extno	varchar	5	
	description	varchar	255	null
extinfo	extno	varchar	5	
	type	smallint		null
	status	smallint		null
extpg	pageno	varchar	5	
	searchcode	varchar	5	null
	speechsrcarea	int		null
	pagecat	varchar	3	null
extpgm	pageno	varchar	5	
	psano	smallint		
gdgrp	groupno	varchar	5	
generic	extno	varchar	5	
	csp	int		
	cust	smallint		null
	lim	int		null
	type	int		
	name1	varchar	20	null
	name2	varchar	20	null
	info	varchar	20	null
	pres	varchar	2	null
grprva	grpno	varchar	5	
	welno	smallint		null

	queno	smallint		null
	reqrueno	smallint		null
	cidreqno	smallint		null
	ewta	smallint		null
hgrp	groupno	varchar	5	
	traffic	smallint		null
	queuelen	smallint		null
	limno	smallint		null
	trunkcat	smallint		null
	service	varchar	9	null
	selcat	varchar	3	null
	cust	smallint		null
	name1	varchar	20	null
	name2	varchar	20	null
	info	varchar	20	null
	pres	varchar	2	null
histtaskinfo	taskid	int		
	batchid	int		
	procid	int		
	procinfo	varchar	2048	
	status	smallint		null
	resultdesc	varchar	255	null
hot	hotfrom	varchar	5	
	hotto	varchar	26	null
	hltype	smallint	2	null
icuequ	icuind	smallint		
	equ	varchar	11	null
idiv	idivfrom	varchar	5	
	idivto	varchar	10	null
indabb	extno	varchar	5	
	indabbno	int		
	type	smallint		null
	transno	varchar	26	null
ipext	extno	varchar	5	
	password	varchar	30	null

isdn	dir	varchar	5	
	cat	smallint		null
	traf	varchar	8	null
	serv	varchar	8	null
	cdiv	varchar	9	null
	roc	varchar	6	null
	adc	varchar	8	null
	acctyp	smallint		null
	cust	smallint		null
	name1	varchar	20	null
	name2	varchar	20	null
	info	varchar	20	null
	pres	varchar	2	null
	da	varchar	5	null
ivmbox	vsdno	varchar	5	
	extno	varchar	5	
	vcat	varchar	2	null
	pergr	varchar	2	null
	lang	varchar	2	null
lvmsys	vsdno	varchar	5	
	equpos	varchar	11	
	sideno	varchar	2	null
lang	idx	smallint	5	
	name	varchar	16	
lim	id	smallint		null
marker	taskid	int		
	batchid	int		
	procid	int		
	primkey1	varchar	32	null
	primkey2	varchar	32	null
	viewname	int		
	marked	smallint		
mdmgrp	id	smallint		
mdn	odnno	varchar	5	
	mdnno	varchar	5	

	keyno	varchar	3	
	callalt	varchar	1	null
memgrp	grpno	varchar	5	
	grpmem	varchar	5	
	type	smallint		
	initorder	int		null
mns	odnno	varchar	5	
	mnsno	varchar	5	
	dig	varchar	20	null
msgint	extno	varchar	5	
	term	varchar	5	null
	typeintserpos	smallint		null
odn	extno	varchar	5	
	catno	smallint		null
	traffic	varchar	9	null
	service	varchar	8	null
	calldivcat	varchar	9	null
	routingcat	varchar	6	null
	transcat	varchar	1	null
	addcat	varchar	11	null
	callalt	varchar	1	null
	insttype	varchar	3	null
	cust	smallint		null
	name1	varchar	20	null
	name2	varchar	20	null
	info	varchar	20	null
	pres	varchar	2	null
	datype	smallint		null
	lang	smallint		null
odnadn	adnno	varchar	5	
	odnno	varchar	5	null
	keyno	varchar	3	null
odnfunc	extno	varchar	5	
	keyno	varchar	3	
	ktype	varchar	3	

	value	varchar	5	null
	dig	varchar	20	null
odntaut	tautno	varchar	5	
	odnno	varchar	5	
	keyno	varchar	3	
operator	id	int		
	equpos	char	11	null
pgagrp	grpcodeno	varchar	5	
	pageno	varchar	5	
pgchl	channelno	smallint		
	psano	smallint		
	equ	varchar	11	null
phyequ	equpos	varchar	11	
	boardid	smallint		null
	status	smallint		null
	prodno	varchar	20	null
	rev	varchar	8	null
pninfo	extno	varchar	5	
	profile	smallint		
	position	smallint		
	answerno	varchar	20	null
	timeout	smallint		null
	busygoto	smallint		null
	frinternal	smallint		null
	froperator	smallint		null
	frpublic	smallint		null
	useonce	smallint		null
pnstatus	extno	varchar	5	
	profile	smallint		null
priana	extno	varchar	5	
	auxno	varchar	5	null
	cat	smallint		null
	traffic	varchar	8	null
	service	varchar	9	null
	calldivcat	varchar	9	null

	routingcat	varchar	6	null
	addcat	varchar	9	null
	transcat	varchar	1	null
	insttype	varchar	4	null
	icat	varchar	4	null
	cust	smallint		null
	name1	varchar	20	null
	name2	varchar	20	null
	info	varchar	20	null
	pres	varchar	2	null
psarea	searchareano	smallint		
	blockingtime	smallint		null
	repetitionno	smallint		null
	signaldiagtype	varchar	3	null
	signaldiagvar	varchar	10	null
	holdingtime	varchar	6	null
rfp	bpos	varchar	8	
	rpn	smallint	2	
route	id	smallint		
routrunk	id	char	11	null
	equpos	char	11	null
	route_id	smallint		
rvadata	annnum	smallint		
	rvanum	smallint		
	annfrom	int		null
	annto	int		null
	devtype	smallint		null
rvamsg	msgnum	smallint		
	msgname	varchar	60	null
satgrp	sat	varchar	5	null
	ancd	varchar	5	null
	node	smallint		null
	ofIno	varchar	10	null
	inftyp	varchar	1	null
	ofItim	varchar	4	null
	ovflow	smallint		null
----------	-------------	----------	------	------
sms	extno	varchar	5	
	msgserver	int		
	iodevice	varchar	14	null
spext	extno	varchar	5	
	specexttype	int		null
taskinfo	taskid	int		
	batchid	int		
	procid	int		
	procinfo	varchar	2048	
	status	smallint		null
	resultdesc	varchar	255	null
taufunc	extno	varchar	5	
	keyno	varchar	3	
	value	varchar	5	null
	dig	varchar	20	null
usedext	extno	varchar	5	
	type	smallint		null
	equpos	varchar	11	null
vcat	catno	smallint		
	traffic	varchar	8	null
	service	varchar	9	null
	calldivcat	varchar	9	null
	routingcat	varchar	6	null
	descp	varchar	30	null
vmport	extno	varchar	5	
	portno	varchar	5	
	infocomind	varchar	2	null

More Extension Manager Information

I Troubleshooting

MML Commands

Operator Workstation Data

Directory Assistance Databases

You must use the Directory Configuration Utility to set up directory data structures before using Directory Manager. After using this utility to create directory assistance data structures, you can add contents using Directory Manager or the Directory Import utility.

Application/Utility	Description		
D.N.A. Directory Import Utility	The Directory Import Utility can initialize your directory database with subscriber extension information extracted from PBX hard disk tables or from appropriately formatted ASCII text files.		
D.N.A. Directory Manager Application	Directory Manager is a day-to-day administrative application for both populating and managing the contents of Operator Workstation subscriber records.		

Operator Workstation Configuration

The following notes explain how and where Operator Workstation configuration settings are stored.

How Settings Files are Created

Operator Workstation user configuration and directory configuration settings are stored on Operator Workstation server and client machines. User and directory configuration files are not included with the initial installation of the Operator Workstation application. Instead, these files are created either when a user first makes changes to Operator Workstation settings, or when the user accepts the default settings and logs off Operator Workstation the first time.

Permissions for Changing User and Directory Settings

D.N.A. user permissions, which are controlled by the D.N.A. Server User Configuration Utility, are stored in the security database on the SQL Server. Note that one of the permissions for Operator Workstation is Preferences. The Operator Workstation application checks this setting to determine of the logged user is permitted to make changes to the Operator Workstation settings found under the **Options** menu.

Where to Find Settings Files

User configuration settings are stored in the *username.ows* file, and the directory configuration settings are found in the *username.stg* file. These files are located in the **\Dna_s\Ows\Data** or **Dna_c\Ows\Data** sub-directories, for server and client PCs, respectively.

Operator Console Settings

Operator Console Configuration settings are stored in the Windows NT/2000 Registry under the *HKEY_LOCAL_MACHINE\SOFTWARE\Ericsson\OPI\CurrentVersion* key.

More Operator Workstation Information

- Troubleshooting
- Frequently Asked Questions
- NCOP-OWS

Directory Structures

D.N.A. Directory Structures

Refer to the directory structure illustrations in this section to validate system integrity. These structures represent the D.N.A. server and client directory configurations created by the D.N.A. installation program.

Although the files contained in individual directories may vary from system to system, these fundamental structures must be maintained. Any differences may indicate the need to re-install some or all D.N.A. components.

Directory Manager (Server)



Technical Guide

BusinessPhone Operator Suite 5.0

Administrative Tools (Server)

Technical Guide



149

Operator Workstation (Server)



Directory Manager (Client)



Technical Guide

Administrative Tools (Client)



Operator Workstation (Client)



Frequently Asked Questions

Directory Manager

Question: Directory Manager supports the following checkbox options.

- Show in Visitor Registration OCX
- Show in DNA Directory OCX
- ٠

How are these controls implemented?

Answer: The DNA Directory OCX file (i.e. *DNA_S\Share\bin\DNADir.ocx* or *DNA_C\Share\bin\DNADir.ocx*) is used by many DNA and Non-DNA applications, including Operator Workstation, CCA, PSC, etc. It can also be used by third-party vendors or Web based applications.

When used by third-party vendors, the **Show in DNA Directory OCX** option will enable/disable this display capability for the selected Directory Manager entry.

Question: What does the extension category in Directory Manager stand for?

Answer: In Directory Manager, the extension category is shown in the Subscriber window. When you select an extension from the **Extension to Add** list box, the category is shown in the Category list box. If you add a new extension, you may choose a category for it by using the Category list box. Categories apply to all extensions, not just primary extensions.

The extension category was implemented to integrate Directory Manager and Operator Workstation with PSC. Directory Manager and Operator Workstation treat the extensions the same regardless of their categories. Since Directory Manager or Operator Workstation does not use the extension category, it is not shown at all in Operator Workstation, and it is not shown prominently in Directory Manager. Directory Manager just provides an easy way to assign a category to a new extension so that PSC can use the category.

More Directory Manager Information

- Troubleshooting
- Database Organization

D.N.A. Server

Question: Why do I repeatedly see the warning "PBX watchdog timed out" in the event log?

Answer: This warning shows up if the Ericsson PBX Service is running but does not have a connection to the MD110 via a CT-adapter. If you do not plan to use OWS on your D.N.A. Server you can stop the messages by running the OWS / PBX Extension Line control panel program and set the com port to none.

Question: Is it true that you should not configure a D.N.A. Server as a Primary Domain Controller (PDC)? We have a customer who has made there D.N.A. Server the Wins and PDC on their NT domain for about 60 pc's, we are noticing some very strange things happening on this LAN, Operator Workstation running very slowly etc.

Answer: It has been noted that there are problems if your installation is supporting a fairly large D.N.A. installation with more than 20 operators, you have a lot of changes made to the database, and are using the diversion and messaging facilities.

It is also assumed that you are using a standard 10 M-bit Ethernet LAN with the server connected via a hub. Indeed, such a configuration will exhibit such conditions (as you mentioned) as slow Operator Workstation performance and unpredictable network performance. This is probably due to the fact that making a lot of changes forces RDS to repopulate the database. However, at the same time there are a lot of requests coming in from the clients to the server to get information from SQL.

Initially, it may appear that the problem would be in the server, but this is not necessarily the case. Instead, it is possible that the network card cannot handle the volume of information being sent and received, resulting in traffic collisions and impacted packages. This in turn will further increase the network traffic load because of the increased rate of re-transmissions.

Note A 10Mbit ethernet LAN should never have a network utilization above 30%.

The conclusion, in this case, is that the fewer requests the server's network card must handle the better the performance. You can achieve better performance by either reducing the amount of traffic generated and received by the server and not assign it as a PDC and WINS. Another possible solution would be to change from a hub to a switch for connecting the server to the LAN. This solution provides dedicated bandwidth to and from the server. Alternatively, a 100M-bit network card and port on the hub could also be a solution.

To determine if the problem is the server or the network/network card, run Windows NT/2000 Performance Monitor and use the object "network segment" with counter %network utilization% and object "network interface" with counters Bytes total/sec, Bytes sent/sec, Packets Outbound Discarded and Packets Outbound Errors. This should give an indication of where the problem lies.

Note Try to get the "Windows NT in the Enterprise" course material from Microsoft, where these details are explained.

Wins and Dhcp should not be a problem for 60 PCs. Also, If your PDC only handles logon requests for these 60 PCs, there should be no problem. There exists similar installations and they work fine.

Important Microsoft does state that you should never install SQL on a PDC, as it does affect system performance.

Operator Workstation

Question: How do I setup message diversion to work in a stable way?

Answer: The issue is that it is not always the best idea to put a General Information Communications Interface (GICI) link over the Agent Box. The GICI link is used for Operator Workstation (OWS) messages and diversions. You can have RDS connect with the GICI Access Agent via the Telnet protocol (this Telnet connection is open all the time). However, a problem arises when the network link fails, or the Agent Box is restarted, etc. Windows NT/2000 does not inform D.N.A. that the Telnet connection is lost. This means that when phones are initiating diversions (with *23*x#), the Agent Box cannot deliver data to the Remote Data Server (RDS). The Agent Box does not have a buffer, so the data will be lost. When, on the other hand, Operator Workstation attempts to send a diversion (or message) it will try to contact the Agent Box without success and will re-establish the Telnet connection. The MML connection towards an Agent Box (for Extension Manager) is not so critical, and there is no problem in this area.

Technical Guide

As an intelligent solution you can use the Serial Communications Server (SCS) to connect on one side towards the Remote Data Server (RDS) and on the other side towards an RS-232 connection to the ICUboard. This SCS Server must be a Windows NT/2000 computer that is located near the PABX to setup SCS start the SCS service in Control Panel / Services then run *scssetup.exe*. The communication between RDS and SCS is done via Named Pipes. Windows NT/2000 monitors each Named Pipe and informs the application when a pipe is broken. Then RDS will buffer the Operator Workstation messages and diversions and SCS will buffer the phone diversions. When the network link is re-established all the data will be transferred. (max. down time of link is 24H).

Question: What kind of local databases does Operator Workstation use?

Answer: The LDBs have *.*DAT* and *.*NDX* files (like FoxPro) but they are in an Ericsson specific format. The local database files are a binary tree based design implemented by Ericsson. It is not based on any commercial products. You cannot read it with any 3rd party applications.

To refresh the local databases try to delete the following files: \DNA_C\OP\DATA\ *.DAT and *.NDX and restart Operator Workstation. Do not delete the *.OWS and the *.STG files because they are the configuration files for each user account in Operator Workstation. If the *.DAT and *.NDX files are not rebuilt again you will have a problem with your network or your RDS Service.

To refresh the local databases

- 2 Delete the files \DNA_S\OPI\DATA\ *.DAT (or \DNA_C\OPI\DATA\ *.DAT) and *.NDX
- **3** Restart the Operator Workstation.
- 4 Do not delete the *.OWS and the *.STG files because they are the configuration files for each user account in Operator Workstation. If the *.dat and *.ndx files are not rebuilt again you have some problem with your network or Remote Data Server.

Problem: Operator Workstation application crashes (fails) within 5 hours of startup in a configuration where an English language NT/2000 server is running with a Norwegian NT/2000 workstation.

Solution: The problem is in the default configuration of the Norwegian NT/2000 Workstation and the English NT/2000 Server. When installed, they default to **Disable Distributed COM**.

To solve this problem

- **1** Login as the NT/2000 Administrator.
- 2 Run **DCOMCNFG.EXE**. You should find this file under *WinNT\System32* directory.
- 3 In Default Properties, select **Enable Distributed COM**. Enabling this flag eliminates this Operator Workstation crash problem.

Digital Telephone Set

Question: What are the key assignments for managing calls via the Digital Telephone Set (DTS)?

Answer: This is the key configuration for handling calls via a DTS in D.N.A.

DTS Key OWS Function

Prog	On/Off Duty
Clear	Clear Left and Right
Speaker	Answer incoming call

Access 1	Speech left
Access 2	Speech right
Inquiry	Both-way speech
Transfer	Extend

Question: How does the receipt function in the Operator Workstation messaging dialog box work?

Answer: If a MAPI session has been established, the Snd Rcpt key sends the message with a request for a return receipt. If the recipient's mail system honors the request, the operator's mailbox receives a message when the recipient opens the message from the operator.

If sender and receiver both use the same mail server or post office (i.e. Microsoft Exchange Server or Microsoft Mail with a work group post office) return receipts are quite reliable. If one or both parties use SMTP mail, the results are less reliable.

If the receiver is using Outlook with preview, it is possible for the message to be read without being opened. In that case, the return receipt is not sent until the message is either opened or deleted. If it was read in a preview and then deleted, the return receipt will say that the message was deleted without being read!

Question: What is the function of the Operator Workstation meter key?

Answer: Call metering requires hardware support on the MD110. If the MD110 is equipped with pulse counters and the public exchange uses metered trunks, then the operator can request that trunk calls be metered and get the pulse count (which represents time and charges) when the call ends. The count is displayed in the dial box. If the system does not support metering, pressing the meter key just displays **Meter** in the dial box, and then **VACANT** in the speech window. In this case it is better to program some other function for the key.

Operator Workstation LAN

Question: How much bandwidth is needed for a good performance in the Operator Workstation?

Answer: This is impossible to say without knowing how many subscribers, UDFs, keywords, etc. your database has. Each time your Operator Workstation starts up, it copies the LDB of the server to the clients. If you have the size of the LDB, you know how much data will be copied over the network (only at startup of Operator Workstation and by default at 0200 Hours).

For normal operation, during the day, Operator Workstation does not use much network traffic. This is of course depending on how many changes they do in Directory Manager during the day (changes will be send to the LDB of Operator Workstation client).

Factors other than bandwidth are more likely to cause network performance problems. In particular, be careful about the operating system security setup and the DNS and/or WINS servers. If possible, keep the D.N.A. client machines in the same Domain as the D.N.A. server. Whether your network uses a WINS (Windows Internet Naming Service) server or DNS (Domain Name Service) for address resolution, try to insure that an outage on that server does not adversely affect the D.N.A. machines. Problems with WINS/DNS do not affect Operator Workstation directly, but can become a factor if other applications are used concurrently. For example, something as simple as expanding a subdirectory in the Explorer or the Network Neighborhood can take a ridiculous amount of time if the primary WINS server is offline.

Similarly, the logon and load of the user profile can be delayed as much as 15 minutes when the primary domain controller is down.

The only time when bandwidth may be an issue is immediately after RDS has finished a database repopulation. It then pushes all the new local tables and indices to all its registered clients. Depending on the size of the database and the number of clients, the network (and RDS) can be very busy for a few minutes.

RDS repopulation can be controlled via the RDS configuration utility. Its activity can be monitored (and recorded if desired) with the RDM utility. Both should be available in \DNA_S\MRS\BIN on the DNA server.

More Operator Workstation Information

- Troubleshooting
- Directory Assistance Databases
- NCOP-OWS
- E-mail Integration

Remote Data Server

Question: What is the LOGDB?

Answer: In the \DNA_S\MRS\DATA\RDS directory there is a part of the local database called LOGDB. This part of the database is getting bigger and bigger. It seems that RDS is sometimes very busy updating this file resulting in problems on the Operator Workstation clients. What is this LOGDB used for and why is it getting so big?

LOGDB is the transaction log for RDS's local databases. All the updates to the local databases will be registered in this transaction log, and it is quite natural that it grows as new subscribers are added, deleted, or updated.

Also, updates from messages and diversions are also logged. RDS uses this transaction log to synchronize all the DNA clients. This transaction log gets cleaned up on a nightly basis. Please refer to RDS Configuration Utility - SCHEDULE 2 - Local Database Clean Up Scheduled Audit.

Question: Why is RDS so busy after using Dirpop?

Answer: If you (for example) use dirpop.exe and close Dirpop before it changed anything, you may experience RDS active for about 20 minutes or so and take up substantial CPU time. Each change in Directory Manager is updated in the LDBs (local databases). These LDBs are mainly used by Operator Workstation (plus EMG and LFS).

When Dirpop updates the database, these changes are not transferred to the LDBs during the importing. This would take to much CPU and Network resources. This is why Dirpop gives the command to populate the local databases to RDS when you exit. When you have used Dirpop, RDS has to make sure that the LDBs have the same information as the SQL database. This does take some time and resources, but Dirpop and RDS do not provide any notice to whether you actually changed something or not.

Question: What does "Enable Automatic Data Synchronization from Extension to Directory D.N.A. Database" mean?

Answer: This is a checkbox on the **RDS Options** tab. The Extension Manager database has three tables that need to be queried by RDS for internal purposes. However, since RDS only has access to the Directory Manager database, these three tables should be kept synchronization between Extension Manager and Directory Manager databases.

If this is checked, RDS performs database synchronization with Extension Manager by copying Site, Divr, and Numser tables from EMGDB (Extension Manager side) to DIRDB (RDS side) at startup time. The Site table contains information on sites, the Divr table diversion reason codes, and the Numser table number series. It is checked by default and we highly recommend you to keep it checked.

Question: How does the Standby Remote Data Server work?

Answer: If (for example) RDS crashes, it switches over to the standby side and generates a *DrOhan.log* crash dump file under WINNT directory. You will also get the following message in the Event Log.

E1186 - Remote Data Server Unexpectedly Terminated - Switching Over To Standby Remote Data Server

This log entry indicates that the standby Remote Data Server has taken over the RDS business. The new active RDS spawns for another standby process to monitor it. Unfortunately, the new active RDS is now running as a process and not as a service. This is because it is not possible to run two instances of the same service simultaneously.

Serial Communications Server

Question: Can I run two different diversion systems on one GICI port?

Answer: It could be practical to run two different diversion programs on the same GICI port when introducing a new diversion program. Then you can have old and new running in parallel for a period before switching.

The optional SCS service (a.k.a. GICI Server) in D.N.A. was designed for that purpose. It allows multiple DNA servers to share the same GICI port and it also allows a third party Interception Computer to share the same GICI port. It is however not recommended to run multiple diversion and directory systems due to the overhead in work with updating two systems instead of one.

See Also Configuration

D.N.A. Application Suite

Question: What different releases for D.N.A. exist?

Answer: The following table contains the releases of D.N.A.

Technical Guide

Versi on	Release Information
DNA 3.4	Business Phone Operator Workstation version
DNA 4.1	Business Phone version
DNA 5.0	General release version of DNA5

Registry

Question: What are the following Operator Workstation registry keys used for?

Answers:

HKEY_LOCAL_MACHINE\Software\Ericsson\OPI\CurrentVersion\Number

This key holds a prefix number that will be dialed before the directory number of the subscriber selected in the directory list box. A typical use is to enable an easy way to override diversions.

HKLM\Software\Ericsson\OPI\CurrentVersion\UseAltSpelling

This key is intended to control the display of the closest matched names in the directory. Previous versions of Operator Workstation showed only the first and last names in the directory list box, even when the name that caused the match was an alternate spelling. The default is now to show the name that matched, surrounded with pairs of asterisks. By setting this registry value to 0, the name display reverts to the pre-DNA 4 method.

HKEY_LOCAL_MACHINE \Software\Ericsson\OPI\CurrentVersion\Secrecy

This key holds the feature access code for the Business Phone secrecy feature.

HKEY_LOCAL_MACHINE \Software\Ericsson\OPI\CurrentVersion\ActivateMapiDialog

When this value is set to **1** and MapiResolveName fails the MAPI dialog is displayed to permit the user to choose an email address.

HKEY_LOCAL_MACHINE \Software\Ericsson\OPI\CurrentVersion\SendMessageOnCancel

The default value for SendMessageOnCancel is **1**. When set to **1**, a message is sent when the MAPI Resolve Name dialog box is displayed and the user clicks the **Cancel** button. The ActivateMapiDialog registry item must also be set to **1** to display the MAPI Resolve Name dialog box.

SQL Server

Question: I cannot administer my SQL Server anymore, what to do?

Answer: There have been other cases in which the SQL Server for a D.N.A. system has become difficult or impossible to control by normal methods. In most cases, the trouble begins when the log segment of the syslogs database is running out of space. When that happens, apparently the only command the SQL Server can respond to is "stop".

Sometimes, a simple restart will clear up the problem. That turned out to be the case for a D.N.A. server that had been running continuously for 40 days. (It could not allocate any more pages in *tempdb* that was running in 2MB in RAM.) If the server fails to restart, try starting it from the command line with the /m

(single user mode) and/or the /f (minimally configured mode) options. Then make any necessary repairs and restart normally.

A list of the command line options could be found in the Transact-SQL Reference Help, available under the Help menu of the SQL Server Enterprise Manager.

Click the Search button, then the Find tab. Type in "command line" and scroll down the resulting list to the topic "sqlservr Command-line Executable".

ClockSync

Question: Does anyone know what happens if you have more than one ClockSync Server running on the network? How does a specific client know which ClockSync Server it needs to read? I do not see a computer name in the ClockSync part of the registry.

When you have both a CCM and a D.N.A. server present in one NT/2000 domain, how will the CCM clients know that they need to use CCM server ClockSync, and vice versa for D.N.A. clients?

Answer: It is OK to have multiple ClockSync servers on the network. The ClockSync server on which they were installed will update the clients.

This is defined in the Registry in:

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/ClockSync/Parameters/ServerMachineN ame

The use of Windows NT/2000 named pipes means that the time request event is directed. ClockSync does not use TCP/IP Broadcast packets to send out the time.

If you have two servers (CCM and DNA) each with a ClockSync Server process (EnableServer in the above key is 0x1), you could change one to be a client of the other. For example change CCM server machine to be a ClockSync client of the DNA server, then change all the CCM client machines to ask the DNA server for time updates. If you change the CCM server and not the CCM clients, then they will not get the updates.

Note A ClockSync client cannot also act as a server.

SNMP

Question: I started one or more of the services that are flagged as manual start but they didn't show up in EVM, what's wrong?

Answer: EVM, SNMP and DMI don't know which services are installed until they are started for the first time, due to a limitation in DMI that won't be propagated to EVM if the DMI runtime is already running. The solution is to briefly stop and then restart the CIMgr service. From that point on, all components will be aware of its existence whether it's running or not.

Configuration

Customers

Service Provider Customer Groups

Service provider customers can be divided into two types.

- **Type I** Represents customers that have their own Operator Workstation and require the Service Provider to provide operator functionality through the NCOP-OWS only after working hours. These customers will have their own DNA Server, with DNA Administrative Tools, Directory Manager, and Operator Workstation software installed.
- **Type II** Represents customers that do not have their own Operator Workstation and require the Service Provider to provide operator functionality through the NCOP-OWS. These customers do not have their own DNA Server, and require the Service Provider to configure and manage their directory in the Service Provider DNA Server.

Configuring Type I Customers

After successfully installing Directory Manager, and Operator Workstation server and client installations:

- **1** Run the RDS Configuration Utility.
- 2 In the RDS Options dialog box, disable the **Enable Automatic Data Synchronization From Extension To Directory D.N.A. Databases** option. This prevents RDS from attempting to synchronize data from the extension database to the directory database.
- 3 In the PBX Information dialog box, enable the **PBX Network Setup As Uniform Numbering Plan** option. This will hide the node ID when customers use Directory Manager to assign extensions to their subscribers.
- 4 Click the PBX Site Information Settings >>> button. Add as many PBX MD110 Centrex nodes as the customer's extensions are distributed on. Then, in the PBX Extension Numbering Series Settings >>>, add the appropriate extension ranges the customer is allowed to enter in Directory Manager. (Note that the customer is expected to enter only CDIR extensions, and will not know what EDIR extensions are.) The D.N.A. server is ready for use by the customer.

Note The customer should not have permission to access and modify the RDS Configuration Utility, this is to prevent them from adding extra nodes and extension numbering series.

Configuring Type II Customers

- 1 Run Directory Manager on the Service Provider D.N.A. server.
- 2 Configure the directory for each of the Type II customers. (Note that each Type II customer should be assigned a particular department, and all subscribers that belong to a given Type II customer should be under the same department with their corresponding Customer Node ID (Node ID >= 1000) and CDIR extensions.)

Each of the departments will be later used to identify which customer it is. For example, customers D through Z in the example above can be configured in the Service Provider Directory Manager as departments named "Customer D", "Customer E", etc.

D.N.A. Server

After successfully installing Directory Manager, Operator Workstation, NPM, and other D.N.A. server and client components:

- 1 Run the MD Support Utility and synchronize the MD110 Centrex data to the SP D.N.A. server.
- 2 Run Numbering Plan Manager (NPM) and configure each customer's numbering plan. This information is distributed to the NCOP-OWS clients by RDS on the service provider's D.N.A. Server, to be used for context switching between customer directories, making outgoing calls, identifying incoming calls, etc.

- 3 Run RDS Configuration Utility and in the RDS Options dialog box, make sure that the Enable Automatic Data Synchronization From Extension To Directory D.N.A. Databases option is enabled. This allows RDS to synchronize data between the extension and directory databases.
- 4 In the PBX Information dialog box, disable the **PBX Network Setup As Uniform Numbering Plan** option. This will show the node ID when the service provider uses Directory Manager to assign extensions to subscribers.
- 5 Configure the RDS Replication dialog box. There are two items to configure; **Subscriptions** and **Publications**. Under **Subscriptions** for each Type I customers that have their own D.N.A. server, add subscriptions to their D.N.A. server. Also, add a subscription to the service provider's D.N.A. Server to subscribe the Type II customers.
- 6 Under **Publications**, for each customer add a publication to the subscriptions made above. For customer Type II you need to publish a subscription from the SP D.N.A. server. For example, Customer D needs to be configured as follows:

🗱 RDS Configuration Utility - [Local DNA Server] Ericsson	
<u>Configuration</u> <u>Maintenance</u> <u>View</u> <u>H</u> elp	
2 🖬 ? R?	
RDS Options Message Waiting Options Message Diversion Options GICI Ports RDS Schedules	PBX Information RDS Replication
Subscriptions	
SUBSCRIPTION1 SP DNA Server SUBSCRIPTION2 Customer A DNA Server	Settings >>>
SUBSCRIPTION3 Customer B DNA Server	Add
	Delete
Publications	
	Settings >>>
	Add
	Delete
, Log on success RDS = I	SQL-OD-

The information in the **Customer Name** list box comes from Numbering Plan Manager. If NPM is not installed, this item will be grayed-out. For customer Type I, publish a subscription from that customer's

subscription. If Customer A has more than one D.N.A. server, it is possible to add more than one subscription in the publication. Continue the publication of the rest of the customers.

Serial Communication Server

Use the following procedure to install the Serial Communications Service (SCS). (Note that you must log on as a Windows NT/2000 administrator.)

1 Run and install the D.N.A. client installation program from the service provider's D.N.A. Server. It is important that the SCS Service is installed from the service provider's D.N.A. Server since it needs to access the Numbering Plan Manager database information.

2 Next, run the NT/2000 Control Panel and start **Services.** Set the "StartUp..." of the **Ericsson SCS** entry to **Automatic**. Then start the "Ericsson SCS" NT/2000 service.

3 Next, run the SCS Configuration Utility from the D.N.A._C\SHARE\BIN directory and configure the SCS GICI devices. For each MD110 Centrex GICI communication port, set the Maximum DN Length to **10**. Make sure the Filler Character and Maximum Terminal ID Length matches that of the MD110 Centrex configuration.

4 Next, configure the customer list associated with this GICI port by clicking **Customer List** >>> button. Enter the D.N.A. Server Name of Type I customers and associated customer name. For Type II customers that have their directories maintained on the service provider's D.N.A. Server, enter the service provider's D.N.A. Server Name and select **All Other Customers** as a choice for the customer name.

5 For third party customers that require sharing of the GICI connection, add a "Third Party Connection" and set the **Coupled SCS Device ID**. Configure the customer list by selecting **Customer List** >>> button for the Third Party GICI connection port. In this dialog box, enter any Server Name of the third party customer and associated customer name. (Note that only the first entry in the customer list is used. If you enter more associated customers in the list, these entries will be ignored by SCS; (i.e. only one customer is allowed to be associated to a third party GICI connection).

6 Finally, run the RDS Configuration Utility on the service provider's D.N.A. Server and each of the D.N.A. Servers for Type I customers and configure RDS GICI ports to make SCS Connections. Make sure that you map the correct RDS GICI port to the correct SCS Serial Device. Incorrect mapping may result in GICI messages being sent to the wrong MD110 Centrex PBX.

See Also

Frequently Asked Questions

Web Site Security

If you have installed PPMLite or Ericsson Communication Assistant you may want to set up SSL security for the Web Site. This involves the use of Certificate Authorities (CA). There are several CAs on the Internet that will issue certificates and Verisign (www.verisign.com) is one of the largest. If you are also running Certificate Server (included in Windows NT 4.0 Option Pack 4), you can issue your own server certificate. To request a certificate from a CA, you need to generate a New Key Request from the Key Manager and send it to the CA. To use Key Manager you must have Internet Service Manager and Internet Information Server installed in Windows NT 4.0. This feature is standard in Windows 2000.

Note Client-side browsers will not automatically trust the certificate that you generate since it is not a well-known CA such as Verisign, however they will still work.

Windows NT

To request a certificate from a CA from Windows NT

1 Run the Internet Service Manager by selecting Start ▶ Programs ▶ Windows NT 4.0 Option Pack ▶ Microsoft Internet Information Server ▶ Internet Service Manager.



- 2 In the Microsoft Management Console window directory tree, expand the Internet Information Server directory to display its subdirectories.
- **3** Expand the PPMLite or Ericsson Communication Assistant server directory to display its subdirectories.
- 4 Click on the **PPMLite** or **ECA** directory and click the **Properties** icon in the toolbar.
- 5 Click the Directory Security tab in the <PPMLite or ECA> Properties dialog box.

6	Click the Edit	button under	Secure	Communications.

ca Properties					2
Virtual Directory	Documents Dir	ectory Security	HTTP Head	lers Custom Err	rors
Anonymous	Access and Auther	ntication Control			
\$	Enable anonymous access and edit the authentication methods for this resource.				
- Secure Com	munications				
	Use Key Manager process of receivir	to create a Cerl ng a SSL Certific	ificate Reque ate for this re	st. This starts th source.	e
				Key Managa	er
- IP Address a	nd Domain Name f	Restrictions			
8	Grant or Deny acc Domain Names.	ess to this resou	urce using IP /	Addresses or Inte	ernet
				Edjt	
	ОК	Can	cel	Apply	Help



7 Click the Key Manager... button to run the Key Manager program.

8 In the Key Manager tree, select **WWW** and click **Create New Key...** on the **Key** menu to open the Create New Key wizard. You have two options in the first page of the wizard.

Create New Key	×
	To begin creating a key, you must first target a specific certificate authority. This can be either a remote authority that is accessed through an intermediate file, or a local online authority. If you choose a remote, file based authority, you will be responsible for sending the file and receiving the response. An online authority will be administered automatically. • Put the request in a file that you will send to an authority C:\NewKeyRq.txt Browse • Automatically send the request to an online authority Microsoft Certificate Server Properties
	< <u>B</u> ack <u>N</u> ext > Cancel

- 9 If you selected the Put the request in a file that you will send to an authority option, you will need to send the contents of that file to a CA yourself (or you can use the request to generate your own certificate through Certificate Server). Once you have received the result from the CA, you will need to install that key into Key Manager by selecting WWW in the tree and selecting Install Key Certificate... on the Key menu. It will then ask you for the file that the digital certificate is in. If you received the key by email, you will need to cut & paste the certificate into a text editor such as Notepad and save it to a file.
- **10** If you select the **Automatically send the request to an online authority** option, then a key should appear under the WWW tree in Key Manager. Once the certificate is installed, you need to enable



SSL communication for PPMLite or Ericsson Communication Assistant.

- 11 Exit Key Manager.
- 12 Click Edit... under Secure Communications in the <PPMLite or ECA> Properties dialog box.
- 13 Check Require Secure Channel when accessing this source in the Secure Communications dialog box.

14 Depending on how secure you want your site to be, you can configure client certificates to suit your needs. The default is set to **Do not accept Client Certificates**.

Secure Communications	×
Key Manager is used to create new Key requests and man Key Certificates.	age your installed
Key Manager Encryption Setti	ngs
Require Secure Channel when accessing this resource	
Client Certificate Authentication	
Do not accept Client Certificates	
C Accept Certificates	
Require Client Certificates	
Enable Client Certificate Mapping	
Client Certificates can be mapped to Windows NT User Acco allows access control to resources using Client Certificates.	ounts. This
E <u>d</u> it	
OK Cancel <u>H</u> elp	

15 Click on OK to accept the changes. With SSL security, you preface your URL with https:// instead of the usual http://. For example, change http://www.mysite.com/ppmlite to https://www.mysite.com/ppmlite.

Windows 2000

- 1 To request a certificate from a CA from Windows 2000
- 2 Run the Internet Service Manager by selecting Start ▶ Programs ▶ Administrative Tools ▶ Internet Services Manager.
- **3** In the Internet Information Services window directory tree, expand the server directory to display its subdirectories.

- _ 🗆 × Services <u>A</u>ction <u>V</u>iew • **I** Tree Path Name * 🔁 Scripts d:\inetpub\scripts 🝓 Internet Information Services 🛞 IISHelp d:\winnt\help\iishelp 🗄 🛄 × bt_libra 🛞 IISAdmin 🗄 😴 Default FTP Site D:\WINNT\System32\inetsrv\iisadmin 🗄 🤣 Default Web Site 🛞 IISSamples d:\inetpub\iissamples 🛞 MSADC 🗄 🦪 Administration Web Site d:\program files\common files\system\msadc 🧃_vti_bin 🕀 🌭 Default SMTP Virtual Server D:\Program Files\Common Files\Microsoft Shared\Web Se.. 🛞 CertSrv 🗄 🍥 Default NNTP Virtual Server D:\WINNT\System32\CertSrv 🛞 CertControl D:\WINNT\System32\CertSrv\CertControl 🗟 CertEnroll D:\WINNT\System32\CertSrv\CertEnroll 🛞 TestCert D:\Inetpub\www.root D:\WINNT\web\printers Printers 📃 images 📃 _private 📃 _vti_cnf 🚞 _vti_log 🚞 _vti_pvt 🚞 _vti_script 🗋 __vti__txt 💽 help.gif 0 iisstart.asp 4
- 4 Click on the Default Web Site directory.

5 Open the Properties dialog box by clicking the **Properties** icon **1** on the toolbar.

6 Click the Directory Security tab.

Default Web Site Prope	erties			? ×			
Web Site Operators Directory Security	Performance IS/ HTTP Headers	API Filters H Custom Err	Home Directory	Documents Extensions			
Anonymous access a	nd authentication cor	ntrol					
Enable a authentio	Enable anonymous access and edit the authentication methods for this resource.						
□ IP address and domai	in name restrictions—						
Grant or IP addre	deny access to this r sses or internet doma	esource using in names.					
			Edjt				
Secure communications							
Require enable o	Require secure communications and enable client certificates when this resource is accessed.		<u>S</u> erver Certific	ate			
resource			<u>V</u> iew Certific	ate			
			E <u>d</u> it				
	ок	Cancel	Apply	Help			

- 7 Click the Server Certificate... button under Secure Communications and follow the instructions in the Wizard.
- 8 Open the Secure Communications dialog box by clicking the **Edit...** button under **Secure Communications**.
- 9 Check Require secure channel (SSL).

10 Depending on how secure you want your site to be, you can configure client certificates to suit your needs. The default is set to Ignore Client Certificates.

Secure Communications	×			
Require secure channel (SSL)	1			
Require <u>1</u> 28-bit encryption				
Client certificates				
Ignore client certificates				
C Accept client certificates				
Require client certificates				
Enable client certificate mapping Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates. Edit				
Enable certificate trust list Current CTL: New Edjt				
OK Cancel <u>H</u> elp				

11 Click on OK to accept the changes. With SSL security, you preface your URL with https:// instead of the usual http://. For example, change http://www.mysite.com/ppmlite to https://www.mysite.com/ppmlite.

For More Information See:

How to Configure Certificate Server for Use with SSL on IIS

NCOP-OWS

There is a general market requirement to be able to offer a twenty-four hour seven-day-a-week operator service. Many companies cannot justify the cost of having an operator on site outside of normal working hours, yet there is a market resistance, particularly high in Europe, to the use of answering machines. Network Centralized Operator Workstation (NCOP-OWS) can be a cost-effective way of delivering this type of service, enabling a single operator to support a large number of customers.

NCOP-OWS is intended to offer this service only to customers using service provider-managed PABX solution, based on the Ericsson MD110 Centrex switch with D.N.A. Operator Workstations. There are a number of configurations required to successfully install and manage a NCOP-OWS with a large number of customers. This document is intended to address the D.N.A. administrator's specific needs to successfully configure the NCOP-OWS.

Definitions

SP (Service Provider)

Technical Guide

FID	(Feature Implementation Description)
D.N.A.	(Dynamic Network Administration)
DMG	(Directory Manager)
OWS	(Operator Workstation)
NCOP-OWS	(Network Centralized Operator Workstation)
EMG	(Extension Manager)
PMG	(Performance Manager)
NPM	(Numbering Plan Manager)
RDS	(Remote Data Server)
LDS	(Local Data Server)
SCS	(Serial Communication Server)
EDIR	(Exchange Directory Number)
CDIR	(Customer Directory Number)
LC	(Location Code)

Service Provider Customer Groups

Service provider customers can be divided into two types.

- **Type I** Represents customers that have their own Operator Workstation and require the Service Provider to provide operator functionality through the NCOP-OWS only after working hours. These customers will have their own DNA Server, with DNA Administrative Tools, Directory Manager, and Operator Workstation software installed.
- **Type II** Represents customers that do not have their own Operator Workstation and require the Service Provider to provide operator functionality through the NCOP-OWS. These customers do not have their own DNA Server, and require the Service Provider to configure and manage their directory in the Service Provider DNA Server.

The illustration below represents an example of a Service Provider with Type I and II customers.



Type I customers are represented by customers A, B, and C that have their own DNA servers. Customers D through Z, which are configured on the Service Provider DNA server, represent Type II. The DNA server for customers A, B, and C require that the Administrative Tools, Directory Manager, and OWS software to be installed. The Service Provider DNA server requires all DNA software to be installed. Directory from customers A, B, and C are replicated from their DNA servers to the Service Provider DNA server. Directories for customers D through Z are replicated from the Service Provider central directory into separate local directories (as shown above). The NCOP-OWS uses the replicated directories A through Z to conduct automatic and manual context switching.

Configuring Type I customers

After successfully installing Administrative Tools, Directory Manager, and Operator Workstation server and client installations, run the registry editor (REGEDT32.EXE) on the DNA Server, and set the following registry key to 1.

HKEY_LOCAL_MACHINE\SOFTWARE\Ericsson\RemoteDS\Manager\AllowVirtualNodes

This is a hidden key used to allow the RDS Configuration Utility to add new PBX Node Information, since the customer cannot run MD110 Support to synchronize the PBX Node Information and Extension Numbering Series against the MD110 CENTREX switch.

Next run the RDS Configuration Utility and in the RDS Options dialog box, disable the **Enable Automatic Data Synchronization From Extension To Directory D.N.A. Databases** option. This is to stop RDS from attempting to synchronize data from the extension database to the directory database. In the PBX Information dialog box, enable the **PBX Network Setup As Uniform Numbering Plan** option. This will hide the node ID when customers use Directory Manager to assign extensions to their subscribers.

In the PBX Site Information **Settings** >>>, add as many PBX MD110 CENTREX nodes as the customer's extensions are distributed on, and then in the PBX Extension Numbering Series **Settings** >>>, add the appropriate extension ranges the customer is allowed to enter in Directory Manager.

Note The customer is expected to enter only CDIR extensions, and does not know what EDIR extensions are! The customer should not have permission to access and modify the RDS Configuration Utility, this is to prevent them from adding extra nodes and extension numbering series. Now the DNA server is ready for use by the customer.

Configuring Type II customers

Run Directory Manager on the Service Provider DNA server, and start configuring the directory for each of the Type II customers. Each Type II customer should be assigned a particular department, and all subscribers that belong to a given Type II customer should fall under the same department with their corresponding Customer Node ID (Node ID >= 1000) and CDIR extensions. Each of the particular departments is later used to identify which customer it is.

🎦 Directory Manager - [Local DNA Ser	ver] Ericsson							_ [X
Application Department Subscriber Extern	nal <u>D</u> ata <u>T</u> od	ols <u>V</u> iew <u>H</u> elp)						
T 0 94 R+ R- R. 0+ 0)_ Cq 👘	1- th							
Ericsson Inc.		Last Name	First Name	Middle Name	Hon.	Extension	Department	Cost Center	
H External	1	Einstein	Albert		Dr.	1003:51	Customer D	12345	
	2	Planck	Max		Dr.	1003:52	Customer D	12345	$ \Sigma $
	3						Customer D		Р
									e
		1							s
		1							o
		1							n
Customer J		1							
-Customer K		1							Л
Customer L		1							$\langle \rangle$
Customer M		1							
Customer N		1							F
Customer O		1							n
		1							c
		1							t
		1							i
		1							0
		1							17
		1							K I
		1							
		1							
		1							o
Letter Customer Z	_	1							m
		4) i	
							-302-		

Configuring the SP DNA Server

After successfully installing the Administrative Tools, Directory Manager, Operator Workstation, NPM, and other DNA server and client installations, run MD110 Support and synchronize the MD110 CENTREX data to the Service Provider DNA server. Then run the Numbering Plan Manager (NPM) and configure each customer's numbering plan. This information is used by RDS on the Service Provider DNA server to distribute to the NCOP-OWS clients to be used to context switch between customer directories, making outgoing calls, identifying incoming calls, etc.

Next run the RDS Configuration Utility and in the RDS Options dialog box, make sure that the **Enable Automatic Data Synchronization From Extension To Directory D.N.A. Databases** option is enabled. This is to allow RDS to synchronize data from the extension database to the directory database. In the PBX Information dialog box, disable the **PBX Network Setup As Uniform Numbering Plan** option. This shows the node ID when the service provider uses Directory Manager to assign extensions to their subscribers.

Next, configure the RDS Replication dialog box. There are two items to configure.

- Subscriptions
- Publications

Under the Subscriptions for each Type I customers that have their own DNA server, add subscriptions to their DNA server. Also add a subscription to the Service Provider DNA server itself to subscribe the Type II customers. For example, in the above example, we should subscribe from the Service Provider DNA server and Customer A, B, and C DNA servers.

RDS Configuration Uti	ity - [Local DNA Server] Ericsson 📃 🗐
\underline{C} on figuration \underline{M} a intenance	<u>V</u> iew <u>H</u> elp
🖻 🖬 🤋 🕅	
RDS Options GICI Ports	Message Waiting Options Message Diversion Options PBX Information RDS Schedules RDS Replication
SUBSCRIPTION SUBSCRIPTION	SP DNA Server Settings >>>
SUBSCRIPTION SUBSCRIPTION4	Customer B DNA Server Customer C DNA Server Add
	Delete
Publications	
	Siettings >>>
	Add
	Delete
Log on success	

BDS Configuration Utility - [Local DNA Server] Ericsson	
RDS Options Message Waiting Options Message Diversion Options GICI Ports RDS Schedules	PBX Information RDS Replication
Subscriptions	
SUBSCRIPTION1 SP DNA Server SUBSCRIPTION2 Customer A DNA Server SUBSCRIPTION3 Customer B DNA Server	Settings >>>
SUBSCRIPTION4 Customer C DNA Server	Add
	Delete
Publications	
	Settings >>>
	Add
	Delete

Under the Publications, for each customer add a publication to the subscriptions made above. For customer Type II need to publish a subscription from the Service Provider DNA server.

The information of the **Customer Name** list box comes from the Numbering Plan Manager. If NPM is not installed, then this item will be grayed out. For customer Type I, you need to publish a subscription from that particular customer's subscription.

If Customer A has more than one DNA server, it is possible to add more than one subscription in the publication. Continue the publication of the rest of the customers.

Configuring the NCOP-OWS

After successfully installing Administrative Tools, and Operator Workstation client installations, run the registry editor (REGEDT32.EXE) on the NCOP-OWS client, and set the following registry key to 1.

HKEY_LOCAL_MACHINE\SOFTWARE\Ericsson\OP\CurrentVersion\CentralizedWorkstation

This key is used to indicate that this Operator Workstation client is an NCOP-OWS. Next run the Operator Workstation client and configure the communication ports, user preferences, etc. as you normally configure for a normal Operator Workstation client. Now the NCOP-OWS is ready for use.

To improve the performance of the NCOP-OWS, we recommend you run LDS on the same PC as the NCOP-OWS to help RDS synchronize the directory replications locally to the NCOP-OWS. Use the following procedure to install LDS. You must have logged in with an administrator account to be able to perform the first step successfully.

- 1 Run the Control Panel and start Services. Modify the StartUp... of the Ericsson LDS to Automatic.
- 2 Start the Ericsson LDS service.
- 3 Run the LDS Configuration Utility from the *DNA_C\SHARE\BIN* directory and configure the LDS Replication Subscription and Publication items as you have done in the RDS Configuration Utility when configuring the Service Provider DNA server.
- 4 Run the registry editor (*REGEDT32.EXE*) on the NCOP-OWS client, and set this key to the client computer name that the LDS service and NCOP-OWS is running on.

HKEY_LOCAL_MACHINE\SOFTWARE\Ericsson\LocalDS\LDSServerName

5 Set the following key to 1. This forces NCOP-OWS to connect to LDS on the client NCOP-OWS PC rather than to RDS on the Service Provider DNA server.

HKEY_LOCAL_MACHINE\SOFTWARE\Ericsson\LocalDS\UseLDS

Configuring the SCS

Use the following procedure to install SCS. You must have logged in with an administrator account to be able to perform the first two steps successfully.

- 1 Run Control Panel and start the Services, modify the StartUp... of the Ericsson SCS to Automatic.
- 2 Start the Ericsson SCS service.
- 3 Run the SCS Configuration Utility from the DNA_C\SHARE\BIN directory and configure the SCS GICI devices. For each MD110 CENTREX GICI communication port, set the Maximum DN Length equal to 10. Make sure that the Filler Character and Maximum Terminal ID Length matches that of the MD110 CENTREX configuration.
- 4 Configure the customer list associated with this GICI port by selecting Customer List >>> button. In this dialog box, enter the DNA Server Name of the Type I customers and the associated customer name. For Type II customers that have their directories maintained on the Service Provider DNA Server, enter the Service Provider DNA Server Name and select All Other Customers as a choice for the customer name as shown below.
- 5 For third party customers that require sharing of the GICI connection, add a "Third Party Connection" and set the "Coupled SCS Device ID". Next configure the customer list by selecting "Customer List >>>" button for the Third Party GICI connection port. In this dialog box, enter any Server Name of the third party customer and associated customer name. Note that only the first entry in the customer list is used. If you enter more associated customers in the list, then these entries are will be ignored by SCS; i.e. only one customer is allowed to be associated to a third party GICI connection.
- 6 Next run RDS Configuration Utility on the SP DNA Server and each of the DNA Servers for Type I customers and configure RDS GICI ports to make an SCS Connection. Make sure that you map the correct RDS GICI port to the correct SCS Serial Device. Incorrect mapping may result in GICI messages being sent to the wrong MD110 Centrex PBX.

Performance

After successfully installing D.N.A. client installation with Centrex Operator Workstation option run the Operator Workstation client and configure the communication ports, user preferences, etc. as you normally configure for a normal Operator Workstation client.

To improve the performance of the NCOP-OWS

- 1 Run LDS on the NCOP-OWS PC. This helps RDS synchronize the directory replications locally to the NCOP-OWS. Use the following procedure to install LDS. Note that you must have logged in with an NT/2000 administrator account to be able to perform the first step successfully.
- 2 Run the NT/2000 Control Panel and start **Services**. Set the "StartUp..." of the **Ericsson LDS** entry to **Automatic**. Then start the "Ericsson LDS" NT/2000 service.
- 3 Run LDS Configuration Utility from the *D.N.A._C\SHARE\BIN* directory and configure the LDS Replication Subscription and Publication items as you have done in RDS Configuration Utility when configuring the SP D.N.A. server.
- 4 Run the registry editor (REGEDT32.EXE) on the NCOP-OWS client, and modify the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Ericsson\LocalDS\LDSServerName and set this key to the client computer name that the LDS service and NCOP-OWS is running on. Also modify HKEY_LOCAL_MACHINE\SOFTWARE\Ericsson\LocalDS\UseLDS and set this key to 1. This will force NCOP-OWS to connect to LDS on the client NCOP-OWS PC rather than to RDS on the SP D.N.A. Server. Now the NCOP-OWS is ready for use using LDS.

More Operator Workstation Information

- Troubleshooting
- Directory Assistance Databases
- Frequently Asked Questions

Operator Workstation

E-mail Integration

The Operator Workstation (OWS) application, which is a part of the Dynamic Network Administration (D.N.A.) suite, enables operators to take messages and deliver them via electronic mail systems. Operator Workstation employs Messaging Application Programming Interface (MAPI) functions for preparing and sending messages. Operator Workstation can obtain e-mail addresses from an external messaging system or from the D.N.A. subscriber database.

Due to the variety of e-mail systems and their associated security requirements, a number of factors can prevent Operator Workstation from sending e-mail. It is the intent of this document to explain the requirements that must be met for successful integration of e-mail with Operator Workstation.

Operator Workstation E-mail Requirements

Operator Workstation will send e-mail when it can:

- Load the MAPI library
- Perform a null logon
- Obtain an e-mail address

Loading the MAPI library

Operator Workstation can load the MAPI library if a MAPI-compatible e-mail system has been installed. Microsoft Mail from Windows NT/2000 and Microsoft Exchange satisfy this requirement. Look for *c*:*winnt\system32\mapi32.dll*, or use the Task Manager to determine if the *MAPISP32.EXE* process is running. There may be other MAPI-compatible e-mail systems, but they have not been tested.

Performing a Null Logon

A Windows NT/2000 user ID and password may (or may not) be needed to make a network connection to the work group post office. (If the connection is mapped in the Windows NT/2000 Explorer, be sure to check the "Reconnect at Logon" box.)

The most reliable way of getting the Operator Workstation MAPI logon to succeed is to assign the same user ID to all the accounts an individual operator will use and to start the e-mail client program before Operator Workstation.

VSI and TSS

Voice System Interface

VSI is an ASCII protocol used to establish the serial (RS232) communication between the D.N.A. Serial Communications Server (SCS) and the Host connection of the Integrated Voice Response System (or IVR system). The VSI retrieves or updates Operator Workstation messages and message diversions. This level of integration between Operator Workstation allows Message Diversion Reason and Return Times to be presented by the IVR, without operator intervention.

Setting Up Communications and Configuration Parameters

The VSI user interface allows the system administrator to setup configuration parameters necessary for VSI to establish connections with the IVR (Voice) System. The user interface is similar to that of the Serial Communications Server (SCS) utility. VSI supports a protocol similar to that of TSS or GICI.

The VSI Protocol

As with GICI and TSS, the STX and CR LF characters are used, respectively, for triggering and ending message packages.

STX	Start of Text	ASCII 02
CR	Carriage Return	ASCII 13
LF	Line Feed	ASCII 10
0	End of text msg	ASCII 48
MMMM	Voice Mailbox Number	1-10 characters
RRR	Diversion Reason	000-999
Т	Diversion Type	0 - Non Passive (Divert Phone)
		1 - Passive (Do Not Divert Phone)
SSSS	Start date/time*	12 character format (YYMMDDHHMMSS)
EEEE	End date/time*	12 character format (YYMMDDHHMMSS)
DD	Record ID	00-99
------	------------------------	------------------
KK	Length of Message text	00-80
TEXT	Message text**	0-160 characters
V	Voice Reason ***	0-9
XX	Terminal number	2-5 characters
NN	Number of msgs/div.	00-99
1	First part of text msg	ASCII 49
PPP	PBX Node ID	000-999
Y	Check Sum Byte****	ASCII 32-127

* If the Start and End date/time contains YYMMDD000000 then only the date is specified. If it contains 000000HHMMSS then only the time is specified. If it contains 000000000000 then the default or indefinite date/time is specified.

** Even though the message text maximum is 160 characters, Max field length VoiceDesigner can handle 132 characters. Long messages must therefore be split into two parts. Max (actual) text in one message is 80 characters.

*** 0 = Unknown, 1 = Message Diversion, 2 = Direct forwarding, 3 = Busy, 4 = No answer. These values are configured using VSI Configuration Utility.

**** This is the 7-bit arithmetic sum of all the bytes in the message, disregarding the checksum and the final CR and LF. If the sum is smaller than 20H (32 Decimal), then 20H is added to it.

All messages sent between VSI Service and the receiver should acknowledge the VOICE System. An ACK (06H) must be sent if the received message is correct. A NAK (15H) must be sent if the received message is invalid due to incorrect checksum or missing the end code (i.e. CR LF). In the event the sender did not receive an acknowledgement message within 5 seconds, the sender re-transmits the message.

Sending of acknowledge messages can be deactivated by using the VSI Configuration Utility. For the VSI protocol, it is required that all parts of each message type are included in order to be acknowledged by the Voice System Interface.

All messages sent between VSI Service and the Voice System include a checksum byte. The VSI service can disregard the checksum byte if the checksum option is deactivated using the VSI Configuration Utility. Calculating the checksum is done by a 7-bit arithmetic sum of all the bytes in the message disregarding the checksum and the final CR and LF. If the sum is smaller than 20H (32 Decimal), then 20H is added to it. Following is a C-language example to calculate the checksum.

int checksum(str, len)
char *str;
int len; {
 int sum = 0;

while (len-- > 0)
sum += *str++;
sum &= 0x7f;
if (sum < 0x20)
sum += 0x20;
return (sum);
}</pre>

Capacities and Limitations

It must be possible to setup communication through at least 4 ports simultaneously towards a single voice system. This enables multiple Voice System callers to simultaneously access D.N.A. services. Note that this capacity may be increased in the future.

Also note that more than one voice system may be connected in future releases. In this first version, handling of one Voice System only can be enough. Configuration settings for baud rate, COM port, SCS port etc. should be the same as for the Time System Server (TSS).

Time System Interface

D.N.A. Time System Interface (TSI) is an optional D.N.A. service module that connects to an external time monitoring system. TSI allows diversions to be entered in the time monitoring system, transferred to the D.N.A. Directory Manager application, and registered in the D.N.A. Directory database. As well, Message Waiting (MWT) indications can be sent from D.N.A. to the time monitoring system.

Interface

The time monitoring system is connected to a V.24 (RS-232C) port directly on to D.N.A. Server. Several time monitoring systems can be connected to D.N.A. at once. D.N.A. Time System Interface Module can be configured for 256 connections of each protocol type. In practice, the maximum number of connections is limited to the customer's Windows NT/2000.

Logical Interface

The logical interface between D.N.A. and the various time monitoring systems is defined in CCITT's Rec. V.24. The protocol is defined by a number of signals sent between the time monitoring system and D.N.A. Time System Interface. These signals are composed of a group of characters, each consisting of one start bit, seven to eight information bits, one parity bit, and one stop bit. The information bits are to be coded in accordance with ASCII. Baud rate, seven/eight information bits, parity, XON/XOFF and modem control are selectable.

Protocols

Five different protocols can be applied to the D.N.A. Time System Interface: CTR, GENERAL, FLEXIM, ESMI, and TIMECON. The protocols are grouped into different protocol families: CTR, GENERAL, and TIMECON belong to group 1 and FLEXIM and ESMI belongs to group 2.

Asynchronous RS-232C, 8 data bits, no parity, transfer rate select able. The character code is 7 bit ASCII, with the Finnish special characters code as follows:

Finnish Character Coding

ä { 7B hex ö - 7C hex

- å } 7D hex
- Å [5B hex
- Ö \ 5C hex
- Æ]5D hex

Message Format

<STX><message type><data><BCC><CR><LF>

- STX = 02H, Start of message
- message type = A char which determines how the rest of the message should be interpreted.
- data = Data space
- BCC = The 7-bit arithmetic sum of all the bytes in the message disregarding the checksum itself and the final CR. If the sum is smaller than 20H (32 dec), then 20H is added to it.
- CR = End of message
- LF = Optional

FLEXIM Protocol

The phone switch operator has a FLEXIM info terminal. FLEXIM sends a message to the D.N.A. Time System Interface each time a person logs in or out using his card. The message contains that person's id information (card number, phone number or personal id-number) and in addition the return time (if known), the login/logout time (optional 1) and the validation time (optional 2).

The D.N.A. Time System Interface tells FLFXIM if any person has a call request or some other message. The next time such a person logs in or out, this message will be displayed on the FLEXIM console in plain text form in addition to the time and date when it was entered. A person can have multiple messages in the system at the same time - when the login or logout is completed, all read messages are deleted from the system. A message may contain a maximum of ten 16-character lines.

In addition, FLEXIM sends Time Sync messages to the D.N.A. Time System Interface.

Either end can initiate data transfer. All messages are acknowledged as either correct or faulty. There are two kinds of fault acknowledgement messages: frame error and message error.

Frame error means that the receiver has gotten the beginning code of the message but not the end code, or that the checksum is wrong. The sender must send the message again.

Message error means the receiver has received a message that has a correct length and a correct checksum, but which contains an invalid message. The sender writes an entry about the faulty message in its own log file and continues by sending the next message in line (if any). The faulty message is not re-transmitted.

When the FLEXIM send program starts it first sends the status information of all the people in the system to the receiving end, regardless of what data has been previously transmitted. In the event of a frame error (see above), message re-transmitting is attempted until midnight. If the frame error persists after 00:00 the message is discarded and the system revert back to sending all of the system status information from the beginning. The same situation forms in the event of a takeout. The system waits 5 seconds for an acknowledgement message before retrying.

When the status information for all the people in the system has been successfully sent the program starts sending information on logouts and logins from the program starting time onwards.

Messages sent from FLEXIM to D.N.A. Time System Interface

Login/logout message

STX = Start of message X = Reason code TAB = Field separator X = Phone number / Card number / ID number (field length 1-11,bytes) TAB X = Other Reason code (length 0-3 bytes) TAB DDMM = Return date (4 bytes if specified, otherwise 0) TAB HHMM = Return time (4 bytes if specified, otherwise 0) TAB DDMM = Login/logout date (optional') TAB HHMM = Login/logout time (optional 1) TAB DDMM = Validation date (optional 2) TAB HHMM = Validation time (optional2) BCC = Checksum CR = End of message LF optional 1: Configurable when the system is installed. optional 2: Configurable when the system is installed, contains option I.

Reason Code

2 In

- 3 Out
- 4 Trip in
- 5 Trip out
- 6 Vacation out
- 7 Sick out
- 8 Overtime out
- 9 Other Reason in
- 0 Other Reason out
- a Lunch out

b Personal out

Other Reason is a customer-specified function. Pressing a number and the "Other Reason" key on the FLEXIM terminal uses it. This results in either `0' (In) or `9' (Out) being passed to the info system, with the other reason number (`0' ... `199') in the Other Reason field of the message.

Return date/time is not checked by the system, it is always sent exactly in the form that the user types it in - it is possible to leave incomplete or impossible return times. The return time must be in numeric form. However, in the FLEXIM system the login/logout information and the return date/time information are given separately, so when the user specifies a return date the D.N.A. Time System Interface receives two messages with the same reason code. The second of these contains the return date/time information.

Login/logout time, when sent, is always some time of the on going day. The information is not necessarily sent in a chronological order, however.

Validation date/time comes into play when the so-called "double login/logout" feature of the system is in use, in which the user gives information of a future event using the FLEXIM terminal (for example: "Working overtime today, on a trip tomorrow". The validation field gives the time when the second event becomes valid. In a double-login/logout situation, the D.N.A. Time System Interface may receive up to three consecutive "logout" messages for the same person.

- A logout message-without a validation time or a return time, for example a simple "Out".
- A message with a double-log field, for example "Trip" with a validation time and date of 8:00 AM the next morning.
- A message with all of the information in the previous case and the addition of a return time/date field.

The interval between these messages may be several minutes, and messages from other people may occur between them, naturally.

Examples

Normal Login <STX> 2 <TAB> 150349115E <TAB> <TAB> <TAB> <BCC> <CR>

Normal Logout <STX> 3 <TAB> 150349115E <TAB> <TAB> <TAB> <BCC> <CR>

Trip In <STX> 4 <TAB> 123 <TAB> <TAB> <TAB> <BCC> <CR>

Trip Out + return time <STX> 5 <TAB> 124 <TAB> <TAB> 1507 <TAB> 1530 <BCC> <CR>	

Trip Out + return + log time <STX> 5 <TAB> 124 <TAB> <TAB> 1507 <TAB> 1530 <TAB> 1307 <TAB> 1300 <BCC> <CR>

Trip Out + return + log + validation <STX> 5 <TAB> 124 <TAB> <TAB> 1507 <TAB> 1530 <TAB> 1307 <TAB> 1300 <TAB> <1407> <TAB> 0800 <BCC> <CR>

Vacation + return time <STX> 6 <TAB> 1256 <TAB> <TAB> 1305 <TAB> 0800 <BCC> <CR>

Sick + return time <STX> 7 <TAB> 1115 <TAB> <TAB> 1405 <TAB> 0630 <BCC> <CR>

Overtime Out <STX> 8 <TAB> 1115 <TAB> <TAB> <TAB> <BCC> <CR>

Other Reason + code + return <STX> 0 <TAB> 1503 <TAB> 2 <TAB> 305 <TAB> 1200 <BCC> <CR>

Other Reason + code (In) <STX> 9 <TAB> 890 <TAB> 3 <TAB> <TAB> <BCC> <CR>

Absence deactivate registration

STX = Start of message X = Reason code (2 or 4 or 9) TAB X = Card number TAB TAB TAB TAB TAB TAB TAB CAB BCC = One byte checksum CR = End of message

D.N.A. has only one absent code while FLEXIM has many. Because of this, the field F sent from FLEXIM with the values 2, 4 or 9 are translated by D.N.A. as deactivate absence. It will delete corresponding diversion in D.N.A. that previously was created by the time system diversion originator. Diversions that were created by other diversion originators will only be deactivated.

Absence activate registration: The same as login message.

Reason code sent from FLEXIM with the values 3, 5, 6, 7, 8, A or B will all be translated by D.N.A. Time System Interface as activate absence. It will create a diversion for the corresponding subscriber. The D.N.A. Time System Interface absent code that will be used for the diversion will be defined by the configuration command TRANS.

Since not all fields in a message are required, a message can be composed in several different ways. See the following examples:

<STX> 2 <TAB> 11999 <TAB> <TAB> <TAB> <BCC> <CR>

Deactivate absence for card number 11999. Note three is the minimum number of < TAB> after the card number, even if the message does not contain any more information after the card number.

<STX> 3 <TAB> 2356 <TAB> <TAB> 0312 <TAB> 1445

Activate absence for card number 2356 with return date and time 3 December 14:45. Reason code 3 will be translated to corresponding D.N.A. Time System Interface absent code and assigned to the diversion.

<STX> 0 <TAB> 445577 <TAB> <X> <TAB> 2806 <TAB> 2106 < <TAB> 0732 <BCC> <CR>

Activate absence for card number 445577 with return date 28 June and from date and time 21 June 07:32. Other reason code <X> will be translated to corresponding D.N.A. absent code and assigned to the diversion.

Time Sync messages

STX = Start of message

K = `K' is the Time Sync message type

TAB

YYMMDDHHMMSS = Date and time (12 bytes)

BCC = Checksum

CR = End of message

If the D.N.A. Time System Interface does not respond to a Time Sync message, it is not resent. If the D.N.A. Time System Interface responds with a frame error, the sending of the message is retried (max. three times).

FLEXIM message acknowledgements

Correct: <STX> <A> TAB <id field, as in message> <CR>

Message Error: <STX> <N> <CR>

Frame Error: <STX> <E> <CR>

Note As has been said before, a "Frame Error" message is sent only in case of an error in the message frame (Start/End codes or checksum). A message with a correct frame but bad contents is acknowledged with a "Message Error" message.

If no acknowledgement is received, the message is resent. Retries continue until midnight, at which time a "line down" condition is logged and all status info is resent. The status info is resent until successful, after which normal sending of login/logout messages is resumed.

Messages sent from D.N.A. Time System Interface to FLEXIM

Call requests

STX = Start of message

S = `S' is the Call Request message type

TAB

X = Personal ID field (1-10 chars)

'' = SPACE (optional 3)

MMDDHHMM = Request ID (optional 3)

TAB

message = The message body, max. 16 chars

TAB

```
message = A second message (mix. 10 messages)
```

etc.....

BCC = Checksum

CR = End of message

optional 3: Configurable when the system is installed

The Request ID is equal to the time and date that the message was entered into the system. Using this field, the D.N.A. Time System Interface can sends messages that have an entry time that is different from the current (real) time. The default if to consider the entry time to be the current real time if this field is missing.

Removal of messages

STX = Start of message

P = `P' is the Remove Message message type

TAB

X = Personal ID and optional Message ID as in the Call Request message

BCC = Checksum

CR = End of message

This message causes the removal of all call requests for the given person from the FLEXIM system. If a Message ID is specified, only matching messages are removed.

Removal of all messages

STX = Start of message

P = Remove Message -field type

BCC = Checksum

CR = End of message

This messages causes the removal of all call requests sent by the D.N.A. Time System Interface from the FLEXIM system.

3.1.1.2.4 Init request-

STX = Start of message

I = I' is the Init Request message type

CR = End of message

The FLEXIM system acknowledges the message and sends the status of all the people in the system to the info system.

D.N.A. Time System Interface message acknowledgements

As FLEXIM.

General Protocol

Data messages exchanged between D.N.A. Time System Interface and the time monitoring system are composed by ASCII coded characters. The messages are composed of the following fields

Login/logout message

STX = Start of message

- X = Message type (B or C or D)
- X = Card number (field length 1-11,bytes)
- X = Reason code (A-Z, a-z)
- X = Ignored data (field length 1 byte)
- X = Return time (the length is depending on the message types)
- X = Message waiting indication
- ETX = Start text

BCC = Checksum

- <STX> Start of Text A one byte ASCII code denoting the start position of the text. Each message
 will start with the STX field.
- Message type A one-character message type with the value B, C or D. D.N.A. Time System Interface will ignore messages with other message types. The ignored message will also be acknowledged with ACK.
- Reason Code A one-character absent reason code (A-Z, a-z). The translation table for D.N.A. absence codes will be defined by the configuration command TRANS.
- Ignored data A one-character long data field ignored by D.N.A. Time Information System. (Could hold any value).
- Return Time A four character long number giving the time of return for message type C. This field becomes a six plus four character long number for message type D. See further description of message type D. Interpretation depends on absent reason code given. (DDMM = Day and month. HHMM = Hour and minute.)
- Message Waiting Indication A one character long data field specifying if message-waiting indication should be activated or deactivated.

Technical Guide

- <ETX> Start text A one byte with ASCII character ETX. Each message will start with ETX.
- BCC Checksum A one-byte check character. The check character is calculated as an XQR sum of all characters from F up to and including <ETX> (<STX> is not included).

All messages sent between D.N.A. Time System Interface and the time monitoring system should be acknowledged by the receiver. An ACK must be sent if the received message is correct. A NAK (H15) must be sent if the received message is invalid. Sending acknowledge messages can be deactivated by using the configuration command ACK.

For the General protocol it is required that all parts of each message type are included in order to be acknowledged by the D.N.A. Time System Interface.

Messages sent from General Time Monitoring System to Time System Interface

Arrival and Gone Out Registration STX = Start of message

- B = Message type is set to B
- X = Card number (field length 1-11,bytes)
- X = Reason code (A-Z, a-z), lowercase: arrival, upper case: gone out
- X = Ignored data (field length 1 byte)
- ETX = Start text
- BCC = Checksum

If the absent reason code is a lower case character, the message is considered to be an arrival message. In this case, D.N.A. Time System Interface deletes all old diversions created from the time monitoring system and deactivates all other active diversions.

If the absent reason code is an upper case character, the message is considered to be a gone out registration. D.N.A. Time System Interface creates a diversion with the given absent reason code and a default return time.

Example : <STX>B1234a <ETX>? An arrival message (lowercase a), for card number 1234. (The check character is not calculated correct in the example.)

Gone Out Registration

- STX = Start of message
- C = Message type is set to C
- X = Card number (field length 1-11,bytes)
- X = Reason code (A-Z, a-z). absent reason code.
- X = Ignored data (field length 1 byte)

TTTT = Return time (DDMM or HHMM: 4 bytes if specified, otherwise 0)

ETX = Start text

BCC = Checksum

This message is always a gone out registration. D.N.A. Time System Interface creates a diversion with the given absent reason code and the return time that is specified. Depending on the absent reason code, the TTTT is interpreted either as a time (HHMM = Hour and Minute) or as a date (DDMM = Day and Month). For the time format D.N.A. Time System Interface will use a default date to create a complete return time. For the date format D.N.A. Time System Interface will use a default time when creating the complete return time. The connection between a certain absent reason code and a time/date format is defined during installation.

Gone Out Registration

STX = Start of message

- D = Message type is set to D
- X = Card number (field length 1-11,bytes)
- A = Reason code (A-Z, a-z)
- X = Ignored data (field length 1 byte)
- DDMMYYHHMM = Return time (the length is 10)

ETX = Start text

BCC = Checksum

This message is always a gone out registration. D.N.A. Time System Interface creates a diversion with the given absent reason code and the return time that is specified.

The return time can contain both information about date (DDMMYY) and time (HHMM). If DDMMYY has the value 000000 then no return date is included. D.N.A. Time System Interface will then use the default date for the current absent code. IF HHMM has the value "0000 then no return time is included. D.N.A. Time System Interface will then use the default time. The connection between a certain absent reason code and a default return date/time is defined during installation.

Messages sent from Time System Interface to General Time Monitoring System Message Waiting Indication

STX = Start of message

- C = Message type is set to C
- X = Card number (field length 1-11,bytes)
- M = Set to A if activate, set to B if deactivate
- ETX = Start text
- BCC = Checksum

To activate the message waiting, the M character is set to "A". To deactivate the message waiting, the M character is set to "B". Using the configuration command WAIT can deactivate sending of the message waiting indication.

CTR Protocol

Data messages exchanged between D.N.A. Time System Interface and the CTR Time Monitoring System are composed of ASCII coded characters. The messages are composed of the following fields:

STX = Start of message

- X = Message type (2 digits from 65 to 71)
- X = Card number

X = Absent reason code (0~9)

X = Return time (MMDD or HHMM)

CR

LF

- <STX> Start Text A one-byte field with the ASCII character STX. Each message will start with STX.
- Card Number A four-character long card number. ("0000"-"9999") Card number length is usually defined by the configuration command CARD, but for the CTR system, the card number length is fixed to 4.
- Absent Reason Code A one character absent reason code ("0"-"9"). Translation table for D.N.A. absence codes will be defined by the configuration command TRANS.
- Return Time A four character long number giving the return time. HHMM (MMDD = Month and day, HHMM = Hour and minute.)
- • <CR> Carriage Return A one-byte field with the ASCII character CR.
- • <LF> LF A one-byte field with the ASCII character LF.

Each message sent from the CTR system will end with the combination <CR> <LF>. For the CTR protocol, it is required that all fields of each message are included in order to be acknowledge by the D.N.A. Time System Interface.

Messages sent from the CTR Time Monitoring System to D.N.A.

Arrival Registration

Upon receiving this message from the CTR system, D.N.A. Time System Interface deletes all time monitoring system diversions and deactivate all other active diversions for the given card number.

STX = Start of message 65 = Message type is set to 65 X = Card number CR LF

Gone Out Registrations

Upon receiving this message from the CTR system, D.N.A. Time System Interface will create a diversion with a default absent reason code and a default return time for the given card number.

STX = Start of message 66 = Message type is set to 65 X = Card number CR LF

In this case, D.N.A. Time System Interface will create a diversion with the given absent reason code and a default return time.

STX = Start of message 67 = Message type is set to 65 X = Card number A = Reason code CR LF

D.N.A. Time System Interface will in this case, update a previously created time monitoring system diversion with the specified return time. D.N.A. Time System Interface will use a default date to create a complete return time.

```
STX = Start of message
68 = Message type is set to 68
X = Card number
HHMM = Reason code
CR
LF
```

Update a previously created time monitoring system diversion with the specified return time. D.N.A. Time System Interface will use a default time to create a complete return time.

STX = Start of message 69 = Message type is set to 69 X = Card number MMDD = Return time CR LF

Messages sent from Time System Interface to CTR Time Monitoring System

Sending of these messages can be disabled in D.N.A. Time System Interface by using the configuration command WAIT.

Technical Guide

Deactivate Message Waiting

Upon receipt of this message, D.N.A. Time System Interface will deactivate message waiting for card number X.

STX = Start of message 70 = Message type is set to 70 X = Card number CR LF

Activate Message Waiting

D.N.A. Time System Interface will in this case, activate message waiting for card number X.

STX = Start of message 71 = Message type is set to 71 X = Card number CR LF

ESMI Protocol

The ESMI protocol is in the same protocol family as the FLEXIM protocol.

Messages sent from ESMI Time System To D.N.A. Time System Interface

The message format (absence codes):

```
STX = Start of message
X = Message type (2 or 3 or A or E)
TAB
X = Identification number (1 - 10 digits)
TAB
MS = Reason code for out (1-9: pre-defined. 10-63: free)
TAB
DDMM = Return date (0 to 4 digits)
TAB
HHMM = Return time (0 to 4 digits)
BCC = Checksum
CR
```

Explanation of the records

- STX Start of message (= ASCII 2)
- • X Message type: 2 = in, 3= out, A = reply message ok, E = reply message error
- TAB TAB-mark, works as a separator
- xxxxxx Identification number, length 1 10 digits
- MS Reason code for out (1-2 marks if given, otherwise 0 marks). Explanations used: 1=trip, 2=vacation, 3=sick, 4=health care, 5= business, 6=own, 7=overtime, 8=extended working time, 9=lunch, 10...63 free codes

- • DDMM The return date. 0-4 digits
- • HHMM The return time. 0-4 digits. The date and time of return wouldn't be set if it is not known.
- • BCC Checksum.
- • CR Carriage-Return. In this case the separator won't send anything.

Message will re-transmit after 5 S, if TS won't get any reply. Also if TS-system gets error message, retransmit will be done. Re-transmit will be done only once. If the OK -reply won't come after this, system continues with a new message.

Reason codes in TS-system (in case): All messages will be sent by "in" code.

Out codes: - All reason codes will be in MS field.

Others: Correction message will be sent from TS-system

Reply from the TS-system to D.N.A. Time System Interface

Reply, if the message is OK:

```
STX = Start of message
A = Message type is set to A
TAB
X = Identification number (1 - 10 digits)
CR
```

Reply, if there is an error in the message:

STX = Start of message E = Message type is set to E CR

Messages sent from D.N.A. Time System Interface to ESMI Time System

TS-system terminal setting message:

```
STX = Start of message
S = Message type is set to S (S is TS-system message)
TAB
XXXXXX = Identification number (1 - 10 digits)
TAB
ss...s = Message contents
TAB
ss...s = Message contents
TAB
BCC = Checksum
CR
```

Explanation of the records

STX Start of message (= ASCII 2) X Message type: S = TS terminal message, A = reply message ok, E = reply message error TAB TAB-mark, works as a separator

XXXXXX Identification number, length 1 - 6(10) digits

ss... s TS Terminal message contents, CR or TAB not included. A message can include up to 10 text rows. Since a message row in D.N.A. Time System Interface can be up to 40 characters, these rows will be divided into several text rows. Words longer than 20 characters will be truncated. Overall, length should not exceed 80 characters.

Note Only the first two ss...ss records will be approved as TS-system terminal message, others will not be handled. If ss... ss records are blanks, will the XXXXX persons TS terminal message be removed

BCC Checksum, will be counted by marks (including the STX-mark) sum mod 128, and if the sum is under 20H, there will be added 20H. CR Carriage-Return

Reply from the D.N.A. Time System Interface to TS-system if the message is OK;

```
STX = Start of message
A = Message type is set to A (A is OK)
TAB
XXXXXX = Identification number
CR
Reply, if there is an error in the message:
STX = Start of message
E = Message type is set to E (E is error)
CR
```

TSI systems checking and replies:

Message should start with STX S TAB -marks and checking sum should be right, otherwise error in message -reply will be sent, In case: error in reply, TS-system won't send any error in message -reply.

TIMECON Protocol

The TIMECON protocol is in the same protocol family as the GENERAL protocol.

Stamping Message

The stamping message type: "B" and "C", is equal to the stamping message into GENERAL-protocol. However the return time should be interpreted different than in GENERAL-protoco1 (see below).

Return Time

The return time unit is determined in the contents of this field.

If position (3 & 4) is 01 - 12, it is treated as a date; otherwise as a time, this means that time contains minutes I to 60 and hours 1-24.

Clock Message

TIMECON has a message called clock message, the clock message is repeatedly sent from time system to TSI as an online check. TSI should answer with an <ACK> if this message is OK.

STX = Start of message

```
X = Message type (A or D or Z)

HHMM = Time information

YYMMDD = Date information

EXT

BCC = Checksum

X - Message type is something else than "B" or "C".

TSI algorithm:

IF F in ("A", "D", "Z") THEN Intepret_Clock_Message

HHMM - Time info HHMM

TSI algorithm:

IF ABS (HHMM - D.N.A. Time) > 5 min THEN Logg_Warning

IF ABS (HHMM - D.N.A. Time) > 15 min THEN Logg_Error

YYMMDD Date number starting with a value of 0001 from 76-01-01.

TS-system algorithm: None, ignore this field
```

The time info from TSU will be check and logged as a Warning if it differs 5 - 15 minutes and an error will be logged if it differs more than 15 minutes, it should only log first time it receives a time zone outside D.N.A. time.

It should be possible to change the range value for the invalid time zone, but it will default be 5 min and IS min.

Exchange Interface

The D.N.A. Interface is compatible towards the exchange from ASB50101 R4/1 and later releases of the exchange.

See Also

Introduction

Message Types

There are two types of invalid messages.

Frame error - This means that the receiver has received the beginning code of the message but not the end code, or that the checksum is wrong. The sender must send the message again. This is done when the receiver sends a NAK to the sender.

Message error - The receiver has received a message that has a correct length and correct checksum, but which contains an invalid message. The receiver sends an ACK message to the sender and writes an entry about the faulty message in its own log file or NT/2000 event log. The sender continues sending the next message in line (if any). The faulty message is not re-transmitted by the sender.

IVR/Voice System to VSI Messages

Show information about extension on Operator Workstation ID in Node Number because of Reason Text

Action Request	Command	Example
Show information about MMMM on Operator Workstation XX in node	STX 50 MMMM W XX PPP Y	STX 50 1234 1 99 001 Y CR LF

PPP because of W

CR LF

Initiate Message Diversion Type for extension because of Reason from Start until End with Reason Text.

Action Request	Command	Example
Initiate diversion for MMMM because of RRR from SSSS until EEEE	STX 60 MMMM RRR T SSSS EEEE KK TEXT Y CR LF	STX 60 1234 000 0 961231113000 961231123000 15 "Gone To Lunch" Y CR LF
Delete Message Diversion with	recID for Extension	
Action Request	Command	Example
Delete diversion DD for MMMM	STX 61 MMMM DD Y CR LF	STX 61 1234 01 Y CR LF
View Message Diversion(s) for	Extension	
Action Request	Command	Example
View diversion(s) for MMMM	STX 62 MMMM Y CR LF	STX 62 1234 Y CR LF
Initiate Message Text for Exten	sion	
Action Request	Command	Example
Initiate message TEXT for MMMM	STX 70 MMMM KK TEXT Y CR LF	STX 70 1234 16 "Call home soon" Y CR LF
Delete Message Text for Extens	sion	
Action Request	Command	Example
Delete message DD for MMMM	STX 71 MMMM DD Y CR LF	STX 71 1234 02 Y CR LF
View Message(s) for Extension	I	
Action Request	Command	Example
View message(s) for MMMM	STX 72 MMMM Y CR LF	STX 72 1234 Y CR LF
Download all Message Diversion	ons and Messages from D.N.A.	
Action Request	Command	Example
Database Synchronization Message	STX 90 Y CR LF	This message is sent from VOICE System to VSI Service to download all messages and diversions from the D.N.A. Server to VOICE System. This is used to synchronize database information between both systems when VOICE System restarts.
View (synchronize) D.N.A. syst	em time	
Action Request	Command	Example
Time Synchronization Message	STX 91 YYMMDDHHMMSS Y CR LF	This allows VSI Service to check the local date/time of the

D.N.A. Server against the local date/time of the VOICE system. If local date/time deviates more than 1 minute and less than 10 minutes, then VSI Service prompts a warning message in the D.N.A. Server NT/2000 event log. If local date/time deviates more than 10 minutes, then VSI Service prompts an error message in the D.N.A. Server NT/2000 event log.

IVR/Voice System from VSI Messages

Start of showing Message Diversion(s) for Extension that has Number of Message Diversions

Action Request	Command	Example
Start of showing message diversion(s) for MMMM that has NN diversions	STX 10 MMMM NN Y CR LF	See below
Show Message Diversion with	recID for Extension	
Action Request	Command	Example
Show diversion DD for MMMM	STX 11 MMMM DD RRR T SSSS EEEE KK TEXT Y CR LF	See below
End of showing Message Dive	rsion(s) for Extension	
Action Request	Command	Example
End of showing diversion(s) for MMMM	STX 12 MMMM Y CR LF	(1234 has 2 diversions, lunch (0) 11:30-12:30 and vacation (7) June 25th until July 12th)
		STX 10 1234 02 Y CR LF
		STX 11 1234 01 000 0 961231113000 961231123000 15 "Gone To Lunch" Y CR LF
		STX 11 1234 02 007 0 960625000000 960712000000 25 "Vacation To The Bahamas" Y CR LF
		STX 12 1234 Y CR LF
Activate Message Diversion fo	r Extension	
Action Request	Command	Example
Activate diversion for MMMM	STX 13 MMMM DD PPP RRR T SSSS EEEE KK TEXT Y CR LF	STX 13 1234 01 001 000 0 961231113000 961231123000 15 "Gone To Lunch" Y CR LF

Deactivate Message Diversion for Extension				
Action Request	Command	Example		
Deactivate diversion for MMMM	I STX 14 MMMM Y CR LF	STX 14 1234 Y CR LF		
Start of showing Message(s) for	or Extension that has Number	of Messages		
Action Request	Command	Example		
Start of showing message(s) for MMMM that has NN messages	r STX 20 MMMM NN Y CR LF	See below		
Show Message with Number o	f characters with recID for Exte	ension		
Action Request	Command	Example		
Show message DD for MMMM	STX 21 MMMM DD KK TEXT 1 Y CR LF	See below		
	or			
	STX 21 MMMM DD KK TEXT 0 Y CR LF)		
End of showing Message(s) fo	r Extension			
Action Request	Command	Example		
End of showing message(s) for MMMM	STX 22 MMMM Y CR LF	(1234 has 2 messages, first with 130 characters, second only few)		
		STX 20 1234 02 Y CR LF		
		STX 21 1234 01 80 "This message contains information		

about this and that, especially that. Please" 1 Y CR LF STX 21 1234 01 50 " remember that this is a year small

that this is a very small example only" 0 Y CR LF

STX 21 1234 02 15 "Short message" 0 Y CR LF

STX 22 1234 Y CR LF

Indicate that Extension has a Message Waiting Indication

Action Request	Command	Example	
Indicate message waiting indication for MMMM	STX 23 MMMM Y CR LF	STX 23 1234 Y CR LF	
Erase the Message Waiting	Indication for Extension		
Action Request	Command	Example	

Erase message waiting STX 24 MMMM Y CR LF STX 24 1234 Y CR LF indication for MMMM

Time System Interface

Note: This functionality is a MD110 specific feature and is not fully verified with BusinessPhone Communication System.

D.N.A. Time System Interface (TSI) is an optional D.N.A. service module that connects to an external time monitoring system. TSI allows diversions to be entered in the time monitoring system, transferred to the D.N.A. Directory Manager application, and registered in the D.N.A. Directory database. As well, Message Waiting (MWT) indications can be sent from D.N.A. to the time monitoring system.

The D.N.A. Time System Interface enables the D.N.A. Directory Database to receive message diversions from Time Entry Systems. If an employee checks out, the Time System can forward the check out time to the D.N.A. Server (a special time system protocol via a serial link). The D.N.A. server can then initiate a diversion for the subscriber's phone.



Compatibility with Other Network Elements

- MD110
- Business Phone

See Also

Time_System_Interface_Communications Communications%Time_System_Interface_Communications

BusinessPhone .cfg example

```
; ------
;Use to enable Automatic Logon in Windows NT
;
     Validate=
                1 or YES
                 0 , null, or NO (default)
;
    DomainName= (string)
;
     if the value is not specified, default DomainName will be used.
     UserName= (string)
     if the value is not specified, default UserName will be used.
;
     UserName will be added into DNA user table which is case sensitive if PBX
     Synchronization is selected in the pre-configuration options. It must be Exact match
:
     with NT logon name.
     Password= (string)
     if the value is not specified, automatic logon feature is disable.
;
[NTlogon]
Validate=0
UserName=seawern
Password=123456
[GICIPortConfiguration]
Enable=0
ConnectionType=BusinessLink
PortName=BusinessPhone250
;
     Enable =
                1 or Yes
;
;
                 0, null, or No (default)
                 if the value is not specified, warning will be logged and 0 will
;
                 be used as default
;
;
    NumberOfExtensions = (number)
                        A number between 0 and 200000, if not a warning will be logged
.
;
     NumberOfSubscribers = (number)
                        A number between 0 and 200000, if not a warning will be logged
;
     NumberOfConcurrentUsers
                           = (number)
;
                        A number either -1 or between 0 and 19999, if not a warning will
                        be logged. For unlimited users set the value to -1
[Licence]
```

BusinessPhone Operator Suite 5.0

Technical Guide

Enable=1 NumberOfExtensions=1000 NumberOfSubscribers=100000 NumberOfConcurrentUsers=0

; 1 or Yes Enable = ; 0, null, or No (default) ; if the value is not specified, error is displayed ; ; Users = UserID with description and the list of applications with the node numbers for which the privileges is to be set in the format [UserID]=[Full Name];[Description];[Application Abbreviation], ; [Node Number], [Node Number], ...; [Application Abbreviation], [Node Number], [Node Number] Example : tstusr=FirstName LastName;Test User Description;EMG,1,2,3; DMG; PDM, 1, 2 The above example will create a user with ID 'tstusr' and will set the maximum Privileges for application EMG for Nodes 1, 2 and 3, application DMG and application PDM for Nodes 1 and 2 : [Full Name] and [Description] are optional and can be blank ; Example : tstusr=;;EMG,1,2,3 The above example will create a user with ID 'tstusr' and Privileges set for EMG for Nodes 1, 2 and 3 To set the Privileges for all the applications in all the nodes for a ; given user use 'all' keyword instead of the application name. Example : tstusr=FirstName LastName;Test User Description;all ; The above example will create a user with ID 'tstusr' and will set the maximum Privileges for all the applications for Nodes 1 to Maximum Node When setting the Privileges for all the applications using 'all' keyword, there is no need of setting Privileges for any other applications as the privilege is set for all the applications in all the nodes for that user. Warning is displayed if done. : Below is the list of a [Application Abbreviations], The following applications are node dependent and must use with one node at least. Otherwise, error message will be displayed. ; EMG Extension Manager Extension Manager Lite EMGLITE ; MDS MD110 Support PDM Performance Manager ; ;

Technical Guide

: The fol	lowing applicat	tions are node independent Frror message will be
; display	ved if used with	n node
: alberta/	DTR	Directory Configuration
	BPDMG	Directory Manager
7	DNAWAP	Mobile Executive
;	EXPORT	Export Utility
;	HSI	HSI Configuration
;	LDAP	LDAP Configuration
;	LDAPSVR	LDAP Server
;	LDS	LDS Configuration
;	MULTNT	Operator Configuration
;	NAMEID	Name Identity Conversion
;	NPM	Numbering Plan Manager
;	OWSCNTX	OWS MD110 Centrex
;	OWSBASIC	OWS MD110 Basic
;	OWSSUPR	OWS Supervisor
;	PCOPI	Operator WorkStation
;	PPMLITE	PPM Lite
;	RDS	RDS Configuration
;	SERVER	DNA Server Configuration
;	SCS	SCS Configuration
;	TMG	Trunk Configuration
;	TSS	TSS Configuration
;	USER	User Configuration
;	VSI	VSI Configuration
;	BPOWS	BusinessPhone Operator WorkStation
;		
;======================================		
[UserPrivileges]		
Enable=1		
Administrator=Administrator;A	dmin;all	
OWS=Operator Workstation User	;OWS USER;BPOWS	; BPDMG
PowerUser=PowerUser with Min	Conf;RDSConf;RD	S;TMG;BPOWS;EXPORT;BPDMG
Supervicor=OWS Supervicor;OWS	USER; BPOWS; BPD	MG
;=====================================	r Defined ====================================	
;Profile# = Name, DATA Type,	Searchable, ico	n
;Person# = Name, DATA Type,	Searchable, ico	n
;Confidential# = Name, DATA T	уре	
;Department# = Name, DATA Ty	pe, icon	
;External# = Name, DATA Type	, Searchable, i	con
;Function# = Name, DATA Type	, Searchable, i	con
;Room#= Name, DATA Type, Sear	chable, icon	
;Information# = Name, DATA Ty	pe, Searchable,	icon
;		
;Enable =1 or 0(default) - Use	er Defined Field	ds section will be skipped if Enable=0
;		

BusinessPhone Operator Suite 5.0

```
;Maximum number of Profile fields specified by NumberProfileFields
;
             Person - 16, Confidential - 4, Department - 4, External - 6,
              Function - 4, Room - 4, Information - 4
;
;
;DATA Type from: 'N/A' =0, 'COST_CENTER' =1, 'DEPARTMENT' =2, 'EMAIL' =3,
       'NAME' =4, 'PHONE' =5, 'SECRETARY' =6, 'TEXT'=7, 'PRINTER=8',
;
;
       'TIME SYSTEM CARD NUMBER' =11, 'PAGER ID'=12,
       'ROOM'=13, 'VOICE ANNOUNCEMENT FILE' =14, 'COMPUTER' =15,
;
       'IP ADDRESS' =16, 'WWW HOME PAGE' =17, 'VOICE SYSTEM MAIL BOX NUMBER' =18,
;
       'STREET ADDRESS' =19, 'CITY' =20, 'STATE' =21, 'POSTAL CODE' =22,
;
       'COUNTRY' =23, 'COMPUSERVE ID' =24, 'MEMO ID' =25, 'MARKUP CATEGORY'=26,
       'PERSONAL MARKUP CATEGORY' =27, 'FIXED CHARGE' =28,'INFORMATION 1'=29,
;
       'INFORMATION 2' =30, 'ADDRESS 1' =31, 'ADDRESS 2' =32, 'ADDRESS 3'=33,
;
       'ADDRESS 4' =34, 'JOB TITLE' =35, 'INFORMATION_FILE' =36,
;
;
       'FAX_NUMBER' =37, 'MOBILE_NUMBER' =38, 'UNIQUE ID' =39, 'EMPLOYEE_NUMBER'=40,
       'EMPLOYEE TYPE' =41, 'CAR LICENSE' =42, 'HOME PHONE' =43,
;
;
       'FOLIO NUMBER' =44, 'GUEST STATUS' =45, 'EXTENSION TYPE' =46,
       'GROUP ID' =47, 'LANGUAGE' =48, 'AUTHORIZATION_CODE' =49,
;
       'CLASS_OF_SERVICE' =50, 'EXCHANGE ID' =51, 'USER ID' =52,
;
;
       'USER PASSWORD' =53, 'EXTENSION_CATEGORY' =54
;
;Searchable = YES or NO
;
;Icon from: NONE, FAX, PHONE, ASSISTANT, HOME,
;
             MAIL, SECRETARY, CELLULAR
========
[UserDefinedFields]
Enable=1
;Number of Profile fields is even number from 8 to 20
NumberProfileFields=14
Profile1= Prof Assistant, 6, Yes, ASSISTANT
Person1= User ID, 52, Yes
Person2= Computer Name, 15, No,
Person3= Secretary, 6, Yes, SECRETARY
Confidential1= User Password, 53, No
Person4= E-mail Address, 3, YES, MAIL
Person5= FAX Number, 37, YES, FAX
Person6= Mobile Number, 38, YES, CELLULAR
Person7= Phone Number, 5, YES, PHONE
Person8= Room Number, 13, YES,
```

InfoFile Procedure

7 Use the Windows NT Explorer to locate and execute (double-click) the Registry Editor pro gram REGEDT32.EXE in the \WINNT\SYSTEM32\ directory.

- 8 Locate the HKEY_LOCAL_MACHINE dialog panel. To locate the Registry entries you want to configure, double-click SOFTWARE Ericsson OPI, then click CurrentVersion. The Info File configuration options will be displayed in the edit window on the right.
- **9** Double-click the **InfoFileExe** entry to open the String Editor dialog box. Then type the path and name for the information application you have chosen as your operators' instructional re source (e.g., C:\INTERNET\NAVIGATOR\NETSCAPE.EXE).

Note that you must provide a full path name in this case. Once the program executes, your information resource must provide an explicit path to the instructions you wish to provide.

Stand-alone Installation - Single Node

D.N.A Server • BusinessPhone BusinessLink Sever Service (V.24 connection to PBX on COM port)

- BusinessPhone BusinessLink 32-bit Client DLL
- BusinessPhone Software Licensing Server (WIBU-Box on LPT Port)
- BusinessPhone Software Licensing Client
- MS Windows NT SQL Server or Workstation
- D.N.A. Server software (Management Repositors Server)
- Operator Suite Application (e.g.Operator Workstation and/or Directory Man ager)



Network Installation - Single Node

 D.N.A Server
 BusinessPhone BusinessLink Sever Service (V.24 connection to PBX on COM port)**

- BusinessPhone Software Licensing Server (WIBU-Box on LPT Port)
- MS Windows NT SQL Server or Workstation

	 D.N.A. Server software (Management Repositors Server)
Client 1	 BusinessPhone BusinessLink 32-bit Client DLL
	 BusinessPhone Software Licensing Client
	 Operator Suite Application (e.g.Operator Workstation, Directory Manager)
Client 2	 BusinessPhone BusinessLink 32-bit Client DLL
	 BusinessPhone Software Licensing Client
	 Operator Suite Application (e.g.Operator Workstation, Directory Manager)
Client 3	 BusinessPhone BusinessLink 32-bit Client DLL
	 BusinessPhone Software Licensing Client
	 Operator Suite Application (e.g.Operator Workstation, Directory Manager)

**) If the BusinessPhone PBX is based on Version 5.0 or higher and has also an installed IPU-board, the BusinessLink Server can communicate with the BusinessPhone via the TCP/IP connection, which means no COM port is required.



Network Installation - Sinlge Node / Server and Client combined

D.N.A Server • E

- BusinessPhone BusinessLink Sever Service (V.24 connection to PBX on COM port)**
- BusinessPhone BusinessLink 32-bit Client DLL
- BusinessPhone Software Licensing Server (WIBU-Box on LPT Port)
- BusinessPhone Software Licensing Client
- MS Windows NT SQL Server or Workstation
- D.N.A. Server software (Management Repositors Server)
- Operator Suite Application (e.g.Operator Workstation and/or Directory Man

	ager)
Client 2	 BusinessPhone BusinessLink 32-bit Client DLL
	 BusinessPhone Software Licensing Client
	 Operator Suite Application (e.g.Operator Workstation, Directory Manager)
Client 3	 BusinessPhone BusinessLink 32-bit Client DLL
	 BusinessPhone Software Licensing Client
	 Operator Suite Application (e.g.Operator Workstation, Directory Manager)

**) If the BusinessPhone PBX is based on Version 5.0 or higher and has also an installed IPU-board, the BusinessLink Server can communicate with the BusinessPhone via the TCP/IP connection, which means no COM port is required.



Network Installation Single Node / Telephony Server

Telephony Server	 BusinessPhone BusinessLink Sever Service (V.24 connection to PBX on COM port)**
D.N.A Server	 BusinessPhone BusinessLink 32-bit Client DLL BusinessPhone Software Licensing Server (WIBU-Box on LPT Port) MS Windows NT SQL Server or Workstation D.N.A. Server software (Management Repositors Server)
Client 1	 BusinessPhone BusinessLink 32-bit Client DLL BusinessPhone Software Licensing Client Operator Suite Application (e.g.Operator Workstation, Directory Man ager)
Client 2	BusinessPhone BusinessLink 32-bit Client DLLBusinessPhone Software Licensing Client

• Operator Suite Application (e.g.Operator Workstation, Directory Man ager)

Client 3

- BusinessPhone BusinessLink 32-bit Client DLL
- BusinessPhone Software Licensing Client
- Operator Suite Application (e.g.Operator Workstation, Directory Man ager)

**) If the BusinessPhone PBX is based on Version 5.0 or higher and has also an installed IPU-board, the BusinessLink Server can communicate with the BusinessPhone via the TCP/IP connection, which means no COM port is required.



Network Installation - Multi Node / Corporate Network



** ... if 2 or more BusinessLink Servers are configured within the RDS (GICI/CSTA Options tab) it is possible to monitor 2 or more different Switches in a corporate network.

You start the E-mail client before Operator Workstation be done by double-clicking the Inbox on the desktop, or the Inbox shortcut in the Startup program group in the Windows NT/2000 user profile used by each operator. If an Operator Workstation shortcut is also included in the startup group, make sure that it runs after the e-mail client.

Obtaining an E-mail Address

Operator Workstation looks in two places: the Address Book for the local MAPI-compliant e-mail system (by using the MAPIResolveName function in mapi32.dll), and in the user-defined fields of the "subscriber" table in the SQL database "dirdb" which are of type EMAIL. (Note: Operator Workstation must have a data connection to the SQL server or it will not try to send e-mail.)

E-mail Related D.N.A. System Administration

There are a number of administrative tasks to perform for successful integration of e-mail with Operator Workstation, including directory configuration, RDS configuration, and system maintenance.

Directory Configuration

Use the Directory Configuration Utility to define any EMAIL fields in the database - before running any other programs that will use the database, e.g. Directory Import, Directory Manager, and Operator Work Station.

RDS Configuration

Use the RDS Configuration Utility to control how the Message Waiting lamps on subscriber telephones are utilized when e-mail messages are sent. It is usually best to not turn on the Message Waiting Lamp for e-mail messages because the subscriber can retrieve them without the operator's help. When RDS is configured to turn the lamps on, they are only extinguished when the operator deletes or prints all the messages for a subscriber.

System Maintenance

D.N.A. user account permissions - Control over the Operator Workstation e-mail options (and all the other Operator Workstation user configuration settings) is determined by the Preferences permission for the Operator Workstation in the D.N.A. User Configuration Utility. Choose Read/Write to allow operators to change their settings. Choose Denied to prevent changes.

Subscriber database maintenance - It is important for continued success that changes in the D.N.A. subscriber database, the Windows NT/2000 user accounts, and the e-mail accounts are coordinated. Establish a procedure whereby updates in one system are made available for review and possible update in the other systems. Consider appointing someone specifically responsible for directory updates.

Troubleshooting

Two effective ways of troubleshooting Operator Workstation e-mail problems involve using Windows NT/2000's Performance Monitor, and the D.N.A. Remote Data Monitor utility.

Troubleshooting Operator Workstation E-mail with Performance Monitor

Technical Guide

Check whether Operator Workstation has successfully attached to a MAPI session with the help of Performance Monitor. When Windows Messaging (which is actually an Exchange client) is running, there are two processes of interest: exchng32.exe and mapisp32.exe. Set up Performance Monitor to watch the processor time and thread count for these two by selecting "Add to Chart", Object: Process, Instance: mapisp32.exe, and Counter: "% Processor time". Add another trace by selecting Counter: "Thread Count". Repeat the counter selections for Instance: exchng32.exe, then click "Done". You should have four traces on the chart now. If e-mail is sent with the mail program or by the Operator Workstation Message dialog, spikes will be seen in the processor time for both processes. Now "Exit and Log Off" from the mail program. If Operator Workstation succeeded with it's NULL MAPI logon, the thread count for mapisp32.exe will remain constant while the count for exchng32.exe falls to zero. If it has not, the thread count for mapisp32.exe will fall to zero within a few seconds of exchng32.exe.

Troubleshooting Operator Workstation E-mail with Remote Data Monitor

Use the Remote Data Monitor to help determine when messages are sent via e-mail. RDM.EXE is the utility program, usually found on the D.N.A. server at DNA_S\MRS\BIN, which reports Remote Data Service events. When RDS is configured to not turn on the Message Waiting lamps for e-mail, a lit lamp indicates that e-mail was NOT sent. The events reported by RDM enable you to determine whether the lamp was turned on without the need to go to each telephone.

The following typical sequence of RDS events indicates e-mail was sent.

[97/12/24 10:32:30] I7027 - Message From Client 1724: Message Waiting On; RecordID=780, NodeID=1, DN=66794

[97/12/24 10:32:31] I7128 - Broadcast To Clients: Message ID=7, TableID=1, RecordID=780, Update Type=8

[97/12/24 10:32:31] I7132 - Local Database Update Event Signal

[97/12/24 10:32:31] I7128 - Broadcast To Clients: Message ID=7, TableID=1, RecordID=780, Update Type=8

[97/12/24 10:32:31] I7296 - Local Database Update End Of Event Signal

The next sequence indicates a failure. Note the extra message sent via the MD's GICI port to turn on the lamp.

[97/12/24 10:36:00] I7027 - Message From Client 1724: Message Waiting On; RecordID=780, NodeID=1, DN=66794

[97/12/24 10:36:00] I7128 - Broadcast To Clients: Message ID=7, TableID=1, RecordID=780, Update Type=8

[97/12/24 10:36:00] I7132 - Local Database Update Event Signal

[97/12/24 10:36:00] I7128 - Broadcast To Clients: Message ID=7, TableID=1, RecordID=780, Update Type=8

[97/12/24 10:36:00] I7296 - Local Database Update End Of Event Signal

[97/12/24 10:36:00] I7182 - Message To GICI ERICSSON1 Communication Port COM3: \0x02066679400\0x0D\0x0A

More Operator Workstation Information

- Troubleshooting
- Directory Assistance Databases
- Frequently Asked Questions

Remote Data Server

Remote Data Server (RDS) is a D.N.A. service module that maintains continuous network database synchronization between PBX nodes, the D.N.A. SQL server, and all D.N.A. local databases.

Security Data Server

The Security Data Server (SDS) provides high-level security in the form of licensing enforcement. SDS references encrypted licensing data to enforce authorized license limits. SDS also accesses data based on Logging Facilities Server requests.

System Clock Synchronization

D.N.A. client and server installations maintain ongoing clock synchronization. D.N.A. Server provides synchronization via client polling, server-initiated client updates, and clock drift monitoring and correction with the server's clock as reference.

To Generate Reports Using Access

- 1 Click the Attach Table tool on the Access toolbar to attach the SQL Database.
- 2 After selecting SQL Database, Access prompts you for a data source. Select the data source pointing to the SQL server with BusinessPhone data.
- 3 Login to the SQL server by entering thirdpty as the user ID and password. Click on the Options buttons to select a database.
- 4 Select a table from the list displayed and attach all tables that you want to use for your reports.
- 5 Click on the Query tab, and then on the New button to define a New Query. In order to correctly set the table relations, you should refer to the technical documentation for the specific D.N.A. application.
- 6 After setting the table relationships, run the query and check the results to see if the data is coming back correctly. Click on the ! tool on the toolbar to run the query.
- 7 Once you are satisfied with your query, click on the **Report** tab and then click on the **New** button. Access prompts you with the Database dialog box. Select the query that you defined in the previous steps, and then click on the **Report Wizard** button.
- 8 The report wizard guides you through the steps of defining a report.
- **9** Select the fields and the sort order that you want to include in your report, and define the report style and page orientation.
- **10** The Report Wizard asks you for a report title. After you have entered the title of the report, you can choose to run the report or go to report design view to further customize the report layout.

To Log Off

If the application is your only logged D.N.A. application, you will be logged off both that application and the D.N.A. Server. However, if you are logged on to other D.N.A. applications, you will only be logged off the current application. Your access to the other applications will not be affected.

- 1 Select Exit from the Application menu.
- 2 Click **OK** on the confirmation dialog box. Your session will be terminated.

To Logon

- 1 When you select a D.N.A. support application from the **Administrative Tools** taskbar, the support application will start, and the User Log On dialog box is displayed.
- 2 Type your User Name and Password into the corresponding edit boxes. As you type the password, a string of asterisk characters (*******) appears in the Password edit box, one asterisk for each character you type. Both the User Name and Password fields are case-sensitive, and you are allowed only a limited number of attempts.
- 3 Select a local or remote server from the **DNA Server** drop-down list. The initial security authorization check and all subsequent validation actions are directed toward the server you select.
- 4 Click the **OK** button. If your user name and password are valid, you will be logged on to the application with the access authorizations permitted in your user profile.

Index

Α

Access	
Administrative Tools	
Application Data	
Application Link	
Applications	
Archival Backup	

В

Backup	
Basic Configuration for the Server	80
Basic Requirements	
BusinessPhone .cfg example	
5 1	

С

38, 143, 144, 145, 146

D

D.N.A	10, 11, 12, 60, 141, 142
D.N.A. CAAPI	
D.N.A. CTI	
D.N.A. Server	
Data	
Database	
Database Compression	
Database Organization	
Databases	
Directory Assistance	
Directory Browser	29, 30, 31, 32, 75, 77
Directory Configuration	
Directory Database	114, 117

Directory Export	
Directory Import	
Directory Link	
Directory Manager	, 109, 111, 132, 134, 135, 136
Directory Setup for Network Installations	
Directory Structures	

Ε

ECA	
E-Mail	
Error Messages	
Event Log	
Event Viewer	
Excel	
Extension Link	
Extension Manager	

F

Facilities	5
FAQ	5

G

Glossary	. 13
4	

Hard Disk	42
Hardware	58

I

Installation 46, 47, 48, 49, 51, 52, 53, 54, 55, 56, 57, 58, 60, 61, 69, 70, 71, 72, 73, 74	9, 80, 87, 88, 89
Installation Checklists	59
Internet Tools	

L

DAP	
DAP Configuration	
cense Administrator	
cense Viewer	
mitations	
ocal Data Server	
ocal Database	
9g Files	
og Off	
ogging	
ngon	
otus Notes	

Μ

Maintenance						
MD110 BC						
MD110 Support						
Messages	87, 179, 180, 181					
Mobile Executive	. 26,	29,	73,	74,	75,	112
------------------	-------	-----	-----	-----	-----	-------
MSDE					40), 41

Ν

Customer Groups;Service Provicer	155
Network Installation - Multi Node / Corporate Network	190
Network Installation - Sinlge Node / Server and Client combined	188
Network Installation Single Node / Telephony Server	189
Network Installations - Single Node	187
New Features	. 15
Next CC	. 23

0

OneBox	
Operator Configuration	
Operator Workstation	111, 131, 132, 134, 135, 137, 138, 139, 162, 163
Outlook Integration	

Ρ

Passwords	
PBX Command Settings	38
PBX Hardware / Software Requirements	
PDM	101
Performance	85, 86
PPM Lite	
Pre-configured Installation	60
Pre-Installation	
Problem Reporting	

R

RDS Performance	
Registry	
Registry Settings	
Remote Data Monitor	
Remote Data Server	
Reports	
Requirements	
Restore	
RichWin	

S

SCS	
Security	
Serial Communications Server	
Server	
Server Configuration	
Server ID	
Server Installation	
Server Requirements	
Servers	
Services	
Settings for Operator Workstation	

Settings for the Directory Manager	
Short Message Service	
SNMP	
SNMP Agent	
SNMP Master Agent	
Software	
Software Licensing	
SQL Database	
SQL Server	
Stand-alone Installation - Single Node	
Supported D.N.A. Server / Client Configurations	

Т

Tempoary Workspace
Time System Interface
Time System Server
Transaction Log
Troubleshooting
Trunk Manager

U

Upgrade	. 51
Upgrading To Operator Suite 5.0	. 63
User Configuration	. 96
Users	. 97
	-

V

Visitor Registration	35
Voice System Interface	

W

WAP	26,	27,	. 28
Windows	, 48,	49,	50
Windows 2000			. 51

Ericsson is shaping the future of Mobile and Broadband Internet communications through its continuous technology leadership. Providing innovative solutions in more than 140 countries, Ericsson is helping to create the most powerful communication companies in the world.

Ericsson Enterprise AB All rights reserved. For questions regarding the product, please contact your Ericsson Enterprise Certified Sales Partner. Also visit us on www.ericsson.com/enterprise